YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

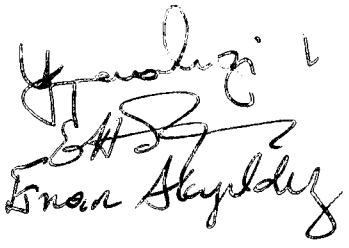
HİYERARŞİK GRUPSAL KURUMLARDA KULLANILACAK BİR ŞİFRE SİSTEMİ

Bilgisayar Yük. Müh. Vedat COŞKUN

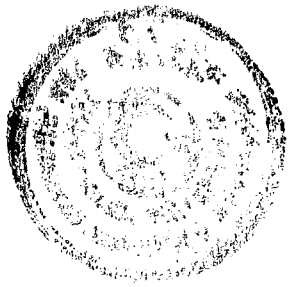
F.B.E. Bilgisayar Bilimleri ve Mühendisliği Dalında
Hazırlanan

DOKTORA TEZİ

Tez Savunma Tarihi : 28 Mayıs 1998
Tez Danışmanı : Prof. Mehmet Yahya KARSLIGİL (Y.T.Ü.)
Jüri Üyeleri : Prof. Dr. Emre HARMANCI (İ.T.Ü.)
Prof. Dr. Ersan AKYILDIZ (O.D.T.Ü.)



İSTANBUL, 1998



İÇİNDEKİLER

SİMGE LiSTESi

d	şifre çözme anahtarı (Decryption Key)
e	şifreleme anahtarı (Encryption Key)
c	uygun sayı (adayı)
g_A	A grubu anahtarı
a	ipucu (hint)
p, q	asal sayı
n	üzerinde modül işlemi yapılan sayı.
$\phi(n)$	Euler Totient fonksiyonu
M	açık mesaj
C	şifreli mesaj (Cryptotext)
E	şifreleme fonksiyonu (Encryption)
D	şifre çözme fonksiyonu (Decryption)
u	uygun sayı
$U(p,q,s)$	uyum adedi
$U_o(p,q \in \{P_L..P_R\},s)$	uyum oranı
$U_{oo}(p,q \in [P_L..P_R],s)$	uyum oranı ortalaması
$U_{ooo}(p,q \in [P_L..P_R],s)$	uyum oranı ortalama ortalaması
Z	tamsayılar { 0, ±1, ±2, ±3, … }
Z^+	pozitif tamsayılar { +1, +2, +3, … }
N	natural numbers : doğal sayılar { 0 } + Z^+
P	prime numbers : asal sayılar kümesi
P_i	i'inci asal sayı; ($P_i < P_j$) ⇔ (i < j); ($P_i = P_j$) ⇔ (i = j)
[a .. b]	{ x ∈ R | a ≤ x ≤ b }
$\lceil x \rceil$	üste yuvarlatma (round up, ceiling)
$\lfloor x \rfloor$	alta yuvarlatma (round down, floor)
[x]	en yakın tamsayıya yuvarlatma
∈	elemanı (element of)
=	eşit
≠	eşit değil
≥	küçük değil
≤	büyük değil
$a \mid b$	a, b'yi böler
$a \nmid b$	a, b'yi bölmez
$\equiv_n$	n modülüne göre denk
$a \equiv_n b$	a ve b, n modülüne göre denktir.
$a = b \ /n$	a ve b, n modülüne göre denktir.
Λ	ve
V	veya
$a \leftarrow b$	a, b'nin değerini alır

ŞEKiL LiSTESi

TABLO LiSTESi

TEŞEKKÜR

Beni eğiten ilkokul, ortaokul, lise, Harp Okulu öğretmenlerime;

Akademik formasyonumu kazanmama yardımcı olan NPGS öğretim üyelerine;

Bilgisayar sevgimin kıvılcımı olan Lcdr. BRADBURRY'ye;

Çalışmalarım için gerekli zamanı bana veren anlayışlı Yb. Lütfi SEVİNÇ'e;

Tezimin bilimsel kontrolünü yapan Doç. Kirkor HARUTUNYAN'a;

Sıcak bir yakınlık ve yardımda bulunan Y.T.Ü. Bilgisayar bölümü araştırma görevlilerine;

Tezimin gelişimine katkıda bulunan Prof. Dr. Ersan AKYILDIZ'a;

Değerli desteği nedeni ile Prof. Dr. Emre HARMANCI'ya;

Fedakar ve anlayışlı annem Fatma COŞKUN'a;

Bugünümü borçlu olduğum biricik babacığım Mehmet COŞKUN'a;

Onsuz başarılı olamayacağım; her zaman sonsuz destek veren değerli hocam

Prof. Mehmet Yahya KARSLIGİL'e

çok teşekkür ederim.

Çalışmamı,

yaşamımın temel dayanağı olan

canım kardeşim

Selma YETKİNER'e adıyorum.

ÖZET

Kurumlar, etkinlik alanlarına bağlı olarak askeri, devlet güvenliği ya da ticari kaygılardan dolayı bünyelerinde mevcut bilgilerin güvenliğini sağlamak isterler. Alınabilecek fiziksel güvenlik yöntemleri yetersiz kaldığında ise bilgi güvenliğini sağlamanın tek yolu, şifreleme yöntemlerinin kullanılmasıdır.

Kurumlar, işlevsel farklılıklar içeren gruplardan oluşurlar. Bilgiler konularına göre farklı grupları ilgilendirebilir. Gruplar içinde de personelin görev farklılığını temel alan bir hiyerarşik seviyelendirme mevcuttur. Bir bilgi bir grubun yalnızca en üst seviyedeki yöneticisini ilgilendirirken, başka bir bilgi daha alt seviye personelini de ilgilendirebilir.

Bu çalışma, hiyerarşik grupsal kurumlarda veri aktarma iletişim güvenliğini sağlamak için kullanılabilecek bir modern (açık anahtarlı) şifre sistemi tanımını içermektedir. Anahtarların üretim, korunma ve dağıtımı ile mesajların dağıtımından Mesaj Dağıtıcısı (MD) sorumludur. MD, sistemde mevcut her kişiye ait olduğu gruba ilişkin bir, ve hiyerarşik seviyeye ilişkin olarak bir olmak üzere iki anahtar dağıtacaktır. Mesajlar, sistemde dağıtılmadan önce hedef grup ile hiyerarşik anahtarların kullanımı ile iki kez şifrelenecektir. İlgili grup ile seviyede bulunan kişiler, ellerindeki anahtarları kullanarak şifrelenmiş mesajları çözebilirler; böylece mesajların ilgili seviye ve gruptaki personel tarafından okuyabilmesi garantilenmiş olur. Anahtar mevcut olmadığı durumda ise şifrelenmiş mesajlardan asıl mesajları üretmek mümkün değildir.

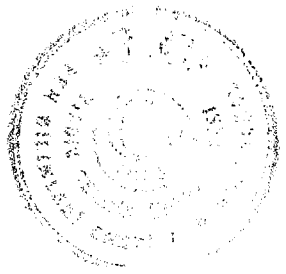
Çalışma: kullandığı algoritma ile, tanımlanan grupsal hiyerarşik modelde şifrelemeyi sağlaması, alt seviye anahtarlarının basit bir işlem ile üretilebilmesi ve yalnızca iki anahtarın muhafazasına ihtiyaç duyurması nedenleri ile özgün bir algoritmayı içermekte olup, bu algoritmada RSA ile El Gamal şifre sistemleri tarafından kullanılmış ve güvenli oldukları ispatlanmış olan tek-yönlü NP-Complete fonksiyonlar temel olarak alınmıştır.

ABSTRACT

The data transferred in an organizational information system must be strictly prevented from exposing by the unautorized users. This study includes the definition of a public-key cryptosystem which can be used in hierarchical and departmental (role-based) organizations to ensure data security. The organizations are composed of departments. While general issues are related to all of the departments, some issues may be related to only one of them. In the meantime, there is a hierarchy in each department. The information may be related to the head of the department (level 1), or to the other levels also. The people in a specific level in the hierarchy is assumed to be capable of viewing the messages addressed to the lower levels too.

Message distributer (MD) is responsible of generating, keeping, and distributing the keys and distributing the messages. MD will distribute a departmental and a hierarchical key to each user according to his/her department and level of hierarchy. The messages will be encrypted twice before the transmission: first using the departmental, and then the hierarchical key. This ensures that the people in the target department and hierarchy can decrypt the encrypted message and read the original message. By using "Hard Problems", it is ensured that the intruders cannot view the original message. The personel in a higher level in the hierarchy can generate the intended level's key via a simple process and decrypt the encrypted message thereafter. This way, people do not need to keep the keys for the lower levels in the hierarchy.

This work includes a cryptographic algorithm designed for the hierarchical and departmental which hasn't been done before, allows production of the lower level keys via a simple calculation which disregards the necessity to hold more than two keys, so it is original. The problems used by RSA and El Gamal Scheme are used properly as a base to ensure higher security.



1. GİRİŞ

1.1 Şifreleme Sistemleri

Bilgilerin gizli kalma gereksinimi, askeri ve diplomatik mesajların güvenli olarak aktarılma zorunluluğu sonucu ortaya çıkmıştır (Seberry, 1989). Bu zorunluluğun başlangıcı ise, medeniyetin başlangıcı kadar eskilere dayanır: örnek olarak eski Ispartalılar, askeri mesajları şifrelemişlerdir. İlk şifrelenmiş bilgi transfer yöntemleri çok basit şekildedir ve bu sistemlerin güvenlikleri temelde kullanılan kuryelere bağlı kılınmıştır; bilgilerin güvenliği kuryenin güvenilirliği ile, mesajın açığa çıkma tehlikesi karşısında alacağı önlemler konusundaki yeteneklerine bağlı olmuştur.

Bilgisayar konusundaki gelişmeler ile birlikte dünya üzerinde birbirinden çok uzakta bulunan bilgisayarların ağ üzerinde birbirleri ile iletişimli olarak çalışmaya başlamalarının sonucu olarak yirminci yüzyılda bilgilerin korunma yöntemlerinde, eski tarihlerdekine nazaran büyük değişiklikler ortaya çıkmıştır. Bilgisayar sistemlerinin ilk olarak ortaya çıktığı dönemlerde fiziksel güvenlik önlemleri, topyekün bilgi güvenliğini sağlamak için yeterli olurken; zaman paylaşımlı sistemler ortaya çıkıp bir bilgisayara bağlı terminaller büyük alanlara yayıldığında ise artık fiziksel güvenlik yöntemi yetersiz kalmıştır.

Zaman paylaşımlı bilgisayar sistemleri ve bir ağ üzerinde çalışan bilgisayarlar için sözkonusu olan bilgi güvenlik sorunları temelde, hem bilgisayarlar ile bunlara fiziksel olarak bağlı olan terminaller arasında, hem de bilgisayarlar arasında mevcut olan iletişim hatlarının güvenliği ile ilişkilidir. Bu hatlar, doğal özelliklerinden dolayı yetkisiz kişilerin erişimine açıktır. Bu durumda yalnızca fiziksel güvenlik önlemleri, bilgilerin güvenliğini sağlamak için yetersiz kalmaktadır. Bu şekilde fiziksel güvenlik yöntemlerinin yetersiz olacağı iletişim hatlarında bilgi güvenliğini sağlamanın tek yolu, şifreleme yöntemlerinin kullanılmasıdır. Sonuç olarak transfer edilen bilgilere yetkisiz kişilerin erişim olasılıkları mevcut, ve alınacak fiziksel önlemler bu olasılığı yeterli düzeyde ortadan kaldırmıyor ise bilgilerin güvenliğini sağlamak üzere şifreleme kullanılır. Şifreleme sistemi, transferi amaçlanan bir yazının gönderici tarafından form değişikliğine uğratılarak kodlu hale

getirilmesi; kodlanmış bilginin alıcıya gönderilmesi; alıcı tarafından kodlu bilginin yeniden dönüşüme uğratılarak normal yazının elde edilmesi ana safhalarından oluşur.

Bilgilerin güvenli iletişimi sağlanmak istendiğinde, bir *şifreleme algoritması* ile *şifreleme protokolü* tanımlanmalıdır. Şifreleme algoritması asıl mesajın kodlu mesaja, kodlu mesajın ise asıl mesaja dönüştürülmesi işleminin tanımını içeren bir algoritmadır. Şifreleme protokolü ise, bilgi transferinin güvenli bir şekilde yapılmasını sağlamak üzere tanımlanmış ve şifreleme algoritmasının kullanılma şeklini de içeren kurallar topluluğudur (Kemmerer, 1988).

Şifre sistemlerinin ilk kullanım şekli, *klasik şifre sistemleri* olarak tanımlanır. Bu sistemlerin temel özelliği, şifreleme ve şifre kırma anahtarlarının ya aynı olmaları, ya da birisi kullanılarak diğerinin üretilmesinin çok kolay olmasıdır. Bu nedenle şifre sisteminin güvenliği, kullanılan anahtarların güvenliğinin sağlanabilmesine bağlıdır, anahtarlardan birisini elde eden kişi, şifre sistemi de kırmış sayılır. Anahtar gizli tutulabildiği taktirde ise; alıcı, anahtar yalnızca gönderici ile kendisinde olduğu için mesajı göndericinin kimliğinden; gönderici de mesajı kimin alacağından emin olur. Klasik şifre sistemleri, *tek anahtarlı* ya da *simetrik şifre sistemleri* olarak da adlandırılırlar (Simmons, 1979). 1976 yılında Diffie ve Hellman tarafından yapılan bir çalışma ile de *modern şifre sistemleri*nin temelleri atılmıştır (Diffie, 1976). Bu tür şifre sistemlerinde *gönderici* ve *alıcı* tarafından iki ayrı anahtar kullanılmaktadır; bu anahtarlardan herhangi birisi kullanılarak diğer anahtarın üretimi ise mümkün değildir. Modern şifre sistemleri, *çift anahtarlı, açık anahtarlı* ya da *simetrik olmayan şifre sistemleri* olarak da adlandırılırlar (Simmons, 1979).

Modern şifre sistemlerinin güvenliği, tasarımda kullanılan *NP problem*lere dayanır. Bunlardan bir tanesi "Verilen a ve b sayıları için $a^x = b \ mod \ n$ eşitliğini sağlayacak olan x sayısını bulma işlemi" olarak tanımlanan *ayrık logaritma* problemidir. William Diffie ile M.Hellman, modern şifre sistemlerinin ilk örneğini oluşturdukları şifre sisteminde, bu problemi temel olarak kullanıp dinlemeye açık kanallarda anahtar transferini mümkün kılan bir algoritma geliştirmişlerdir (Diffie, 1976). Bu algoritmada G göndericisi, A alıcısına bir anahtar göndermek istemektedir. Bu amaçla asal olan bir n sayısı ile bu sayıya göre nispi olarak asal olan bir x sayısı seçilir. G $x^a \ mod \ n$ sayısını A'ya, A ise $x^b \ mod \ n$

sayısını G'ye gönderdiğinde, hem A hem de $G\ x^{ab}\ mod\ n$ sayısını hesaplayabileceğinden; başka kimsenin bilmediği bir anahtarı birbirlerine aktarmış olurlar. Shumely ile McCurley, bu algoritmayı asal olmayan n sayısının kullanılma durumuna göre geliştirmişlerdir. El Gamal ise bu problemi şifrelemede direkt olarak kullanmıştır (Elgamal, 1985). Modern şifre sistemlerinin dayandığı bir başka problem de asal olmayan bir sayının asal çarpanlarını bulma problemidir; Rivest, Schamir ve Adleman'ın bu problemi kullanarak geliştirdikleri RSA şifre sistemi ise bu alanda en fazla bilinen algoritmadır (Rivest, 1978).

1.2 Grupsal Kurum Modeli

Kurumlar, işlevlerine bağlı olarak gizlilik gerektiren bilgileri kullanabilirler. Örnek olarak askeri kurumlar, bünyelerinde gizli bilgiler içerirler. Diğer devlet kurumları da, kurumun ülke güvenliği ile olan ilişkisi oranında gizli bilgilere sahip olurlar. Ticari kuruluşlar, ticari kaygılardan dolayı sahip oldukları üretim yöntemleri, iş yapılan diğer şirket bilgileri, şirketin mali durumu, geleceğe ait yatırım ve üretim planları vb. bilgileri saklı tutmak ve özellikle rakip ticari kuruluşların eline geçmesini önlemek isterler.

Kurumlar, sahip olacakları bilgilerin kurum dışındaki kişiler ile, kurum içindeki yetkisiz kişilerin eline geçmesini önlemek amacı ile ilk önlem olarak güvenilir personel ile çalışmak ister; çünkü kurum başka ne önlem alırsa alsın, güvenilmez bir personel elindeki bilgiyi yetkisiz kimselere aktarabilir. Bir işte çalıştırılacak kişinin güvenilirlik derecesi de, bu kişilerin erişecekleri bilgilerin önem ve gizlilik derecesine bağlı olarak değişir. Çok gizli bilgilerin ancak çok güvenilir personelin erişiminde olması istenirken, gizli olmayan bilgilerin çok daha az güvenilir personelin eline geçmesi kabul edilebilir bir seçenek olarak ortaya çıkar. Her personelin, güvenilirliği ne olursa olsun, yalnızca kendi konusu ile ilgili bilgilere erişebilmesi; başka konularla ilgili kişilerin ise erişimlerinin engellenmesi istenir. Örnek olarak yalnızca muhasebe grubuna ilişkin çok gizli bir bilginin, çok güvenilir de olsa başka bir bölümde çalışan ve konu ile ilgisi olmayan bir personelin eline geçmesinin önlenmesi gereklidir.

Özet olarak kurumlar, işlevlerini yerine getirmek üzere gruplardan oluşurlar. Herbir grup bir ya da daha fazla personelden oluşabilir. Gruplar içinde de hiyerarşik bir yapı mevcuttur. Bazı kişiler görevleri gereğince bu hiyerarşik yapı içinde en alt seviyede olurlar; bu

kişilerin üzerlerinde ise bölüm başkanları, yöneticiler vb. bulunur. Yöneticilerin üzerinde ise grubun en üst düzey sorumlusu bulunur. Dolayısı ile bilgilerin güvenliği dikkate alındığında hem grupsal, hem de güvenlik derecesine ilişkin farklılıklar dikkate alınmalı, ve bilgi transferleri buna göre yapılmalıdır. Güvenlikte buna *bilmesi gereken ilkesi* denir, yani herkes yalnızca bilmesi gerekeni ve bilmesi gerektiği kadarını bilecektir.

1.3 Yapılmış Çalışmalar

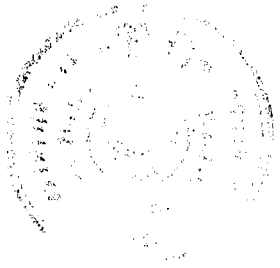
Hiyerarşik ve grupsal kurumlarda kullanılacak herhangi bir şifre sistemi daha önce tanımlanmamıştır. Yalnızca Grupsal bir model için kullanılabilecek olan bir şifre sistemi, El Gamal şeması kullanılarak tasarlanabilir. Bu şifre sistemi, her grup için ayrı anahtarların kullanılması yolu ile kişilerin kendi gruplarından başka gruplara ait bilgilere erişmeleri engelleyebilir. Grupsal sistemlerde kullanılabilecek anahtar dağıtım yöntemleri hakkında çalışmalar Tzonelih Hwang (Hwang, 1992) ile W.P.Lu ve M.K.Sundareshan (Lu, 1992) tarafından yapılmıştır.

Chin-Cheng Chang mesajları önemine, ivediliğine ve açık bilgileri içerme durumuna göre sınıflandırmak gerektiğini belirterek belirli kişilere gönderilmesi gerekli olan bilgilerin şifrelenmesini sağlayan bir şifre sistemi geliştirmiştir (Chang, 1993).

Diğer yandan Selim G. Akl ile Peter D. Taylor tarafından tanımlanan şifre sistemi, hiyerarşik modelde kullanılacak bir şifre sisteminin tanımını içermektedir (Akl, 1983). Bu tez çalışmasında tanımlanmış olan şifre sistemi ise, hiyerarşik ve grupsal yapının her ikisini de içermesi bakımından yeni ve özgündür.

1.4 Çalışmanın Bölümleri

Bu çalışma, yukarıda tanımlanan hiyerarşik grupsal kurum modeli içinde transfer edilecek bilgilerin yalnızca yetkili grup ve minimum erişim seviyesinde bulunan kişiler tarafından okunabilmesini sağlayan şifre sistemi tanımı ile buna ilişkin yapılan hesaplama ve analizleri içermektedir. Şifre kırıcıların kurum içinde aktarılan şifreleri çözmeleri ise *NP problem*lerin kullanılması yolu ile engellenmektedir.



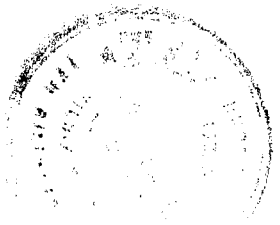
Yukarıda kısaca açıklananan hiyerarşik grupsal modelin detaylı tanımı, çalışmanın ikinci bölümünde yer almaktadır. Bu bölümde ayrıca önerilen modelin dayandığı matematiksel temel, sayı teorisi ile karmaşıklık teorisine ağırlık verilerek ele alınmaktadır.

Tanımlanmış olan hiyerarşik grupsal model için önerilen şifre sisteminin tanımı ile örnek uygulamaları, üçüncü bölümde verilmiştir. Öncelikle, hiyerarşik grupsal model için tanımlanan şifre sisteminin amacı, daha sonra da önerilen şifre sisteminin uygulama adımları açıklanmıştır. Şifre sistemi, *ayrık logaritma* ile *faktörlere ayırma* problemlerini kullanarak, bir grup ile minimum erişim seviyesinde bulunan personelin okuyabileceği mesajların buna yönelik olarak şifrelenerek bilgisayar sisteminde yayınlanması; hedef kitlenin de ellerinde bulunan grup ve seviye anahtarlarını kullanarak şifrelenmiş mesajı çözerek asıl mesajı elde etme genel adımlarından oluşmaktadır. Ek bir özellik olarak şifre sistemi: bir kişinin dilediğinde aynı grubun kendine göre daha alt seviyesine adresli mesajları çözme etmek üzere, elindeki seviye anahtarının kare değerini alarak alt seviye anahtarını elde etme kolaylığını sağlayacak şekilde tasarlanmıştır. Böylece bir kişinin kendine göre aşağıda bulunan tüm seviyeler için ayrı bir anahtarı muhafaza etme zorunluluğu yok edilmiştir. Bir seviye anahtarı kullanılarak üst seviye anahtarını elde etme işlemi ise *NP problem* çözümünü gerektirdiğinden, olanaksızdır.

Şifre sistemi, şu nedenlerle özgün bir çalışmadır:

- Tanımlanan grupsal hiyerarşik model için öngörülen ilk çözüm olması.
- Bir kişinin elinde bulunan seviye anahtarını kullanarak kendisine göre alt seviyenin anahtarını basit kare alma işlemi ile üretebilmesi; üst seviye anahtarı üretiminin ise NP problem kullanımı yoluyla engellenmiş olması.
- Alt seviye anahtarının kolaylıkla üretilebilmesi sağlandığından, bir kişinin kendisine göre alt seviyedeki tüm anahtarları elinde tutma gereksinimininin ortadan kalkmış olması.

Şifre sistemi içinde kullanılmakta olan değerler ile bunların sahip olmaları gereken özelliklere ek olarak, bu değerlerin nasıl üretileceği ve dağıtılacağı ile, kimlerin hangi değerlere erişim haklarının olması gerektiğine de bu bölümde yer verilmiştir. Bölümün



sonunda, iki grup ile dört erişim seviyesine sahip örnek bir kurum için tasarlanan şifre sisteminde kullanılabilecek bir uygulama yer almıştır.

Şifre sisteminde, seviye anahtarları üretimine temel teşkil eden bir c sayısı vardır. Seçilebilir c sayısının n'ye oranının, büyük p ile q sayılarının kullanılma durumunda azalmaması, şifre sisteminin kullanılabilirliğini artıracaktır. Bu konuda yapılan hesaplamalar ile analizler, dördüncü bölümde verilmiştir. Bu bölümde ayrıca p ile q sayılarının seçimine ilişkin tanımlar, hesaplamalar ve bu hesapların analizleri de bu bölümde yer almıştır. Yapılan hesaplamalar sonucunda p ile q sayılarının büyümesi karşısında seçilebilir c sayısının n'ye oranında bir azalma olmadığı görülmüştür. Şifre sistemi tasarımcısının şifre sisteminin güvenliğini sağlamak üzere büyük p ile q sayıları seçerken uygulayacağı yöntemin nasıl olması gerektiği, yapılan hesaplamalar sonucu elde edilen sayılar ve bunlara ilişkin grafikler ise çalışmanın ekinde sunulmuştur.

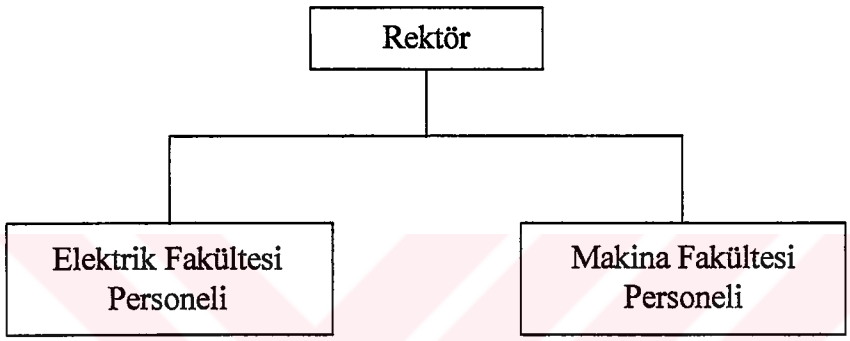
Çalışmanın sonuçları, beşinci bölümde yer almaktadır. Önerilen şifre sisteminin hiyerarşik ve grupsal şifre sistemlerin güvenli bilgi transferinde kullanılabileceği, kurumda mevcut personelin kendi grubu ile en az seviyesine adresli şifrelenmiş mesajları elinde bulunan grup ve erişim seviye anahtarlarını kullanarak çözebileceği ve bu şekilde asıl mesajı elde edebileceği, alt seviyeye ilişkin anahtarların elde bulunan seviye anahtarı kullanılarak kolay bir işlem ile üretilebileceği, ve bu şekilde aynı şifre çözme işleminin gerçekleştirilebileceği, üst seviye anahtarının üretiminin ise olanaksız olduğu detaylı olarak anlatılmıştır. Şifre sistemi tasarımcısının ise büyük sayılar seçmesi gerektiği, büyük sayılarla çalıştığında ise şifre sistemi güvenliğinin azalmayacağı ve bu seçimde hangi kriterlere dikkat etmesi gerektiği yine bu bölümde anlatılmıştır. Bu çalışma temel alınarak yapılacak ilerideki çalışmaların, tasarlanan şifre sistemini hangi yönleri ile geliştirebilecekleri konusundaki öneriler ayrıca belirtilmiştir.

2. DAYANILAN TEMEL

2.1 Hiyerarşik Grupsal Kurum Modeli

2.1.1 Grupsal kurum (role-based security)

Kurumlar, işlevlerini yerine getirmek üzere gruplardan oluşurlar. Herbir grup bir ya da daha fazla personelden oluşabilir. Örnek olarak bir üniversite personeli Şekil-2.1'deki gibi gruplandırılabilir.

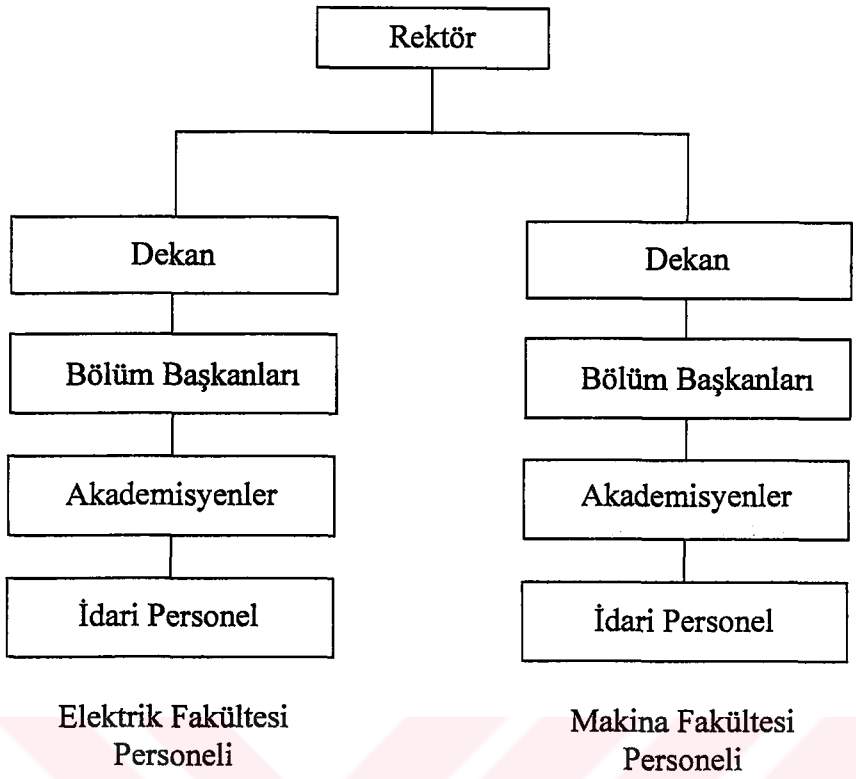


Şekil 2.1 Grupsal Kurum Yapısı

Şekil-2.1'de iki fakülteden oluşan bir üniversite gösterilmiştir. Üniversite'nin yapısı içinde en üstte Rektör vardır. Şekilde gösterilen her iki fakülte personel grubu içinde ise Dekanlar, Bölüm Başkanları, Akademisyenler ve idari personel yeralmaktadır.

2.1.2 Hiyerarşik grupsal kurum

Gruplar içinde de hiyerarşik bir yapı mevcuttur. Bazı kişiler görevleri gereğince bu yapı içinde en alt seviyede olurlar, bu kişilerin üzerlerinde ise bölüm başkanları, yöneticiler vb. bulunur. Yöneticilerin üzerinde ise grubun en üst düzey sorumlusu bulunur. Üniversite örneğindeki grup yapısı, hiyerarşik olarak Şekil-2.2'de gösterildiği gibi ele alınabilir.



Şekil 2.2 Hiyerarşik ve Grupsal Kurum Yapısı

Grup içindeki hiyerarşik yapıya uygun olarak, değişik mevkilere sahip kişilerin erişmeleri gerekli olan bilgilerde de farklılıklar mevcuttur. Öyleki; alt kademede görev alan kişilerin yalnızca önem ve gizliliği düşük bilgilere erişmeleri yeterli iken, üst kademelere çıkıldıkça bu önem ve gizliliğin derecesi artar. Örneğin dekanların kendi fakülteleri ile ilgili tüm dökümanlara erişebilmeleri gereklidir. Oysa bu dökümanlar içinde bölüm başkanlarının erişmelerine gerek olmayan dökümanlar mevcut olabilir. Aynı ilişki akademisyenler ile idari personel için de geçerlidir. Bu durumda grup içinde dağıtımı yapılacak olan bilgilerin sınıflandırılması gereği ortaya çıkar. Bu sınıflandırma değişik kriterlere bağlı olarak yapılabilir. Bunlardan bazıları şunlardır:

- Bilgilerin gizliliği
- Bilgilerin önemi
- Kurumdaki kişilerin güvenilirliği
- Bilgilerin erişilme aciliyeti

Bu kriterler dikkate alınarak kurumda kullanılacak olan erişim seviyeleri oluşturulur. Bu işlem yapılırken herbir kriterin nispi olarak önemi de dikkkate alınr. Bu erişim

seviyelerinin adedi, kurumun iş dağılımı ile, çalışan personelin özel durumları da dikkate alınarak belirlenir. Öyleki bazı kurumlarda bir seviye yeterli olabilirken bazen daha fazla seviyelendirme gerekebilir. Hiyerarşik olarak en fazla bilgiye erişme hakkı *Seviye-1*'de olmak üzere tüm seviyeler numaralandırılır.

Erişim seviyeleri belirlendikten sonra, her bir kullanıcının erişim seviyesi belirlenir. Bu aşamadan itibaren her bir kullanıcının kurum içindeki hangi bilgilere erişme hakkına sahip olacağı hem bağlı olduğu grup ve hem de erişim seviyesi ile belirlenmiş olur.

2.1.3 Tanımlar

Mesaj Sahibi (*MS*) : Bir mesajı üreterek dağıtılmasını talep eden kişidir.

Mesaj Dağıtıcı (*MD*) : Mesajı *MS*'den alarak kurum içinde dağıtımını yapan merkezdir. Bu merkez aynı zamanda *grup Anahtarları* ile *Erişim Anahtarları* üretimini yapmak, gizliliğini sağlamak, yetkisiz kişilerin eline geçmesini önlemek ve erişim hakkına sahip olan birimlere dağıtmaktan da sorumludur.

Harici Mesaj : Diğer kurumlardan gelerek, kurum içinde ilgili kişilere dağıtımları yapılacak olan mesajlardır. Bu mesajlar öncelikle müdüre gelir. Müdür mesajın içeriğine göre hangi grup ve hangi erişim seviye yeterlik belgeli kişilere dağıtım yapılacağına karar verir ve kendi kontrolü altındaki *MD* marifeti ile kurum içinde dağıtımını yapar. Bu durumda *MS*, müdür'dür.

Dahili Mesaj : Kurum içindeki bir kişi tarafından kurum içindeki diğer kişilere dağıtılması talep edilen mesajlardır. Bu mesajların hangi grup ve hangi erişim seviyesindeki kişilere dağıtımının yapılacağına, mesajı üreten kişi (*MS*) karar verir ve mesajı *MD*'ye göndererek kurum içinde dağıtımını talep eder.

2.2 Matematiksel Temel

2.2.1 Küme teorisi

Küme, belirli bir özelliği taşıyan elemanlar topluluğudur. Bir küme, sözü edilen bu ortak özelliğin belirtildiği { : } sembolü ile tanıtılır. Küme elemanını sembolize eden bir değişken ":" işaretinden önce yazılır; Küme içindeki elemanların sahip oldukları ortak özellik ise ":" işaretinden sonra verilir.

Tablo 2.1 Küme Örnekleri

Küme tanımı	Tanımlanan elemanlar
$\{ x : x \in N \wedge x : tek\ sayı \}$	{ 1, 3, 5, 7, ... }
$\{ x^2 : x \in N \}$	{ 0, 1, 4, 9, 16, ... }
$\{ (-1)^x : x \in N \}$	{ -1, +1 }

Evrensel küme : Küme tanımında mevcut tüm elemanları içeren kümedir.
Boş küme : İçinde eleman bulunmayan kümedir ve { } ile gösterilir.
Kümenin uzunluğu : Küme içindeki elemanların sayısıdır ve |{ ... }| ile gösterilir.

2.2.2 Sayı teorisi

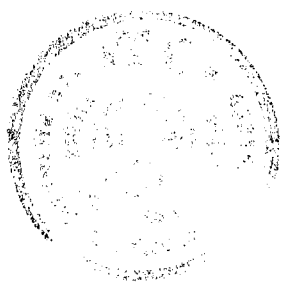
Bu çalışmada aksi söylenmedikçe ele alınacak tüm sayılar, N kümesine aittir.

2.2.2.1 Kalansız bölme

Verilen a ile n sayıları için $n = a * b$ eşitliğini sağlayan herhangi bir b sayısı mevcut ise a, n'yi kalansız bölüyor demektir; ve bu durum $a \mid n$ ile gösterilir. Bu durumda a'ya n'nin *böleni* denilir. Bu eşitliği sağlayacak herhangi bir b sayısı mevcut değil ise a, n'yi kalansız bölmüyor demektir; ve bu durum $a \dagger n$ ile belirtilir.

2.2.2.2 Ortak bölenlerin en büyüğü (Obeb)

Verilen a ve b sayılarının her ikisini de tam olarak bölen pozitif tamsayıların en büyüğüne *Ortak Bölenlerin En Büyüğü* denilir ve bu sayı $Obeb(a,b)$ ile gösterilir. Örnek olarak:
$Obeb(12, 3) = 4$



$Obeb(12, 4) = 3$

$Obeb(11, 3) = 1$

2.2.2.3 Denklik

Verilen a, b ve $n \neq 0$ sayıları için (a-b) değeri n tarafından kalansız bölünebiliyor, yani $n \mid (a - b)$ ise a ile b birbirine (n modülüne göre) denktir. Bu durumda n'ye modül (modulus) denilir. Denklik durumu, aşağıdaki ifadelerden herhangi birisi ile gösterilebilir.

- $a \equiv_n b$
- $b \equiv_n a$
- $a = b \ (mod\ n)$
- $b = a \ (mod\ n)$
- $a \equiv b \backslash n$
- $b \equiv a \backslash n$

2.2.2.4 Asal sayı, bileşik sayı

Bir $p > 1$ sayısı için; $[2..p\text{-}1]$ arasındaki hiçbir a sayısı p'yi kalansız bölemiyor, yani $a \dagger p \ \forall a \in [2..p\text{-}1]$ ise p'ye *Asal Sayı* denilir. Örneğin 11 asal bir sayıdır, çünkü [2..10] arasındaki tüm a sayıları için yukardaki eşitsizlik sağlanmaktadır. Çift sayı olan yegane asal sayı 2'dir; diğer asal sayıların hepsi tek sayıdır.

1'den büyük ve asal olmayan sayılara *Bileşik* (composite) *Sayı* denilir. Z^+ kümesinde olup ne asal ne de bileşik olmayan yegane sayı 1'dir.

- P, asal sayı kümesidir ve tüm asal sayıları içerir, yani $P = \{ 2, 3, 5, 7, .. \}$ olur.
- P_k bu listedeki k'ıncı ($k \geq 1$) asal sayıyı sembolize eder. Örneğin $P_1 = 2$, $P_2 = 3$ dür.
- Bu sayılar küçükten büyüğe sıralanmıştır: $(P_i < P_j) \Leftrightarrow (i < j)$

2.2.2.5 Bağıl asal sayı

Verilen $a > 0$ ve $n > 0$ sayıları için $Obeb(a, n) = 1$ ise; a ile n birbirine göre (bağıl olarak) asaldır. Örneğin:

- $Obeb(8,11) = 1$ olduğundan 8, 11'e göre asaldır.

Bir *a* sayısının *n*'ye göre asal olması için *a* ve *n* sayılarının asal olma zorunluluğu yoktur. Örneğin:

- *Obeb*(4,9) = 1 olduğundan (4 ve 9 sayıları asal olmadıkları halde) 4, 9'a göre asaldır.
- *Obeb*(6,13) = 1 olduğundan (6 sayısı asal olmadığı halde) 6, 13'e göre asaldır.

2.2.2.6 Aritmetiğin temel teoremi

1'den büyük her sayı, bir ya da daha fazla asal sayının çarpımı ile ifade edilebilir. Aşağıdaki şekilde gösterilebilen bu eşitliğe, *Kanonik Açılım* (Canonical factoring of n into prime powers) adı verilir:

$$n = p_1^{s_1} * p_2^{s_2} * \ldots * p_m^{s_m} = \prod_{i=1}^{m} p_i^{s_i} \qquad \forall p_i \in P \tag{2.1}$$

$(p_{i1} < p_{i2}) \Leftrightarrow (i_1 < i_2)$

Aritmetiğin temel teoremi (the fundamental theorem of arithmetic)

1'den büyük her sayı, sayıların kendi aralarındaki dizilişleri önemsiz olmak üzere ancak bir şekilde bölenlerine ayrılabilir.

bağıl asal sayı

Bağıl asal sayı tanımı daha önce yapılmıştı. Kanonik Açılım tanımı kullanılarak yeni bir tanım da yapılabilir: İki sayının Kanonik Açılımı içinde hiçbir ortak asal sayı yok ise, bu iki sayı birbirine göre asaldır.

obeb

Bu tanım da yeniden yapılabilir: İki sayının Kanonik Açılımı içinde yer alan ortak asal sayılar ile bunların ortak katlarının çarpımı, bu iki sayının *Obeb*'idir. Eğer ortak sayı yok ise, bu sayı 1'dir ve dolayısı ile bu iki sayı birbirine göre asaldır.

- $14 = 7 * 2$; $28 = 7 * 2^2$; *Obeb*(14,28) = $7 * 2 = 14$
- $49 = 7^2$; $420 = 7 * 5 * 3 * 2^2$; *Obeb*(49,420) = 7
- $6 = 3 * 2$; $11 = 11$; *Obeb*(6,11) = 1

2.2.2.7 Kalanlar kümesi

Bir $a \equiv_n b$ denkliğinde ($b \leq a$), b'ye *kalan* (residue) denilir. Belirli bir n sayısına bağlı olarak oluşturulabilecek tüm olası denkliklerdeki kalan'ların oluşturduğu $\{b_1..b_n\}$ kümesine ise *kalanlar kümesi* denilir. Bir n asal sayısı için kalanlar kümesi $\{0..n\text{-}1\}$ olur, yani $[0..n\text{-}1]$ arasındaki tüm tamsayılar bu kümeye dahildir.

2.2.2.8 İndirgenmiş kalanlar kümesi

İndirgenmiş Kalanlar Kümesi, kalanlar kümesindeki sayılar içinde n'ye göre asal olan sayıları içeren kümedir. Örneğin 12 sayısının kalanlar kümesi {0,1,2,3,4,5,6,7,8,9,10,11} iken, indirgenmiş kalanlar kümesi {1,5,7,11} olur; çünkü {0,2,3,4,6,8,9,10} 12'ye göre asal değildir.

2.2.2.9 Euler Totient fonksiyonu

Euler Totient Fonksiyonu, indirgenmiş kalanlar kümesi'nde bulunan sayıların adedidir ve $\phi(n)$ ile sembolize edilir. Verilen bir n sayısı için bu fonksiyonun değeri, n 'den küçük ve n'ye göre asal olan sayıların miktarına eşittir:

$\phi(n) = |\{ a : 1 \leq a < n \wedge Obeb(a,n) = 1 \}|$

Euler Totient Fonksiyonu değeri, aşağıdaki şekilde bulunur. Belirtilen tüm p değerleri asal sayıdır.

1. $n = p \Rightarrow \phi(n) = p\text{-}1$ (2.2)

2. $n = p_1 * p_2 * \ldots * p_m \Rightarrow \phi(n) = \phi(p_1) * \phi(p_2) * \ldots * \phi(p_m)$

$$= (p_1\text{-}1) * (p_2\text{-}1) * \ldots * (p_m\text{-}1) \quad (2.3)$$

3. $n = p^s \Rightarrow \phi(n) = n\left(1-\frac{1}{p}\right) = p^{s-1}(p-1)$ (2.4)

4. $n = p_1^{s_1} * p_2^{s_2} * \ldots * p_m^{s_m} \Rightarrow$

$$\phi(n) = n*\left[\left(1-\frac{1}{p_1}\right)*\left(1-\frac{1}{p_2}\right)*\ldots*\left(1-\frac{1}{p_m}\right)\right] \quad (2.5)$$

$$= p_1^{s_1-1}(p_1-1)p_2^{s_2-1}(p_2-1)\ldots p_m^{s_m-1}(p_m-1)$$

2.2.2.10 Bir sayının çarpma işlemine göre tersi (mod n)

Bir a sayısının çarpma işlemine göre tersi (b), a sayısı ile çarpımı sonucunda çarpma işlemine göre etkisiz eleman olan 1 değerini veren sayıdır. Genel sayısal işlemlerde $b = (1 / a)$ dır. a sayısının 1'den büyük tamsayı olduğu durumlarda b sayısı kesirli sayıdır. Oysa modüler aritmetikte bir tamsayının tersi (eğer mevcutsa) yine bir tamsayıdır.

Fermat'ın küçük teoremi

Bir p asal sayısına göre asal olan, yani $Obeb(a, p) = 1$ eşitliğini sağlayan, bir a sayısı için

- $a^{p-1} \equiv_p 1$ olur. (2.6)

Euler-Fermat teoremi

Euler, Fermat teoremini asal olmayan n sayılarına da uygulanacak şekilde genelleştirdiğinde ortaya Euler-Fermat teoremi çıkmıştır:

- $a^{\phi(n)} \equiv_n 1$ (2.7)

Verilen bir a sayısı için aşağıdaki eşitliği veren herhangi bir k sayısı mevcut ise, bu durumda b değeri a'nın n'ye göre tersi olur.

- $a * b = 1 + (k * n)$ $\quad a, k, n \in Z^+$ (2.8)

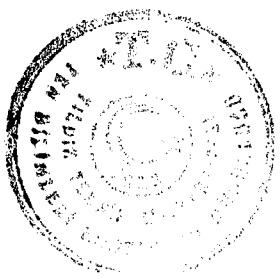
$k * n$ sayısı n modülüne göre 0 (sıfır) değerini verdiğine göre modüler işlem yapıldığında eşitlik aşağıdaki hale gelir:

- $a * b \equiv_n 1$ (2.9)

b, a sayısının tersi olduğuna göre b yerine a^{-1} de yazılabilir. Bu durumda denklem şu hale gelir:

- $a * a^{-1} \equiv_n 1$ (2.10)

Bu denklemi gerçekleyen a^{-1} değerinin varolması için a'nın n'ye göre asal olması gereklidir, yani $Obeb(a,n) = 1$ eşitliği sağlanmalıdır. Bu durumda a'nın tersi aşağıdaki şekilde bulunur:



Denklem-2.7 de her iki taraf a^{-1} ile çarpıldığında:

- $a^{\phi(n)} * a^{-1} \equiv_n a^{-1}$
- $a^{\phi(n)-1} \equiv_n a^{-1}$

Sol ve sağ taraf yer değiştirildiğinde, a'nın tersi olan a^{-1} bulunmuş olur:

- $a^{-1} \equiv_n a^{\phi(n)-1} = a^{\phi(n)-1} \ mod \ n$ (2.11)

n'nin asal olması özel durumunda ise denklem şu hale gelir:

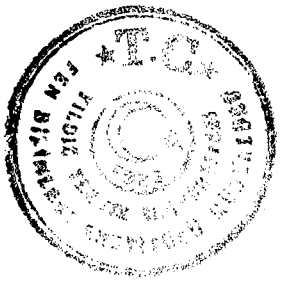
- $a^{-1} = a^{\phi(n)-1} \ mod \ n = a^{(n-1)-1} \ mod \ n = a^{(n-2)} \ mod \ n$ (2.12)

2.2.3 Karmaşıklık teorisi

Belirli bir problemi çözmek üzere tanımlanmış olan, sıfır ya da daha çok sayıda değeri girdi olarak alıp bir ya da daha çok sayıda değeri çıktı olarak üreten iyi tanımlanmış sıralı ve sonlu işlemler topluluğuna algoritma denir (Knuth, 1981). Bir algoritmanın şu özellikleri bulunmalıdır:

- Sonlu olma : Bir algoritma mutlaka belirli adımları icra ederek son bulmalıdır.
- İyi tanımlı olma : Algoritmanın her adımı iyi tanımlanmalıdır. Her durumda adımlarda yürütülecek işlemler belirsiz olmamalıdır.
- Girdi : Her algoritmanın sıfır ya da daha çok sayıda girdisi mevcuttur.
- Çıktı : Her algoritmanın bir ya da daha çok sayıda, girdilerle belirli bir ilişkisi olan çıktısı mevcuttur.
- Etkin : Bir algoritmanın etkin (verimli) olması beklenir. Bu, algoritmanın içerdiği tüm adımların yeterli derecede temel işlemler içermesi anlamındadır.

Bir algoritmanın ne kadar verimli olduğunu analiz etmek için, algoritmanın kullandığı, kaynakları tahmin etmek gereklidir. Bu kaynaklar arasında Bellek Kapasitesi, Depolama Kapasitesi, İletişim Band Genişliği vb. sayılabilir. Oysa genellikle ölçülmek istenen, Hesaplama zamanı olur, çünkü diğer kaynakların elde edilmesi daha kolay iken, zaman genellikle en değerli kaynak olur. Zaman maliyeti aşağıda incelenmektedir.



Bir algoritma, n uzunluğundaki her girdi için en fazla $f(n)$ adımda çalışıyor ise, bu algoritmanın zaman maliyeti (karmaşıklığı) $f(n)$ olur. Bir problemin çözümü için birden fazla algoritma geliştirilebileceğinden ve her algoritmanın zaman maliyeti diğerlerinden farklı olabileceğinden, genel olarak problemler yerine algoritmaların karmaşıklığından bahsedilir. Bir problemin çözümü için yazılan algoritmaların tümünde, örneğin bir minimum zaman ihtiyacı hesaplandığında ise bu değer artık, problemin karmaşıklığı olur.

Geleneksel karmaşıklık teorisi, genelde En Kötü (worst case) karmaşıklık analizi ile ilgilenir. Oysa şifreleme açısından algoritmaların ortalama (average case) karmaşıklığı önemlidir (Salomaa, 1990, Sayfa 58).

2.2.3.1 Karmaşıklık ölçüm fonksiyonları

Bir problemin çözümü için tasarlanan algoritmanın karmaşıklık hesap ölçümü, aşağıdaki fonksiyonlar ile yapılabilir. Burada yapılan anlatımlarda $g(x)$ problemi, $f(x)$ ise çözüm algoritmasını tanımlamaktadır (Wilf, 1992, Sayfa 8). Bu fonksiyonlar, hassasiyetleri ile ters orantılı olarak sıralanmışlardır. Öyleki içlerinde en az hassas sonucu $o(x)$, en fazla hassas sonucu ise $\sim(x)$ fonksiyonları verir.

Küçük o fonksiyonu(Little o)

x sonsuza yaklaştıkça $f(x)$ $g(x)$'den daha yavaş büyüyor ise, *Küçük o* fonksiyonu kullanılabilir.

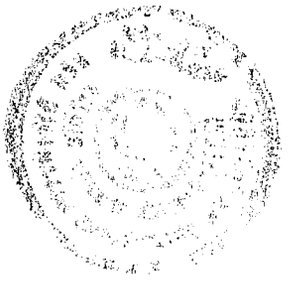
$f(x) = o(g(x)) \Leftarrow lim_{x\to\infty} (f(x) / g(x)) = 0$

Örnek : $x^2 = o(x^5)$

Omega fonksiyonu(Ω)

Ω fonksiyonu, *Küçük o* fonksiyonunun tersidir. Yani x sonsuza yaklaştıkça $f(x)$ $g(x)$'den daha yavaş büyümüyor ise, Ω fonksiyonu kullanılabilir. Bu durumda "$f(x)$, en azından $g(x)$ kadar büyüyor" anlaşılmalıdır.

$f(x) = \Omega(g(x)) \Leftarrow lim_{x\to\infty} (f(x) / g(x)) \neq 0$



$f(x)$ ve $\Omega(g(x))$ fonksiyonlarının Sıfır'dan büyük oldukları dikkate alındığında ise eşitsizlik şu duruma gelir:

$f(x) = \Omega(g(x)) \Leftarrow lim_{x\to\infty} (f(x) / g(x)) > 0$

Büyük O fonksiyonu(Big O)

x sonsuza yaklaştıkça $f(x)$ $g(x)$ kadar, ya da ondan daha yavaş (en fazla $g(x)$ kadar) büyüyor ise, *Büyük O* fonksiyonu kullanılabilir.

$f(x) = O(g(x)) \Leftarrow lim_{x\to\infty} (|f(x)| < c * g(x))$

Örnek : $Sin(x) = O(1)$

Teta fonksiyonu(Θ)

x sonsuza yaklaştıkça $f(x)$ $g(x)$'nin iki çarpan kadar katı arasında kalacak şekilde artıyor ise, Θ fonksiyonu kullanılabilir. $c_1 = 0$ olduğu taktirde *Büyük O* fonksiyonunun elde edileceğine dikkat edilebilir.

$f(x) = \Theta(g(x)) \Leftarrow lim_{x\to\infty} ((c_1 * g(x)) < |f(x)| < (c_2 * g(x)))$ $\qquad (c_1, c_2 \neq 0)$

Yaklaşır fonksiyonu(~)

x sonsuza yaklaştıkça $f(x)$ $g(x)$'e yaklaşıyor ise, ~ fonksiyonu kullanılabilir.

$f(x) = \sim(g(x)) \Leftarrow lim_{x\to\infty} (f(x) / g(x)) = 1$

Örnek : $(x^2 + x) = \sim(x^2)$

Örnek : $(x^2 + 1) = \sim(x^2)$

2.2.3.2 Turing makinası

Tanımda sözü edilen adım ölçümünün hangi model üzerinde yapıldığı çok önemlidir. Çünkü örneğin bir programlama dilinde $a = b + c$ işlemi tek bir komut ile yerine getiriliyor gibi görünse bile, bu işlem aslında kullanılan bilgisayarın özelliğine bağlı olarak birden çok işlemin icrasını gerektirebilir. Farklı dillerde varolan komut çeşitliliğini bir etken olmaktan çıkartıp standard oluşturmak amacı ile, algoritmaların karmaşıklığını ölçmek üzere Turing Makinası (*TM*) kullanılır (Salomaa, 1990, Sayfa 219). *TM*, sonsuz okuma-yazma belleği olan bir sonlu durum makinasıdır (FSM:Finite State Machine). *TM* teorik bir bilgisayar olduğu halde, hesaplamanın gerçekçi bir modelidir. Durumlar *D* ile, girdi-çıktısı yapılan

Bilgiler *B* ile ve **H**areketler de *H* ile markalansın. *D*, sabit adettedir. *H* ise {sola, sağa, durağan} olmak üzere üç ihtimallidir. *TM*, kesikli (discrete) zamanda çalışır. *TM* her safhada belirli bir durumda bulunur. Bir okuma-yazma kafası teyp üzerine yazılmış olan bilgileri her adımda bir adet olmak üzere okur. Belirli bir anda bir durumda olan *TM*, sıradaki *B*'yi okuyunca bir *H* hareketi yapar, dolayısı ile her (D_0, B_0) ikilisi *TM* için bir (D_1, B_1, *H*) üçlüsüne neden olur. S_0 durumunda iken B_0 bilgisini okuyan *TM*, S_1 durumuna geçer; B_0'nin üzerine B_1 yazar; ve okuma-yazma kafası *H* hareketini yapar. Eğer okuma-yazma kafası teybin sol ucuna gelmiş ve H_1 = *sola* ise ya da sağ ucuna gelmiş ve H_1 = *sağa* ise teyp kafasının bulunduğu yere bir boşluk eklenir. Yani *TM* okuma ve yazma kapasitesi açısından sonsuz kaynağa sahiptir.

TM çalışmaya belirli bir başlangıç durumunda ve girdiyi sol baştan itibaren okuyarak başlar. Herhangi bir sonuç durumuna erişildiğinde hesaplama sona erer. Bu taktirde *TM* durur ve teyp üzerinde yeralan bilgi, *TM*'nin çıktısı olur. Bu durumda TM_1 kullanılarak ölçülen zaman karmaşıklık fonksiyonu aşağıdaki şekilde tanımlanabilir:

$f_{TM1}(n) = max$ { *AdımAdedi* | $|w| = n$ olan w girdisi için TM_1 *AdımAdedi* adımda durur. }

Eğer her n için $f_{TM1}(n) \leq p(n)$ olan bir *polinom*:$p(n)$ mevcut ise bu durumda TM_1, polinom sınırlı olarak çalışır (Polinomially bounded). Polinom sınırlı bir *TM* tarafından çözülebilen problemler, *Polinom* problem olarak adlandırılırlar. Polinom sınırlı bir *TM* tarafından çözülemeyen problemler ise *Polinom Olmayan* (NP:Non-Polinomial) problem olarak adlandırılırlar.

Problemlerin ihtiyaç duyacakları zaman hesaplamaları, değişik örnek girdi uzunlukları için Tablo 2.2'de verilmiştir (Johnsonbaugh, 1993, Sayfa 163). Bir işlemin 10^{-6} saniye içinde icra edildiği varsayılmıştır.

Tablo 2.2 Problem Örnekleri

				n			
				10^2	10^3	10^5	10^6
sınıf	Polinom	sabit	O(1)	10^{-6} sn	10^{-6} sn	10^{-6} sn	10^{-6} sn
		logaritmik	O(log log n)	$2 * 10^{-6}$ sn	$3 * 10^{-6}$ sn	$4 * 10^{-6}$ sn	$4 * 10^{-6}$ sn
			O(log n)	$6 * 10^{-6}$ sn	10^{-5} sn	$2 * 10^{-5}$ sn	$2 * 10^{-5}$ sn
		doğrusal	O(n)	10^{-5} sn	10^{-3} sn	0.1 sn	1 sn
		quadratik	O(n log n)	$4 * 10^{-5}$ sn	10^{-2} sn	2 sn	20 sn
			$O(n^2)$	10^{-4} sn	1 sn	3 saat	12 gün
		kübik	$O(n^3)$	$2 * 10^{-3}$ sn	16.7 dk.	32 yıl	31,710 yıl
		üstel	$O(2^n)$	$4 * 10^{-3}$ sn	$3 * 10^{-287}$ sn	$3 * 10^{30089}$ sn	$3 * 10^{301016}$ yıl

2.2.3.3 NP problemler

Aşağıdaki tüm problemler, *NP* problemdir (*n* = girdinin bit olarak uzunluğu) ve bu problemlerin herbirinin çözümü için gerekli olan üstel zaman, şu şekildedir: (Denning, 1983, Sayfa 103) (Ayoub, 1984, Sayfa 688) (Davies, 1981).

$$Zaman = e^{\sqrt{\ln(n) * \ln(\ln(n))}}$$

çarpanlara ayırma (factoring a composite number)

Asal olmayan bir *n* sayısının asal çarpanlarını bulma işlemi, *çarpanlara ayırma* problemi olarak adlandırılır.

ayrık logaritma (discrete logarithm)

Verilen *a* ve *b* sayıları için $a^x \equiv_n b$ eşitliğini sağlayacak olan *x* sayısını bulma işlemi, *ayrık logaritma* problemi olarak adlandırılır.

kök alma (computing root)

Verilen *a* ve *b* sayıları için $x^a \equiv_n b$ eşitliğini sağlayacak olan *x* sayısını bulma işlemi, *kök alma* problemi olarak adlandırılır.

karekök alma (quadratic residue, computing square root)

Verilen a sayısı için $a \equiv_n x^2$ eşitliğini sağlayacak herhangi bir x değerinin varolup olmadığının bulunması işlemi, *quadratic residue* problemi olarak adlandırılır. Bu eşitlikte verilen bir a için x değerinin bulunmasını sağlayan algoritma, n değeri asal olduğu taktirde mevcuttur. Oysa asal olmayan n için quadratic residue problemi, çarpanlara ayırma problemi ile eşdeğerdir (Kranakis, 1986, Sayfa 110). Örneğin tek sayı olan bir asal n sayısı için x değeri Adleman-Manders-Miller teoremi ile bulunabilir (Kranakis, 1986, Sayfa 22).

2.2.4 Şifreleme sistemleri

2.2.4.1 Tanımlar

(Asıl) Mesaj : İki kişi ya da terminal arasında transferi amaçlanan bilgidir. Bu bilgi harf, rakam ya da başka karakterlerden oluşabilir. Her durumda bir dönüşüm (transfer) fonksiyonu kullanılarak bu bilgi bir sayıya dönüştürülebileceği için, mesajın tamsayılardan oluştuğu kabul edilebilir.

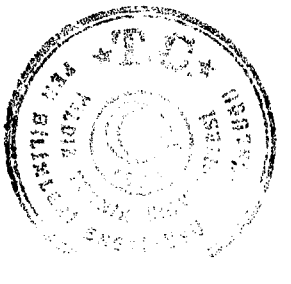
Şifrelenmiş Mesaj : Mesajın, şifreleme işlemi sonucunda elde edilen halidir.

Gönderici : Mesajı transfer eden kaynak kişi ya da terminaldir.

Alıcı : Mesajın gönderilmesi arzulanan hedef kişi ya da terminaldir.

Şifreleme : Alıcıya gönderilen mesajın içeriğini yetkisiz kişilerin anlamasını önlemek üzere, gönderici (alıcı ile önceden anlaşılmış bir şekilde) mesajın formatını değiştirir ve değişmiş olan formatı alıcıya gönderir. Göndericinin yaptığı mesaj formatını değiştirme işlemine *şifreleme* denilir.

Şifre Çözme : Alıcı, şifrelenmiş mesajı aldıktan sonra mesajın özgün halini elde etmek üzere format değiştirme işlemini tersten yapmak durumundadır, ki bu işleme *şifre çözme* denilir.



Protokol : Gönderici ile alıcının, şifreleme ve şifre çözme işlemleri esnasında daha önceden karşılıklı anlaşmaya varılmış bir şekilde uygulama durumunda oldukları sıralı işlemlerdir.

Anahtar : Protokol uygulanırken şifreleme ve şifre çözme işlemlerinin uygulanması aşamasında kullanılması gerekli olan değerdir. Bu değer olmadığı sürece protokol tek başına işlemlerin icrası için yeterli olmaz.

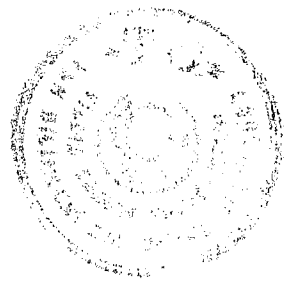
Şifreleme Anahtarı : Alıcıya mesajı şifreleyerek göndermek üzere kullanılması gerekli olan ve yalnızca şifreleme yetkisi olan kişilerin erişebilmesi gereken sayıdır.

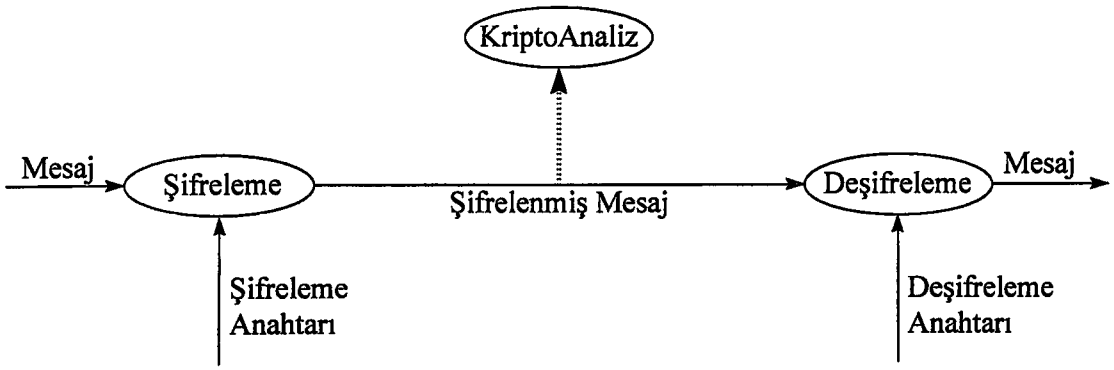
Şifre Çözme Anahtarı : Şifrelenmiş mesajı şifre çözmek üzere kullanılması gerekli olan ve yalnızca yetkili alıcıların erişebilmesi gereken sayıdır.

Şifre Kırıcı : Mesajın transfer edildiği ortamda varolan; ve bu ortamda transfer edilen her bilgiye transferin gerçekleştiği formda erişebildiği varsayılan; mesajın içeriğine erişme hakkı olmadığı halde, bu amaca yönelik bilimsel çalışmalar yapan kişi ya da terminaldir.

Şifre Kırma : Şifre kırıcı, mesaj üzerinde gerçekleştirilen şifreleme işleminin nasıl yapıldığını (ya da bu işlemi bildiği, fakat kullanılan şifre çözme anahtarını) bilmediği halde, mesajın özgün halini elde etmek üzere bazı metodlar uygular. Şifre kırıcıların yaptığı bu işleme *şifre kırma* denilir.

Şifreleme Sistemi : Şifreleme, şifre çözme ve şifre kırma işlemlerinin yapıldığı tüm sistemin ortak adına *şifreleme sistemi* denilir. Şifreleme sisteminin elemanları ve bu sistemde yapılan işlemler, Şekil 2.3'de gösterilmiştir.





Şekil 2.3 Şifre sistemi

(M, C, K, E, D) beşli ilişkisi (five-tuple) ele alındığında seçilen herbir $k \in K$ için bir $E_k \in E$ şifreleme ve buna karşılık gelen bir $D_k \in D$ şifre çözme kuralı mevcut olsun. Seçilen herbir $m \in M$ için $E_k : M \rightarrow C$ ile $D_k : C \rightarrow M$ fonksiyonları kullanımı $D_k(E_k(M)) = M$ eşitliğini sağlıyor ise, bu beşli ilişkisi bir şifre sistemi olur (Stinson, 1996). Tanımda kullanılan terimler, şunlardır:

M : mesaj sonlu kümesi

C : şifrelenmiş mesaj sonlu kümesi

E : şifreleme fonksiyonu

D : şifre çözme fonksiyonu

K : anahtar sonlu kümesi

2.2.4.2 Klasik (simetrik) şifre sistemleri

Şifreleme Sistemlerinin tarihte en fazla bilinen kullanımı *Sezar şifre sistemi*'dir. Bu metotda şifreleme yaparken mesaj içindeki herbir harf alfabedeki belli basamak sonraki harf ile değiştirilerek şifrelenmiş, şifre çözme yaparken ise ters işlem uygulanmıştır. Mesaj içerikleri [$A..Z$] harflerinden oluştuğundan dolayı, dönüşüm yapılarak [0..25] arasındaki sayılar dikkate alınmıştır. Herbir harfin şifreleme ve şifre çözme işleminde uygulanacak olan formüller şöyledir:

- şifreleme $C = E(M) = M + k \ (mod\ 26)$
- şifre çözme $M = D(C) = C - k \ (mod\ 26)$

Bu formüllerde kullanılan terimler, şunlardır:

- M : açık mesaj (message, text, plain text)

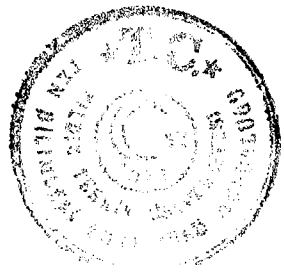
- C : şifrelenmiş mesaj (cryptotext, cypherText)
- E : şifreleme fonksiyonu (encryption function)
- D : şifre çözme fonksiyonu (decryption function)
- k : şifreleme ve şifre çözme işlemlerinin uygulanması sırasında kaydırılacak olan harf sayısı. k, aynı zamanda şifre sisteminin anahtarıdır (**key**). k bilindiği taktirde şifreleme ve şifre çözme işlemleri gerçekleştirilebilir, aksi taktirde işlemler yürütülemez.

Klasik şifrelemede bazen –Sezar şifre sistemi'nde olduğu gibi– şifreleme ve şifre çözme işlemlerinde aynı anahtar kullanılır, bazen de bu anahtarlar birbirinden farklı olabilir. İki ayrı anahtar kullanıldığında ise şifre çözme anahtarı kullanılarak kolay bir fonksiyon ya da metod yardımı ile şifreleme anahtarı elde edilebilir. Bu nedenle klasik şifreleme sisteminde şifreleme ve şifre çözme anahtar(lar)ı yalnızca yetkili kişiler tarafından bilinmelidir. Çünkü şifre kırıcı bu anahtarlardan herhangi birisini ele geçirdiği taktirde, sistemi kırmış sayılır.

Klasik şifreleme yönteminin uygulandığı bir sistemde iki gönderici {*gönderici*$_1$, *gönderici*$_2$} ile bir *alıcı*nın bulunduğunu; ve *gönderici*$_1$'in *alıcı*ya bir mesajı şifreleyerek gönderdiğini düşününüz. Bu durumda aslında yalnız *gönderici*$_1$ ile *alıcı*'nın mesajın içeriğini bilmesi hedeflendiği halde, *gönderici*$_2$ de sistemde kullanılan anahtar'ı bildiği için mesajın içeriğine ulaşabilecektir. Dolayısı ile klasik şifreleme yönteminin uygulandığı bir sistemde bulunan herkese aynı oranda güvenilme zorunluluğu vardır, ki bu da pek gerçekçi değildir.

2.2.4.3 Modern (asimetrik) şifre sistemleri

Modern şifreleme sistemlerinde ise kullanılan şifre çözme anahtarı'nın şifreleme anahtarı'ndan farklı olması nedeni ile klasik şifreleme sisteminden farklıdır. Şifreleme anahtarı kullanılarak yapılacak herhangi bir transfer işlemi ile de şifre çözme anahtarı elde edilemez. Bu durumda şifreleme anahtarının gizliliği yoktur. Ayrıca şifreleme anahtarı açık olarak herkese yayınlanabilir. Çünkü hiç kimse bu anahtarı kullanarak başka bir gönderici tarafından şifrelenmiş olan mesajı çözemez. Böylece sistemde olan herkese aynı oranda güvenme zorunluluğu da ortadan kalkar.



Modern şifreleme sisteminin basit bir örneği olmak üzere ad ve soyad sırasına göre düzenlenmiş bir telefon rehberi ele alınacaktır. Bu rehber kullanılarak ad ve soyadı bilinen bir kişinin telefon numarasını bulmak kolaydır; oysa bilinen bir telefon numarasına sahip kişinin ad ve soyadını bulmak zordur. İlk işlem için örneğin ikili arama (binary search) yeterli olduğu halde ikinci işlemde sıralı arama (sequential search) yapmak gerekecektir. Gönderici, alıcıya örneğin *GEZ* mesajını iletmek istediğinde yapacağı iş, herkesin kullanımına açık olan rehberi kullanarak {*G*, *E*, *Z*} harfleri ile başlayan üç rastgele ad seçmek, ve bu kişilerin telefon numaralarını alıcıya göndermektir. Örneğin Tablo 2-3'deki seçim bu işlem için uygundur.

Tablo 2.3 Rehber

Mesaj	Seçilen İsim	Şifrelenmiş Mesaj
G	Gül	3254535
E	Elif	5467655
Z	Zekiye	3527764

Bu durumda gönderici, alıcıya üç adet telefon numarasından oluşan şifrelenmiş mesajı gönderecektir. Şifre kırıcı; ad ve soyada göre sıralanmış olan rehberi kullanarak telefon numaralarının ait olduğu kişileri bulamaz, dolayısı ile eline geçen şifreli mesajı çözemez. Oysa elinde telefon numarasına göre sıralanmış olan ters telefon rehberi mevcut olan alıcı, kendisine gönderilmiş olan (üç adet) telefon numarasını bu rehberden kolayca bulup numaraların ait olduğu kişilerin adlarının baş harflerini biraraya getirerek özgün mesajı yeniden oluşturabilir.

Verilen tüm x'ler için $f(x)$ değerlerini hesaplamanın *kolay*, fakat verilen –neredeyse tüm– $f(x)$'ler için x değerini hesaplamanın *zor* olduğu fonksiyonlara *tek yönlü fonksiyon* denir (Ayoub, 1984, Sayfa 688). Örneğin bir x sayısının karesi olan $f(x) = x^2$ değerini hesaplamak kolay, fakat bir $f(x)$ değerinin karekökü olan x değerini hesaplamak zor bir işlem olduğundan kare alma işlemi tek yönlü bir fonksiyon olur. Günümüz teknolojisinde ise zorluk, pek çok bilgisayarın biraraya gelip milyonlarca yıl üzerinde çalışmaları gereken işlemlerle kıyaslanır. Biraz önce verilen örnekte ad ve soyadı bilinen kişinin numara sıralı rehberi kullanarak telefon numarasını bulmak kolay, oysa ad ve soyad sıralı rehberi

kullanarak telefon numarası bilinen kişinin adını bulmak zor olduğundan bu işlem bir tek-yönlü fonksiyondur.

Belirli bir ipucunun bilindiği durumlarda ters işlemi yapmak kolaylaşır, fakat bu ipucu bilinmediği taktirde bu işlem hala zor olarak kalır ise bu tür fonksiyonlara *açık kapılı (trapdoor) tek yönlü fonksiyon* denilir (Ayoub, 1984, Sayfa 688). Ters telefon rehberi kullanıldığında telefon numarası bilinen kişinin adını bulmak kolaylaştığından bu konuda örnek bir fonksiyon olur; çünkü ters telefon rehberi, normalde zor olan numara kullanarak ad ve soyad bulma işlemini kolaylaştıran bir ipucu olarak kullanılmaktadır.

2.2.4.4 Şifre sistemlerinin güvenliği

Sistemde transfer edilen (şifrelenmiş mesajlar dahil) tüm bilgilerin alıcıya olduğu kadar, şifre kırıcıya da ulaştığı varsayılır. Bu nedenle bir şifre sisteminin güvenli olması, şifre kırıcı'nın şifrelenmiş mesaj'dan özgün mesajı elde etmesinin güçlüğüne bağlıdır. Bu güçlüğün ölçülme derecesi, karmaşıklık teorisi konusunda anlatılmıştır.

Şifre kırma işlemi konusunda kabul edilmesi standard bir zorunluluk olan yerleşmiş bazı varsayımlar vardır. Bu varsayımlar şunlardır: (Schneier, 1996, Sayfa 5)

- **şifrelenmiş mesaj elde edilmiştir (ciphertext-only attack) :** Şifre kırıcı'nın, sistemde transfer edilmiş olan şifrelenmiş mesajları elde ettiği varsayılmaktadır. Bu durumda elde edilen şifrelenmiş mesajın uzun olması, şifre kırıcı için bir avantajdır. Sezar benzeri şifre sistemlerinde sistemin kırılması için kısa şifrelenmiş mesajlar da yeterli olabilir, çünkü tüm şifreleme işleminde bir tek anahtar kullanılmıştır ve bu anahtarın bulunması zor olmaz. Karmaşık sistemlerde ise daha uzun şifrelenmiş mesajlara ihtiyaç olur.

- **mesaj ve şifrelenmiş mesaj elde edilmiştir (known plaintext attack) :** Şifre kırıcı'nın mesajlar ile birlikte ilgili şifrelenmiş mesajları da elde ettiği varsayılmaktadır. (M, C) ikililerinin de yine uzun ve sayılarının da fazla oluşu şifre kırıcı için bir avantajdır. Sezar şifre sisteminde ise yalnızca bir karakter için elde edilen (M, C) ikilisi tüm şifre sistemini yıkmaya yeter.

- **seçilen mesajların şifrelenmiş mesajları elde edilmiştir(chosen plaintext attack):** Şifre kırıcı'nın, kendi seçtiği istediği sayıda mesaja karşılık gelen şifrelenmiş mesajları üretebileceği varsayılmaktadır. Bu durum, şifre kırıcı için bir önceki seçenekten daha iyidir. Bazı şifre sistemlerinde de oldukça gerçekçidir.

2.2.4.5 RSA algoritması

Göndericinin bir mesajı şifreleyerek göndermesini, alıcının ise şifrelenmiş mesajı çözerek mesaja ulaşmasını sağlayan bir algoritmadır. RSA, güvenliğini büyük sayıların asal çarpanlarını bulma probleminin zorluğuna dayandırır. Protokol, şu şekildedir:

1. Gönderici p ve q asal sayılarını seçer. n'yi hesaplar ve yayınlar.
   $n = p * q$

2. Gönderici, $Obeb(\ e,\ \phi(n)\ ) = 1$ olacak bir e seçer. d'yi hesaplar ve alıcıya güvenli bir yoldan gönderir.
   $d = e^{-1}\ mod\ \phi(n) = e^{\phi(n)-1}\ mod\ \phi(n)$

3. Gönderici, M mesajını şifreleyerek alıcıya gönderir.
   $C = M^e\ mod\ n$

4. Alıcı, şifrelenmiş mesaj'ı çözer.
   $C^d = (M^e)^d mod\ n = M^{e*d} mod\ n = M^{1+(k*\phi(n))}\ mod\ n = M\,(M^{\phi(n)})^k\ mod\ n = M(1)^k\ mod\ n = M$

2.2.4.6 El Gamal şifre sistemi

Gönderici ile alıcı arasında güvenli mesaj transferini mümkün kılan bir algoritmadır. Güvenliğini ayrık logaritma (discrete logarithm) hesabının zaman maliyetinin yüksekliğine dayandırır. Protokol, aşağıda verilmiş olup, kullanılan tüm hesaplamalar p modülüne göredir.

1. Gönderici; p asal ve $g < p$ sayılarını seçerek yayınlar.
2. Alıcı; $x < p$ sayısını seçer. y'yi hesaplar ve yayınlar.

   $y = g^x$
3. Gönderici; bir k seçer. a ile b'yi hesaplar ve yayınlar.

   $k < p$, $Obeb(k, \phi(p-1)) = 1$

   $a = g^k$

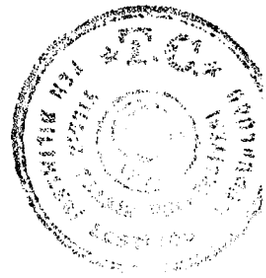
   $b = My^k$

4. Alıcı; $\{p, x, g, a, b\}$ yi bildiğinden dolayı M'yi hesaplar.

   $$M = \frac{b}{a^x}$$

   Gerçekten de:

   $$\frac{b}{a^x} = \frac{M y^k}{(g^k)^x} = M \frac{(g^x)^k}{(g^x)^k} = M$$



3. ÖNERİLEN MODEL

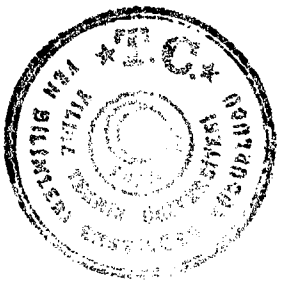
3.1 Önerilen Modelin Tanımı

Önerilen modelin amacı, grupsal hiyerarşik bir sistemde harici ve dahili mesajların güvenli bir şekilde dağıtımının yapılmasını sağlamaktır. Bu modelde harici mesajları müdür, dahili mesajları ise mesajı üreten kişi *MD*'ye göndermektedir. *MD*, dağıtılmak üzere almış olduğu mesajları yalnızca ilgili kullanıcıların erişimlerini mümkün kılacak şekilde şifreleyerek kurum içinde yayınlar. Yetkili kullanıcılar ise ellerine geçen şifrelenmiş mesajları, sahip oldukları anahtarları kullanarak çözerler ve böylece mesaj yetkili alıcılara ulaşmış olur.

Her mesaj, bir grup içindeki minimum erişim seviye yetki belgeli personelin okuması amacıyla hazırlanır. Bu nedenle *MD* bir mesajı aldığında belirtilen grup ve minimum erişim seviyesi kriterlerini gözönüne alarak yetkili kişilerin okuyabilmesi için iki kez şifreler:

- grup ile ilgili olarak
- minimum erişim seviyesi ile ilgili olarak

MD, iki şifrelemede iki ayrı şifreleme alt sistemi ve buna bağlı olarak iki ayrı anahtar kümesi kullanır. Bu anahtarlar, *MD* tarafından belirlenir ve kurum içinde yetkili kişilere mesaj dağıtımı yapmadan önce dağıtılır. Kurum içinde dağıtımı yapılan şifrelenmiş mesajlar ise yetkili kullanıcılar tarafından sahip oldukları grup ve erişim seviyesi anahtarları yardımı ile çözülerek okunabilir. Yetki verilmemiş bir grupta olan kişiler ise gerekli minimum erişim seviyesinde olsalar dahi, ilgili grup anahtarlarına sahip olmadıklarından dolayı hazırlanan şifrelenmiş mesaj'ı çözemezler. Mesajın hazırlanmasında hedef tutulan minimum erişim seviyesinde olmayanlar da yine yetki verilmiş grupta olsalar dahi, gerekli seviye anahtarlarına sahip olmadıklarından dolayı hazırlanan şifrelenmiş mesaj'ı çözemezler.



3.2 Önerilen Modelde Kullanılan Değerler

3.2.1 Genel işlem sayısı

Sistemde, tüm işlemlerdeki modüler aritmetik hesabında kullanılacak bir n sayısı vardır. Bu sayı, p ve q olmak üzere iki asal sayının çarpımına eşittir; yani $n = p * q$ dur. Bu amaçla öncelikle p ile q seçilir ve n değeri hesaplanır.

3.2.2 Hiyerarşik seviye anahtarları

Bu çalışma boyunca tasarlanan şifre sisteminde kabul edilen seviye adedi, $s \in Z^+$ ile sembolize edilecektir.

Erişim seviye durumunu ele almak üzere bir c sayısı yine *MD* tarafından belirlenir, ve bu sayının 1., 2., 4. ve 8. katları *Seviye-1* seviyeden başlayarak personele dağıtılır.

3.2.3 Grup anahtarları

Gruplara bilgi transferini sağlamak üzere her gruba bir grup anahtarı tahsis edilir ve bu anahtar g ile sembolize edilir. Böylece yetkili bir grubun okumasını sağlamak üzere o grup anahtarı ile şifrelenen mesajlar, ancak o grup personeli tarafından okunabilir.

Anahtarlar dağıtıldıktan sonra, mesajlar ilgili minimum seviye ve gruptaki personelin okuyabilmesini sağlayacak şekilde şifrelenir. Daha sonra bu şifrelenmiş mesaj kurum içinde yayınlanır. İlgili grup ve yetki seviyesinde olan kişiler, ellerindeki anahtarları kullanarak *şifrelenmiş mesaj*'ı çözer ve kendilerine ulaştırılması istenen bilgileri okur. Yetkisiz kimselerin bu işlemi yapmaları ise ellerinde grup anahtarı olmadığından engellenmiş olur.

Her mesaj ile birlikte o mesaja özel bir a değeri de belirlenerek protokolde tanımlandığı şekilde kullanılacaktır. Her mesaj için bir a değerinin kullanılmasının amacı, kullanılacak algoritmayı tek-yönlü bir fonksiyona dayandırmaktır. Her mesaj için "ayrı" bir a değeri kullanılmasının nedeni ise, bu güvenliği artırıcı etki yapmaktır. Ayrı bir a değeri

kullanılmasa idi, sahip olduğu uygun yetki belgeleri sonucu bir şifrelenmiş mesaj'ı çözerek burada kullanılan *a* değerini elde eden bir kişi, daha sonra erişeceği bir başka şifrelenmiş mesaj'ı çözme amacı ile aynı *a* değerini kullanabilecekti. Bu durumda ise *a* değerinin kullanılmasının sağladığı ek güvenliğin etkisi azalacaktı.

3.3 Değerlerin Özellikleri, Üretimi ve Dağıtımı

3.3.1 Genel işlem sayısını üretmek ve dağıtmak

MD p ile q asal sayılarını seçerek $n = p * q$ değerini hesaplar. p ile q değerlerini saklar, buna karşılık n'yi tüm kurum personeline dağıtır. Bu andan itibaren *MD* ile kullanıcılar tarafından yapılacak hesaplamalarda elde edilecek tüm değerler n'ye göre modülü alınarak kullanılır.

3.3.2 Hiyerarşik seviye anahtarlarını üretmek ve dağıtmak

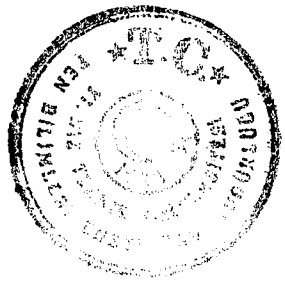
MD c sayısını seçer; $\{c^1, c^2, c^4, c^8 \ (mod\ n)\}$ değerlerini Tablo-3.1'de gösterildiği gibi ilgili erişim seviyesindeki kişilere dağıtır. *MD*, erişim seviyesi ile ilgili şifrelemeyi yapabilmek üzere bu sayıların tersleri olan $\{c^{-1}, c^{-2}, c^{-4}, c^{-8} \ (mod\ n)\}\ mod\ \phi(n)$ değerlerini hesaplar, ve bu değerleri kendisine saklar.

Tablo 3.1 Erişim Seviye Anahtarları

Erişim seviyesi	Şifreleme Anahtarı	Şifre Çözme Anahtarı
Seviye-1	c^{-1}	c^1
Seviye-2	c^{-2}	c^2
Seviye-3	c^{-4}	c^4
Seviye-4	c^{-8}	c^8

3.3.3 Grup anahtarlarını üretmek ve dağıtmak

MD herbir grup için ayrı bir $Obeb(g,n) = 1$ sağlayacak olan g'yi seçer, ve ilgili grup personeline güvenli bir yoldan dağıtır.



3.4 Anahtar Dağıtım Tablosu

MD tarafından yapılacak olan işlemler sonucunda ortaya çıkan anahtar dağıtım tablosu, Tablo-3.2'de gösterilmiştir. *P* personeli, tabloda sahip olduğu *erişim seviyesi* ve bağlı bulunduğu *grup* ile markalanmıştır. Örneğin P_{1A}, *A* grubunda bulunan *Seviye-1* erişim seviyesine sahip personeli tanımlar. Herbir *P* personeli, kendi satırında bulunan seviye şifre çözme anahtarı ile kendi sütununda bulunan grup anahtarını edinme hakkına sahiptir. *n* değeri açık olarak sistemde yayınlanacaktır. *a* değeri ise grupsal şifre çözme işlemini gerçekleştiren kullanıcının erişimine açık hale gelecektir. *p*, *q*, c^{-1}, c^{-2}, c^{-4}, c^{-8} değerleri yalnızca *MD* tarafından bilinecektir.

Tablo 3.2 Anahtar Dağıtım Tablosu

M D	p q	c^{-1} c^{-2} c^{-4} c^{-8}	A	B	
	n	c^1	P_{1A}	P_{1B}	Seviye-1
		c^2	P_{2A}	P_{2B}	Seviye-2
		c^4	P_{3A}	P_{3B}	Seviye-3
		c^8	P_{4A}	P_{4B}	Seviye-4
			g_A	g_B	
			a		

Kısaltmalar :

MD : Mesaj dağıtıcısı
A : A grubu
B : B grubu
g_A : A grubu anahtarı
g_B : B grubu anahtarı

3.5 Şifreleme ve Şifre Çözme

3.5.1 Şifreleme

Mesaj önce grup anahtarı, sonra da erişim seviyesi anahtarı ile şifrelenir.

1. Grup şifresi oluşturulur.

$C_{grup} = Egrup(M, g, a) = (Mg^{-a}, a)$

2. Grup_Erişim şifresi oluşturulur.

$C_{grup\_erişim} = Eerişim(C_{grup}) = \text{Eerişim}(Mg^{-a}, a) = (Mg^{-a}, a)^{e}$

3. Grup_Erişim şifresi kurum içinde dağıtılır.

3.5.2 Şifre Çözme

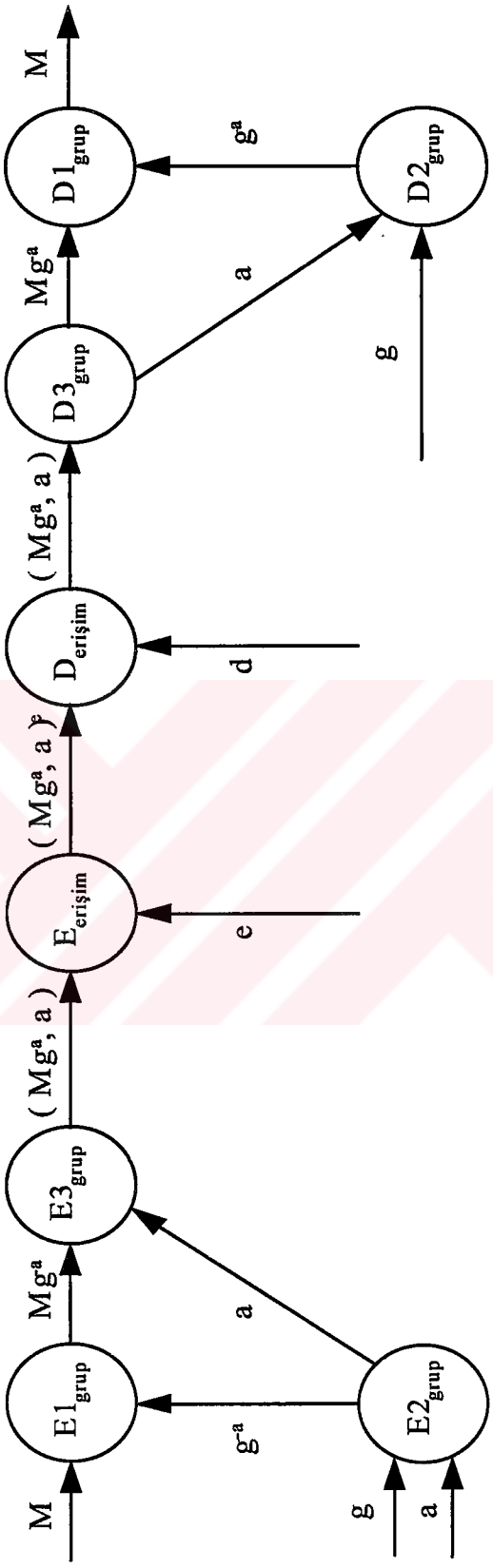
Şifreli mesajları elde eden yetkili kullanıcılar, bu mesajı önce sahip oldukları erişim seviyesi, sonra da grup anahtarı ile çözmelidir.

1. Grup şifresi ayrıştırılır.

$M_{grup} = Derişim(C_{grup\_erişim}) = Derişim((Mg^{-a}, a)^{e}) = ((Mg^{-a}, a)^{e})^{d} = (Mg^{-a}, a) = C_{grup}$

2. Mesaj ayrıştırılır.

$M_{grup\_erişim} = Dgrup(M_{grup}) = Dgrup(Mg^{-a}, a) = M$



Şekil 3.1 Şifreleme ve Şifre Çözme

3.6 Şifre Sisteminin Güvenliğini Sağlayan Etkenler

Tasarlanan şifre sisteminin güvenliği, temel olarak mesajların şifreleme ve şifre çözmesinde kullanılan algoritmaların NP problem oluşlarına dayanmaktadır. Buna ek olarak işlem yapılan n değerinin uzun oluşu da sistemin güvenliğini artırıcı önemli bir etken olarak ortaya çıkar.

3.6.1 Algoritmaların zorluğu

Şifre sistemi, iki ayrı şifreleme alt sisteminden oluşmaktadır. Bunlar *hiyerarşik* ve *grupsal* şifreleme alt sistemleridir.

3.6.1.1 Hiyerarşik şifreleme alt sistemi

Hiyerarşik şifre alt sistemi'nde temel: herbir seviyede bulunan kişilerin kendi seviyelerine adreslenmiş olan mesajları sahip oldukları seviye anahtarlarını; kendilerinden daha alt seviyeye adreslenmiş olan mesajları ise sahip oldukları anahtarlardan üretecekleri ilgili seviye anahtarlarını kullanarak çözmelerinin mümkün kılınmasıdır. Alt seviyenin şifre çözme anahtarını üretmek "kare alma" basit işlemi ile mümkün iken, üst seviye şifre çözme anahtarını üretmek ise Quadratic Residue problemi olduğundan NP zamana ihtiyaç gösterir.

Verilen c^m'yi kullanarak $(c^m)^2$ değerini hesaplamak kolay bir problemdir. Bu nedenle her kullanıcı, bulunduğu erişim seviyesinden daha alt erişim seviyelerinin anahtarlarını basit bir kare alma işlemi ile bulabilir. Oysa ters işlemi yapmak Quadratic Residue problemi olduğundan, zordur. Böylece hiç kimse sahip olduğu erişim seviyesinden daha üst seviye erişim seviyesi anahtarını elde edemez; bu nedenle de üst seviyelere adresli mesajları çözemez.

3.6.1.2 Grupsal şifreleme alt sistemi

Grupsal şifreleme alt sisteminde iki ayrı anahtar kullanılmaktadır. Bunlar grup anahtarı (g) ile, ipucu anahtarı (a) dır. Şifre kırıcı, sistemde açık olarak yayınlanan $(Mg^{-a}, a)^e$ bilgisine serbestçe erişebilir. Fakat d'yi bilmediğinden dolayı Mg^{-a} ya da a bilgilerine ulaşamaz. d'yi

bilen (seviye ayrımına göre yetkili, fakat grup ayrımına göre yetkisiz bir) kullanıcı ise (ki *şifre kırıcı* kabul edilir) *a*'yı elde edebilir. Ama *g*'yi bilmeden hiçbir şekilde Mg^{-a}'dan *M*'yi çekemez. Burada kullanılan, bir Ayrık Logaritma problemidir.

3.6.2 n değerinin uzunluğu

Şifre sisteminin tasarımında kullanılan *n* değerinin uzunluğu, Şifre kırıcı'nın sistemi kırmak amacı ile uygulayacağı muhtemel algoritmaların sonuca ulaşmasında etkili bir unsurdur. Bu çalışmada tasarlanan şifre sisteminde temel alınan problemlerin hepsi *NP* problem olduğuna göre, bu problemlerin polinom zamanda çözümü mümkün değildir. Yine de *n* sayısı küçük tutulduğunda polinom olmayan algoritmaların dahi makul süre içinde sonuca ulaşma şansı doğar. *n* değeri seçilirken gözönünde tutulması gerekli olan etkenler, şunlardır:

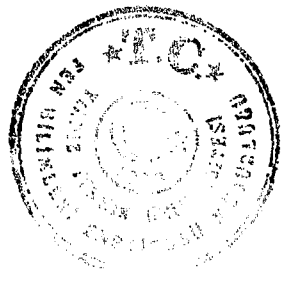
- Şifrelenecek bilginin değeri
- Bilginin gizli kalması gerekli olan süre
- Şifre kırıcı'nın hesaplama yeteneği

(Beth, 1992)'den alınan Tablo-3.3, değişik bilgi çeşitleri için günümüzdeki hesaplama gücüne bağlı olan gerekli gizlilik gereksinim tahminlerini içermektedir. Tabloda yer alan anahtar uzunluğu, *n* değerinin de uzunluğu ile direkt olarak ilişkilidir.

Tablo 3.3 Değişik Bilgiler için Gizlilik İhtiyacı

Bilgi Tipi	Gizli Kalma İhtiyacı	En Kısa Anahtar Uzunluğu
Taktik Askeri Bilgi	Dakika - Saat	56-64 bit
Gelecekteki Faiz Oranları	Gün - Hafta	64 bit
Uzun Vadeli İş Planları	Yıl	112 bit
Ticari Sırlar	10-20 Yıl	128 bit
Hidrojen Bombası Sırları	> 40 Yıl	128 bit
Ajan Kimlikleri	> 50 Yıl	128 bit
Diplomatik Sırlar	> 65 Yıl	≥ 128 bit

Bir problemin çözümü, kullanılan bilgisayarların hesaplama gücü ile direkt olarak ilgili olduğu için *n* değerinin uzunluğu, şifre sisteminin kullanıldığı zamandaki bilgisayar



süratlerine göre ayarlanmalıdır. Gelecekteki bilgisayarların hesaplama gücünü tahmin ederken, genel amaçlı bilgisayarlardaki güç artışı dışında özel amaçlı (örneğin asal çarpanlara ayırma problemini çözmek için tasarlanan) bilgisayar süratlerinin genel amaçlı olaranlara oranla daha hızlı bir artış gösterebileceği unutulmamalıdır.

3.6.3 *p* ile *q* değerlerinin özellikleri

RSA şifre sisteminde kullanılan, ve bu çalışmaya da ithal edilen algoritmada mevcut *p* ile *q* sayılarının seçimine özen gösterilmediği taktirde şifre kırıcının çözmek zorunda olduğu çarpanlara ayırma probleminin kolaylaştığını belirten halen yapılmış çalışmalar vardır. Şifre sisteminin bu açıdan güvenliğini artırmak üzere, aşağıdaki hususların sağlanması gereklidir (Denning, 1983, Sayfa 106). Bu çalışmada kullanılacak olan *p* ile *q* sayılarının belirlenmesi esnasında da belirtilen sınırlamalara bağlı kalınması, şifre sisteminin güvenliğini artıracaktır.

- *p* ile *q* sayılarının uzunlukları birbirine yakın olmalıdır.
- *p*-1 ile *q*-1 sayılarının çarpanları içinde büyük asal sayı mevcut olmalıdır.
- obeb(*p*-1, *q*-1) küçük bir sayı olmalıdır.

Bu çalışmada kullanılan *p* ile *q*'nun belirlenmesi aşamasında da aynı kriterlerin dikkate alınması sağlanmalıdır. Her durumda $M^e \bmod n = M$ eşitliğinin en az 9 mesaj için gerçekleşeceği yine (Blakley, 1978) ile (Blakley, 1979) de belirtilmiştir. Bu durumda mesaj saklanamamaktadır, çünkü şifre kırıcı burada modülü alınmamış bir sayının karekökünü almak durumundadır, ki bu problem polinom zamanda çözülebilir. Oysa *p* ile *q* sayılarının aşağıdaki eşitlik kullanılarak belirlenmesi, kullanılan sayıların 200 basamak ve üstünde olması şartı ile sistem daha dayanıklı olacaktır.

$p = 2p' + 1$, p' tek asal sayı.

3.7 Uygulama

Bir örnek olarak kurum içinde iki adet (*A* ve *B*) grup olduğu varsayılsın. Erişim seviyelerinin de dört adet (*Seviye-1*, *Seviye-2*, *Seviye-3*, *Seviye-4*) olduğu kabul edilsin. Bu durumda mesaj herbir grup-seviye ikilisi için ayrı olmak üzere $(2 * 4) = 8$ kez şifrelenecektir. Şimdi bir mesajın *MD* tarafından herbir birime hangi şifreli mesaj olarak

yansıyacağı ve yetkili kişilerin şifrelenmiş mesaj'dan mesajı nasıl elde edecekleri incelenecektir.

3.7.1 Anahtar Dağıtım Tablosunun Belirlenmesi

1. $p = 47$ ve

   $q = 53$ olarak seçilsin. Bu durumda:

   $n = p * q = 47 * 53 = 2491$, ve

   $\phi(n) = \phi(p*q) = \phi(p) * \phi(q) = (p - 1) * (q - 1) = 2392$ olur.

2. $g_A = 15$

   $g_B = 253$ olsun.

3. $a = 6$ seçilsin.

4. $c = 1243$ seçilsin. Bu durumda Tablo-3.4'deki değerler ortaya çıkacaktır.

   $d_1 = c^1 \bmod n = 1243$

   $d_2 = c^2 \bmod n = 1243^2 \bmod n \equiv_n 629$

   $d_3 = c^4 \bmod n = 1243^4 \bmod n \equiv_n 2063$

   $d_4 = c^8 \bmod n = 1243^8 \bmod n \equiv_n 1341$

   $e_1 = d_1^{-1} \bmod \phi(n) = (c^1 \bmod n)^{-1} \bmod \phi(n) = (c^1 \bmod n)^{\phi(\phi(n))-1} \bmod \phi(n) \equiv_{\phi(n)} 2163$

   $e_2 = d_2^{-1} \bmod \phi(n) = (c^2 \bmod n)^{-1} \bmod \phi(n) = (c^2 \bmod n)^{\phi(\phi(n))-1} \bmod \phi(n) \equiv_{\phi(n)} 1061$

   $e_3 = d_3^{-1} \bmod \phi(n) = (c^4 \bmod n)^{-1} \bmod \phi(n) = (c^4 \bmod n)^{\phi(\phi(n))-1} \bmod \phi(n) \equiv_{\phi(n)} 887$

   $e_4 = d_4^{-1} \bmod \phi(n) = (c^8 \bmod n)^{-1} \bmod \phi(n) = (c^8 \bmod n)^{\phi(\phi(n))-1} \bmod \phi(n) \equiv_{\phi(n)} 1229$

Tablo 3.4 Şifreleme ve Şifre Çözme Anahtarları

	ERİŞİM SEVİYELERİ			
	Seviye-1	Seviye-2	Seviye-3	Seviye-4
d_i	1243	629	2063	1341
e_i	2163	1061	887	1229

Bu durumda oluşacak olan anahtar dağıtım tablosu, Tablo-3.5'de gösterilmiştir.

Tablo 3.5 Anahtar Dağıtım Tablosu

p=47 q=53	$e_1 = 2163$ $e_2 = 1061$ $e_3 = 887$ $e_4 = 1229$	A	B	
n = 2491	$d_1 = 1243$ $d_2 = 629$ $d_3 = 2063$ $d_4 = 1341$	P_{1A} P_{2A} P_{3A} P_{4A}	P_{1B} P_{2B} P_{3B} P_{4B}	Seviye-1 Seviye-2 Seviye-3 Seviye-4
		$g_A=15$	$g_B=253$	
		a=6		

3.7.2 Şifreleme ve şifre çözme işlemleri

Mesaj = 101 için şifreleme ve şifre çözme işlemleri ise *A* ve *B* grupları için ayrı ayrı gösterilecektir:

- **A Grubu İşlemleri**

Şifreleme

1. Grup şifresi oluşturulur.

$g_A^a = 15^6 \equiv_n 1773$

$g_A^{-a} = 1773^{-1} \equiv_n 2321$

$C_{grup} = E_{grup}(M, g_A, a)$

$= (Mg_A^{-a}, a)$

$= (101*2321, 6)$

$\equiv_n (267, 6)$

2. Grup_Erişim şifresi oluşturulur.

$C_{grup\_erişim} = E_{erişim}(C_{grup}) = (Mg_A^{-a}, a)^e = (267, 6)^e$

Seviye-1 : $C_{grup\_erişim} = (267, 6)^{2163} \equiv_n (2194, 1416)$

Seviye-2 : $C_{grup\_erişim} = (267, 6)^{1061} \equiv_n (949, 1438)$

Seviye-3 : $C_{grup\_erişim} = (267, 6)^{887} \equiv_n (379, 269)$

Seviye-4 : $C_{grup\_erişim} = (267, 6)^{1229} \equiv_n (1144, 1898)$

3. Grup_Erişim şifresi kurum içinde dağıtılır.

Şifre Çözme

1. Grup şifresi ayrıştırılır.

$M_{grup} = D_{erişim}(C_{grup\_erişim}) = D_{erişim}((Mg_A^{-a}, a)^e) = ((Mg_A^{-a}, a)^e)^d$

Seviye-1 : $M_{grup} = (2194,1416)^{1243} \equiv_n (267,6)$

Seviye-2 : $M_{grup} = (949,1438)^{629} \equiv_n (267,6)$

Seviye-3 : $M_{grup} = (379,269)^{2063} \equiv_n (267,6)$

Seviye-4 : $M_{grup} = (1144,1898)^{1341} \equiv_n (267,6)$

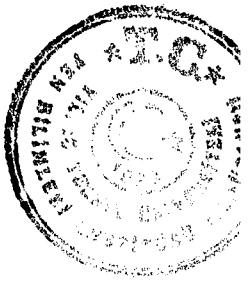
2. Mesaj ayrıştırılır.

$M_{grup\_erişim} = D_{grup}(M_{grup}) = D_{grup}(Mg_A^{-a}, a) = (Mg_A^{-a}, a)(g_A^a)$

$= 267 * 15^6 \equiv_n 101 = M$

Tablo 3.6 A Grubu İşlemleri

	ERİŞİM SEVİYELERİ			
	Seviye-1	Seviye-2	Seviye-3	Seviye-4
d_i	1243	629	2063	1341
e_i	2163	1061	887	1229
C_{grup}	$(101* 15^{-6}, 6) = (101 * 2321, 6) \equiv_n (267, 6)$			
$C_{grup\_erişim}$	$(267,6)^{2163} \equiv_n (2194,1416)$	$(267,6)^{1061} \equiv_n (949,1438)$	$(267,6)^{887} \equiv_n (379,269)$	$(267,6)^{1229} \equiv_n (1144,1898)$
M_{grup}	$(2194,1416)^{1243} \equiv_n (267,6)$	$(949,1438)^{629} \equiv_n (267,6)$	$(379,269)^{2063} \equiv_n (267,6)$	$(1144,1898)^{1341} \equiv_n (267,6)$
$M_{grup\_erişim}$	$267 * 15^6 \equiv_n 101$			



- **B Grubu İşlemleri**

Şifreleme

1. Grup şifresi oluşturulur.

$g_B^a = 253^6 \equiv_n 2084$

$g_B^{-a} = 2084^{-1} \equiv_n 661$

$C_{grup} = E_{grup}(M, g_B, a)$

$= (Mg_B^{-a}, a)$

$= (101*661, 6)$

$\equiv_n (1995, 6)$

2. Grup_Erişim şifresi oluşturulur.

$C_{grup\_erişim} = E_{erişim}(C_{grup}) = (Mg_B^{-a}, a)^e = (1995, 6)^e$

Seviye-1 : $C_{grup\_erişim} = (1995, 6)^{2163} \equiv_n (2324, 1416)$

Seviye-2 : $C_{grup\_erişim} = (1995, 6)^{1061} \equiv_n (1835, 1438)$

Seviye-3 : $C_{grup\_erişim} = (1995, 6)^{887} \equiv_n (2310, 269)$

Seviye-4 : $C_{grup\_erişim} = (1995, 6)^{1229} \equiv_n (27, 1898)$

3. Grup_Erişim şifresi kurum içinde dağıtılır.

Şifre Çözme

1. Grup şifresi ayrıştırılır.

$M_{grup} = D_{erişim}(C_{grup\_erişim}) = D_{erişim}((Mg_B^{-a}, a)^e) = ((Mg_B^{-a}, a)^e)^d$

Seviye-1 : $M_{grup} = (2324,1416)^{1243} \equiv_n (1995,6)$

Seviye-2 : $M_{grup} = (1835,1438)^{629} \equiv_n (1995,6)$

Seviye-3 : $M_{grup} = (2310,269)^{2063} \equiv_n (1995,6)$

Seviye-4 : $M_{grup} = (27,1898)^{1341} \equiv_n (1995,6)$

2. Mesaj ayrıştırılır.

$M_{grup\_erişim} = D_{grup}(M_{grup}) = D_{grup}(Mg_B^{-a}, a) = (Mg_B^{-a}, a)(g_B^a)$

$= 1995 * 253^6 \equiv_n 101 = M$

Tablo 3.7 B Grubu İşlemleri

	ERİŞİM SEVİYELERİ			
	Seviye-1	Seviye-2	Seviye-3	Seviye-4
d_i	1243	629	2063	1341
e_i	2163	1061	887	1229
C_{grup}	$(101* 253^{-6}, 6) = (101 * 661, 6) \equiv_n (1995, 6)$			
$C_{grup\_erişim}$	$(1995,6)^{2163} \equiv_n (2324,1416)$	$(1995,6)^{1061} \equiv_n (1835,1438)$	$(1995,6)^{887} \equiv_n (2310,269)$	$(1995,6)^{1229} \equiv_n (27,1898)$
M_{grup}	$(2324,1416)^{1243} \equiv_n (1995,6)$	$(1835,1438)^{629} \equiv_n (1995,6)$	$(2310,269)^{2063} \equiv_n (1995,6)$	$(27,1898)^{1341} \equiv_n (1995,6)$
$M_{grup\_erişim}$	$1995 * 253^6 \equiv_n 101$			

3.8 Büyük Sayılarla Uygulama

Bir önceki bölümdeki uygulama, daha büyük sayılar ile de tekrarlanmıştır. Bu aşamada 60-130 basamaklı p ile q sayıları kullanılmıştır. Bir seviyenin anahtarından daha alt seviyenin anahtarı üretilirken ise kare alma yerine bazı örneklerde 3. ve 5. üs değeri de hesaplanmıştır. Bu şekilde üretilmiş olan sistem sayıları Ek-F'de yer almaktadır. Bu tabloda yer alan örneklerin özellikleri, Tablo 3.8'de gösterilmiştir.

Tablo 3.8 Ek-F'de yer alan örneklerin özellikleri

Sıra No	Tablo	n uzunluğu (basamak)	Seviye	üs
1	Ek-F-1	130	10	5
2	Ek-F-2	130	11	2
3	Ek-F-3	170	10	2
4	Ek-F-4	210	11	2
5	Ek-F-5	210	11	3
6	Ek-F-6	210	11	2
7	Ek-F-7	210	12	3
8	Ek-F-8	210	14	2
9	Ek-F-9	210	15	3
10	Ek-F-10	230	10	2
11	Ek-F-11	230	11	2
12	Ek-F-12	250	11	2

3.9 Genel İşlem Sayısının Belirlenmesinde Uygulanabilecek Yöntem

Şifre sistemi tasarımında hiyerarşik seviye şifreleme anahtarlarının üretilmesi aşamasında $\phi(n)$'in asal çarpanlarına ayrılması, yani kanonik açılımının bulunması gerekmektedir. $\phi(n)$ değeri, n değerine göreceli olarak daha küçük bir sayıdır, kanonik açılımında n değerine nispeten daha çok asal sayı vardır, bu asal sayılar da p ile q değerlerinde olduğu gibi birbirlerine yakın olmayabilir; dolayısı ile kanonik açılımın bulunması, şifre kırıcının

önce p ile q değerlerinin belirlenmesi, oluşan $\phi(n)$ değerine bağlı olarak da $\phi(\phi(n))$ değerinin hesaplanması yerine: p ile q değerlerinin, belirlenecek asal sayıların çarpımı olarak oluşturulması, dolayısı ile $\phi(n)$ değerinin asal çarpanlarının önceden belirlenmiş olacağından hesaplanmasına gerek bırakılmaması sağlanabilir.

Bu amaçla öncelikle p değeri için aday sayı, Denklem-3.1 kullanılarak üretilecektir.

$p = 2p' + 1$, p' tek asal sayı. (3.1)

Daha sonra, üretilen bu sayının asal olup olmadığının kontrolü yapılacaktır. Bu işlem için halen polinom zamanda çalışan probabilistik testler mevcuttur (Lehman, 1982) (Miller, 1976) (Rabin, 1980): Bir n sayısının asal olup olmadığını kontrol etmek üzere $1 \leq b \leq n$-1 olmak üzere bir b sayısını rasgele seçerek, bu sayının n'i bölüp bölmediği araştırılır. Bölüyor ise n sayısı asal değildir, aksi halde bu konuda bir karara varılamamış olur. Bu şekilde 100 adet b sayısı ile test yenilendiğinde; asal olmayan bir n sayısının asal olmadığının anlaşılma olasılığı $1 - 2^{-100}$ olur, ki bu da oldukça yüksek ve tatmin edici bir orandır. Polinom zamanda çalışan pek çok probabilistik test mevcuttur (Wilf, 1992, Sayfa 149).

n değerinin asal olma durumunun kesin olarak belirlenmesi istendiğinde ise deterministik algoritmalar seçilmelidir, ki bu konuda da yapılmış pek çok çalışma mevcuttur (Adleman, 1983) (Cohen, 1987) (Cohen, 1988). Deterministik algoritmaların karmaşıklıkları aşağıda belirtildiği gibidir. Bu karmaşıklık değeri polinom olmasa da polinoma çok yakındır (Wilf, 1992, Sayfa 150).

$$O((Log(n)^{c*\log(\log(\log(n)))})$$

p ve q değerleri yukarıda tanımlandığı şekilde belirlendiği taktirde, n değeri şu şekilde oluşacaktır:

$p = 2p' + 1$

$q = 2q' + 1$

$n = p * q = (2p' + 1) * (2q' + 1)$

Artık $\phi(\phi(n))$ değerinin hesaplanması için çarpanlara ayırma probleminin çözülmesine gerek yoktur, p ile q değerlerinin hesaplanması esnasında $\phi(n)$'in kanonik açılımı zaten belirlenmiştir:

$\phi(n) = (p - 1) * (q - 1) = ((2 p' + 1) - 1) * ((2 q' + 1) - 1) = 4 p' * q' = 2^2 * p' * q'$

p ile q değerlerinin bu şekilde belirlenmesi durumunda artık şifre sistemi tasarımcısı işlemlerini polinom zamanda yapabilecek olup, bu durumda hızlı üretim ve çalışma ortamına sahip olacaktır.

p, q, n, $\phi(n)$ değerlerinin belirlenmesine örnek teşkil etmek üzere uygulamalar yapılmıştır. Bu amaçla ilk olarak hesaplamalarda kullanılan P asal sayılar kümesi geliştirilerek, $P_1..P_{1,000,000}$ asal sayılar kümesi oluşturulmuştur. Böylece oluşturulan asal sayılar alt kümesi, Ek-G'de yer almaktadır.

Bir sonraki aşamada; $P_2..P_{1,000,000}$ kümesindeki tüm asal sayılar, Denklem-3.1'deki eşitlikte p' olarak kullanıldığında elde edilen sayıların asal sayı olup olmadıkları kontrol edilmiştir. Örneğin $p_i = P_{200}$ olarak uygulandığında, aşağıdaki şekilde bir asal sayı elde edilmiştir:

$p = 2 * p_i + 1 = 2 * P_{200} + 1 = 2 * 1223 + 1 = 2447 \in P$

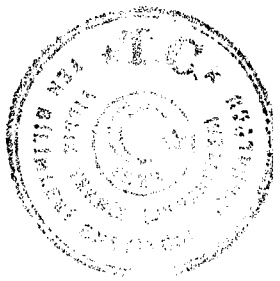
Oysa örneğin $p_i = P_{300}$ olarak uygulandığında, bir asal sayı elde edilememiştir:

$p = 2 * p_i + 1 = 2 * P_{300} + 1 = 2 * 1987 + 1 = 3975 \notin P$

$P_2..P_{1,000,000}$ kümesindeki asal sayılar Denklem-3.1'deki eşitlikte yerine konulduğunda elde edilen asal sayıların bir kısmına, Ek-I'da yer verilmiştir. Bu şekilde üretilen asal sayılar, az önce tanımlanmış olan kriterleri de sağladıkları taktirde, bu bölümde tanımlanmış olan algoritmada kullanılabilirler.

Ek-I'nın 82,211. ve 82,233. satırlarında yer alan değerler örnek olarak kullanıldığında, sistem sayıları şu şekilde belirlenmiş olur:

$p' = P_{999,556} = 15,478,349 \qquad p = 1+2p' = 30,956,699$



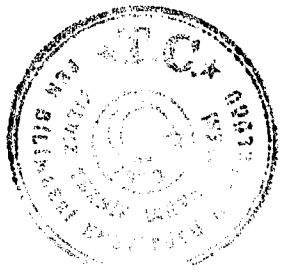
$q' = P_{999,959} = 15,485,339 \qquad q = 1+2q' = 30,970,679$

$n = p * q = 30,956,699 * 30,970,679 = 958,749,987,628,621$

$\phi(n) = 4\,p'q' = 4 * 15,478,349 * 15,485,339 = 958,749,925,701,244$

Bu yöntemin uygulaması, {10, 20, 30, 40, 50, 60} basamaklı p ile q sayıları, dolayısı ile {20, 40, 60, 80, 100 120} basamaklı n sayıları kullanılarak yinelenmiş ve elde edilen değerler Ek-G tablosunda verilmiştir. Sistem sayılarının burada tanımlandığı şekilde belirlenmesi, hem p ile q sayılarının belirlenmesinde dikkat edilmesi gereken şartları sağlamasını garanti etmektedir; hem de şifre tasarımcısı bu işlemi daha kısa sürede yapabilmektedir.

p ile q değerlerinin belirlenmesi aşamasında $\phi(n)$ değerinin asal çarpanlarının baştan bilinmesi gözetildiğinde, p ile q değerlerinin açık olarak bilinen bir yapıda olmasının, şifre kırıcıların işlerini kolaylaştıracağına da dikkat edilmelidir. Bu nedenle p ile q değerlerinin rasgele seçilmesi de bir başka seçenek olabilir. Bu durumda ise $\phi(n)$ değerinin asal çarpanlarının baştan bilinenemesi dezavantajı ile karşılaşılmaktadır. Uyum oranının hesaplanmasına gerek duyulmadığında ise bu yöntem yeterlidir.



4. HESAPLAMA VE ANALİZ

4.1 Tanımlar

4.1.1 Uygun sayı

Bir $c < n$ sayısının hiyerarşik seviye anahtarı olarak kullanılabilmesi için, bu sayının $\phi(n)$ değerine göre tersi olan c^{-1} mod $\phi(n)$ değerinin mevcut olması, bu amaçla da Denklem-4.1'de verilen eşitliği sağlaması gerekmektedir.

$$c * c^{-1} = 1 + (k * \phi(n)) \qquad c \in [2..n\text{-}2] \tag{4.1}$$

Bu eşitliği sağlayan bir c sayısı bulunduğunda, bu sayı 1. seviye için şifre çözme anahtarı olarak kullanılabilir, ki bu durumda $d_1 = c$ olacaktır. Sistemde mevcut 2. seviye için şifreleme anahtarı olarak kullanılacak d_2 anahtarı için ise $d_2 = c^2$ mod n olarak hesaplanacaktır. Bu sayının, 2. seviye şifre çözme anahtarı olarak kullanılması için Denklem-4.1'i sağlaması, yani obeb(d_2,$\phi(n)$)=1 olması gerekmektedir. Bu eşitlik sağlanmıyor ise $d_1 = c$ değeri de 1. seviye şifre çözme anahtarı olarak kullanılamayacaktır, çünkü 1. seviye'nin kullandığı şifre çözme anahtarının karesi hesaplandığında bu değer 2. seviye için şifre çözme anahtarı olarak kullanılamamaktadır. Bu ise tasarlanan şifre sisteminin sahip olması gereken temel özelliği ile çelişmektedir. Bu durumda yapılacak olan işlem, c sayısını değiştirerek başka bir c (dolayısı ile c^2) sayısının bu şartları sağladığı kontrol edilecektir.

Obeb(c,$\phi(n)$)=1 ve obeb(c^2 mod n, $\phi(n)$)=1 eşitliklerinin gerçekleşmesi ve sistemde 2 seviye mevcut olması durumunda bu sayı artık sistemde kullanılabilir bir sayı olmaktadır. Seviye adedinin 2'den daha fazla olması durumunda ise bu işlemin, c'nin diğer katları için de yinelenmesi, bu şekilde s seviye için üretilen { c^1, c^2 .. c^{s-1} } değerlerinin hepsinin obeb(d_i,$\phi(n)$)=1 şartını sağladığı kontrol edilmelidir. Bu şartların hepsini sağlayan bir c sayısı sistemde bu aşamada *kullanılabilir* olmaktadır.

Sistemde kullanılabilir sayıları bulmak amacı ile ilk aşamada [1..n] arasındaki tüm sayıların ele alınması düşünülebilir. Oysa [1..n] arasınaki sayıların bazı ek özellikleri de bu sayının

kullanımına etki etmektedir. Bunlardan ilki, c sayısının kendisi ya da ardışık olarak alınan kare değerleri içinde herhangi birisinin değerinin 1 olmaması gerektiğidir. Çünkü 1 sayısının karekökü zaten bellidir, ve bu da tasarlanan şifre sisteminin güvenliğini teşkil eden "bir seviyeden yukarıya gidilememe" kuralını bozar. Aksi taktirde elinde c'nin herhangi bir değeri olarak 1 olan kişi, artık hiyerarşide bir üst seviyenin şifre çözme anahtarı olan sayıyı da (bu durumda 1) elde etmiş olurdu.

Aynı nedenle n-1 sayısı da kullanılamaz, çünkü $(n\text{-}1)^2 \equiv_n (-1)^2 = 1$'dir ve 1 sayısı için öne sürülen gerekçe burada da geçerlidir. Bu iki nedenle verilen bir n sayısı için kullanılabilir sayı araması ilk aşamada [2..n-2] sayıları arasında gerçekleştirilir.

4.1.2 Güvenilir uygun sayı

$c^2 < n$ olduğu taktirde, şifre kırıcı c^2'nin karekökünü ayrık logaritma problemini çözmeden polinom algoritma kullanarak alabilir. Bu durumda "bir seviyeden yukarıya gidilememe" kuralı bozulmaktadır. Dolayısı ile kullanılabilir sayı araması $\left[\lceil n^{1/2} \rceil .. n\text{-}2\right]$ arasında yapılmalı, c'nin herhangi bir seviye için hesaplanan karesi n'den küçük olduğunda c sayısı sistemde kullanılamaz. Bu şekilde belirlenmiş olan sayıya, *güvenilir uygun sayı* denilir.

Sistemde kullanılabilir sayı bulunması amacı ile [2..n-2] arasındaki sayıların ele alınması ve gerekli şartı sağlayıp sağlamadıklarının araştırılması sırasında ele alınan c değerleri için $c^2 < n$ olma durumu ortalama olarak $(1 / n^{1/2})$ oranda meydana gelmektedir. n sayısının 200 bit civarında olduğu şifre sistemi tasarımında ise bu oran oldukça küçük bir değer olur. Dolayısı ile bu önşart, kullanılabilir sayı adedinin bulunmasında başarı oranını ancak ihmal edilebilir bir şekilde azaltabilmektedir.

Anlatılan şartların bir sonucu olmak üzere, bir $c \in \left[\lceil n^{1/2} \rceil .. n\text{-}2\right]$ sayısının kendisi ile, s-1 kez hesaplanan kare değerlerinin hepsi Denklem-4.1'deki eşitliği yani obeb(d_i,$\phi(n)$)=1 şartını sağlayan sayılar, *güvenilir uygun sayı* olurlar.

Bir örnek olmak üzere Ek-A tablo hazırlanmıştır. Bu tablo, (p=2*3+1=7, q=2*5+1=11, s=4) için yapılan uygun sayı hesaplamalarını içermektedir. Sistem sayıları kullanılarak üretilen diğer değerler ise şu şekildedir:

- $n = p * q = 7 * 11 = 77$
- $\phi(n) = (7 - 1) * (11 - 1) = 60$

Ek-A tabloda yer alan sayılar içinde {23, 67} uygun sayı olurlar. Az önce açıklandığı gibi bu sayıların herbirinin kendisi ile, üç kez (=s-1=4-1) alınan karelerinin hepsinin tersleri mevcuttur.

Tablonun hazırlanması aşamasında, $\left[\lceil n^{1/2} \rceil .. n-2\right]$ arasındaki herbir sayı c sayısı olarak ele alınıp ardışık karelerinin (dördüncü seviyeye kadar) terslerinin varlığı araştırılmıştır. Tersleri mevcut olan her c değeri ile bunun karesi, tersi ile birlikte tabloda gösterilmiştir. Örneğin $c = 7$ değeri için $\{c, c^2 \ (mod\ n)\}$ değerlerinin tersleri mevcut olduğundan bu değerler ile bunların tersleri tabloda gösterilmiştir. Buna karşın $\{c^4 \ (mod\ n)\}$ değeri ise, tersinin mevcut olmadığını belirtmek üzere tabloya konulmamıştır. $\{c^8 \ (mod\ n)\}$ değeri de, bu c değeri için hesaplama bir önceki aşamada sona erdiğinden, zaten hiç hesaplanmamıştır ve dolayısı ile de tabloda yoktur. Dikkat edilirse seviye adedi 3'e düşürülse idi, {19, 47} olmak üzere 2 daha yeni uygun sayı oluşacağı anlaşılmaktadır; ki bu durumda 4 uygun sayı mevcut olacaktı.

Uygun sayılar ile terslerini göstermek üzere bir başka örnek hazırlanarak Ek-B'de verilmiştir. Bu kez tabloda yalnızca uygun sayılar ile bunların her seviyedeki kareleri ve bunların terslerine yer verilmiştir. Bu tablodaki sistemde (p=47, q=53, s=4) parametreleri geçerlidir. Tabloda yer alan c sayıları ile bunların ardışık kareleri şifre çözme anahtarları olarak, sayıların tersleri ise *MD* tarafından şifreleme anahtarları olarak kullanılacaktır.

Bir uygun sayının hangi şifre sistemine ait olduğunu tanımlamak için, bu sayıların uygun sayı olmalarına etki eden parametrelerinin belirtilmesi gerekir; ki bunlar (p, q, s) üçlüsüdür. Bir c sayısının uygun sayı olması ancak ilgili üç parametrenin belirtilmesi ile anlam kazanır. Bir (p, q, s) üçlüsünün seçilmesi durumunda uygun sayı olan bir c sayısı, bu

değerlerden herhangi birisi değiştiğinde artık uygun sayı olmayabilir. Dolayısı ile uygun sayı gösterimi ancak bu üç değerin de belirtilmesi ile anlam kazanır. Bu nedenle uygun sayı, bu çalışmada $u(p, q, s)$ ile gösterilecektir. Örneğin Ek-A için aşağıdaki gösterim kullanılabilir. Bu gösterim (p=7, q=11, s=4) parametrelerinin geçerli olduğu bir şifre sisteminde {23, 67} sayılarının uygun sayı olduklarını ifade etmektedir.

- $u(p=7,q=11,s=4) = \{23, 67\}$

Eğer (p, q, s) değerleri her zaman bu sırada belirtilir ise, artık parametre isimlerinin açık olarak gösterilmesine gerek kalmaz. Bu nedenle örneğin aşağıdaki eşitlik, hiçbir kavram kargaşasına neden olmadan az önceki eşitlik yerine kullanılabilir. Burada p=7, q=11 ve s=4 olduğu anlaşılmaktadır.

- $u(7,11,4) = \{23,67\}$

4.1.3 Uyum adedi

Uyum adedi, uygun sayılar kümesi'nde bulunan elemanların adedidir:

- $U(p, q, s) = |u(p,q,s)|$ (4.2)

Bu formül Ek-A'daki şifre sistemine uygulandığında, aşağıdaki sonuç bulunur:

- $U(7,11,4) = |\{23,67\}| = 2$

Uyum adedi; (p, q, s) değerleri ile tanımlanan bir şifre sisteminde seçilebilecek c sayılarının adedini verdiğinden, şifre sistemi tasarımcısı için çok önemli bir değerdir. Çünkü bu değerin büyüklüğü; seçim alternatifinin fazlalığı anlamına gelir. p ve q değerleri arttıkça uyum adedinin artması, s değeri arttıkça ise uyum adedinin azalması beklenir. Böylece uyum adedinin p ve q değeri ile doğru orantılı, s değeri ile ise ters orantılı olması gerekir. Uyum adedinin s değeri ile ters orantılı olduğu kesindir; örneğin Ek-A tablo incelendiğinde $s = 4$ durumunda 2 adet uygun sayı mevcut iken s=3 olduğunda bu değer 4'e, s=2 olduğunda 8'e, s=1 olduğunda ise 18'e çıkmaktadır. p ve q değerlerinin artması ile birlikte ise uygun sayı aday adedi arttığından uyum adedi'nde artış beklenmesi doğaldır –ki bu beklenti de genellikle doğru çıkar– fakat bu durum s değerinin artışında ortaya çıktığı

şekilde kesin bir ters orantı durumu yaratmaz. p ve q sayıları ile sahip olması umulan doğru orantı, ilerde yapılacak analizlerde detaylı olarak incelenecektir.

4.1.4 Uyum oranı

Uyum oranı, *uyum adedi*'nin n'ye ondalık sayı olarak bölünüp 10,000 ile çarpılması ve en yakın tamsayıya yuvarlanması sonucu bulunan tamsayı değeridir ve bu değer, onbinde olarak oran ifade eder.

$$U_o(p,q,s) = \left[10{,}000 * \left(\frac{U(p,q,s)}{n} \right) \right] \tag{4.3}$$

Bu formül Ek-A'daki duruma uygulandığında, aşağıdaki değer bulunur:
$U_o(7,11,4) = [\ 10{,}000 * (\ 2 / 77\ )\ ] = 259$

Uyum oranı değerinin hesaplanmasına niçin gerek duyulmuştur? Az önce belirtildiği gibi uyum adedinin p ve q değerleri ile doğru orantılı olması beklenir. Bu beklenti genellikle de doğru çıkar. Ama bunun doğruluğu tek başına önemli değildir. Asıl önemli olan, uyum adedi'nde p ve q değerlerindeki artış miktarına orantılı bir artış sağlanmasıdır. Belirli (p,q,s) değerlerine karşılık olarak bulunan uyum adedi dikkate alındığında, p ve q değerlerinde meydana getirilecek olan artışın, uyum adedi'nde de benzer oranda bir artışa neden olması beklenir. Bu nedenle uyum adedi tanımlaması ile yetinilmemiş, uyum oranı tanımlaması da yapılmıştır.

Uyum oranı hesaplamasında elde edilen (*uyumadedi / n*) değerinin ondalık sayı olması bu değerin tablolarda gösterilmesi yanında grafik olarak çizimini de zorlaştıracağından; aksi durumda elde edilecek bir kazanç da olmayacağından; elde edilen bölüm değerinin 10,000 sayısı ile çarpılması (ölçeklenmesi) ve elde edilecek değerlerin en yakın tamsayıya yuvarlanması yolu seçilmiştir. Bu işlem için 10,000 sayısının seçilmesi ise, gösterim için kullanılacak kağıtların ölçüsü ile ilgilidir; kağıtlarda gösterilebilecek en optimal değerler bu şekilde elde edilmiştir. Daha küçük sayıların kullanılması, detaylandırma açısından kısıtlama getirecekti; daha büyük sayılar bu açıdan daha avantajlı olurdu; yine de yeterli derecede hassas değerler bu sayı kullanılarak da elde edilmiştir.

4.1.5 Uyum oranı ortalaması

Bu çalışmada şifre sistemi parametrelerinin seçiminde gözönünde tutulması gereken kriterlerin analizi işlemlerinde, öncelikle bir $[P_L..P_R]$ asal sayı listesi ele alınacaktır (L←Left, R←Right). Daha sonra liste içinden bir sayı p, listedeki sayıların herbiri sırası ile q olarak seçilip herbir (p, q) ikilisi için yeni bir uyum adedi ve uyum oranı değerleri hesaplanacaktır. Bir sonraki aşamada hesaplanacak olan P_k ($L \le k \le R$) sayısının *uyum oranı ortalaması*: P_k sayısının p, liste içindeki diğer tüm sayıların sırası ile q olarak seçilmesi durumunda ve önceden belirtilmiş olan seviye adedine göre hesaplanacak olan $|\{P_L..P_R\}| = R\text{-}L+1$ adet uyum oranı'nın aritmetik ortalaması olacaktır. Dolayısı ile bir P_k sayısı için bu değer aşağıdaki formül ile bulunabilir:

$$U_{oo}(P_k,[P_L..P_R],s) = \frac{\sum_{i=L}^{R} U_o(p_k,p_i,s)}{|\{P_L..P_R\}|} \tag{4.4}$$

Bu çalışmada yapılacak analiz hesaplamalarında iki ayrı grup asal sayı kullanılacaktır. Bu gruplardan ilki $P_{13}..P_{212}$ sayılarından oluşan 200 sayılık gruptur. Diğer grup ise 5000 sayılıktır ve $P_{13}..P_{5012}$ sayılarını içerir. Yapılan hesaplamalarda küçük olan asal sayıların çok uç (extreme) değerler verdikleri gözlenmiştir. Bu nedenle, çalışmada yapılacak uyum analizlerinde $P_1..P_{12}$ asal sayıları kullanılmayacaktır.

4.1.6 Uyum oranı ortalamalarının ortalaması

Uyum oranı ortalamalarının ortalaması, Bir P_k sayısı için $[P_L..P_R]$ sayılarının uyum oranı ortalaması değerlerinin aritmetik ortalamasıdır.

$$U_{ooo}(P_k,[P_L..P_R],s) = \frac{\sum_{i=L}^{k} U_{oo}(P_i,q \in [P_L..P_R],s)}{k} \tag{4.5}$$

Bu değer, p değerinin artışı ile birlikte birikimli (cumulative) olarak elde edilen uyum oranlarının ne şekilde değiştiğinin analizini yapmak üzere tanımlanmıştır.

4.1.7 Uyum sayıları

Uyum sayıları, aşağıdaki değerlerin ortak adıdır.

- *Uyum adedi*
- *Uyum oranı*
- *Uyum oranı ortalaması*
- *Uyum oranı ortalamalarının ortalaması*

4.1.8 Uyum analizi

Şifre sisteminin oluşturulmasında temel olan p, q ve s parametrelerinin doğru olarak seçimi, şifre sisteminin güvenliği açısından çok önemlidir. Şifre kırıcının işini zorlaştıracak parametrelerin seçilmesi, tasarımcının dikkat etmesi gereken önemli bir konudur. Parametrelerin herbirinin ayrı ayrı özelliklerinden başka, bunların birbirlerine göre uyumlu olmaları ve böylece yüksek uyum oranı değeri vermeleri de çok önemlidir.

Uyum sayılarının değerlendirilmesine yönelik analiz işlemi, *uyum analizi* olarak adlandırılmıştır. Hiyerarşik-grupsal şifre sistemi'nde üç ayrı parametre vardır: p, q ve s. Her üç parametre için ayrı ayrı olmak üzere üç ayrı uyum analizi yapılmıştır. Herbir parametrenin analizi, diğer iki parametrenin sabit bırakılması ve bu esnada sözkonusu parametrenin değiştirilmesi yolu ile bunun uyum sayılarına etkisinin araştırılması şeklinde olmuştur. Böylece yapılan analiz sonucunda elde edilen bulguların sistemin tasarımına yönelik olarak davranış belirlenmesine etkisi de her analiz sonucunda irdelenmiştir.

Şifre sisteminde uyum sayıları hesaplamaları için öncelikle bir s değeri seçilmektedir. Uyum hesaplamaları ile buna bağlı olarak yapılan analiz, şifre sisteminin diğer iki parametresi olan p ve q değerlerinin $\{P_L..P_R\}$ asal sayıları içinden seçilmesi sonucunda yapılmaktadır.

4.1.8.1 q parametre analizi

(p, s) değerleri sabit tutularak; q değerinin $[P_L..P_R]$ içinde P_L'den başlayarak P_R ye doğru sıra ile değiştirilmesi ile birlikte uyum oranı'nda meydana gelecek olan değişmelerin analizi, q parametresinin analiz edilmesi işlemidir. Bu analiz; bir p değerinin seçiminden sonra şifre sisteminin diğer bir parametresi olan q'nun, önceden belirlenmiş olan (p, s) ikilisi ile ilişkisi hakkında bilgi verecektir. Bu analiz ile; özellikle seçilecek olan q'nun,

seçilmiş olan p'ye göre bağıl olarak hangi özellikte olması gerektiği konusu açıklığa kavuşabilecektir. p ile q birbirleri yerine kullanılabilecek sayılar gibi göründükleri halde; q, analiz çalışmalarında (p, s) ikilisinin sabit olması halinde $P_L..P_R$ arasında değiştirilerek sonucun analiz edileceği son parametre olarak kullanılacaktır.

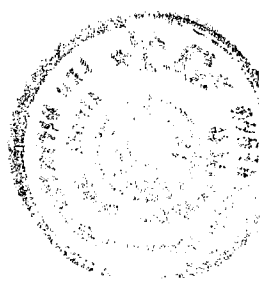
4.1.8.2 p parametre analizi

s değerinin sabit tutulması, q değerinin ise $[P_L..P_R]$ içinde P_L'den başlayarak P_R ye doğru sıra ile değiştirilmesi ile elde edilen uyum ortalamalarının, p değerinin değişmesi ile birlikte uyum oranı ortalaması'nda meydana getirdiği değişikliğin analizi, p parametresinin analiz edilmesi işlemidir. Bu analizde p, s'den sonra belirlenecek olan ikinci parametre olarak kullanılacaktır. Bu analiz, $[P_L..P_R]$ içindeki sayıların hangilerinin ilk etapta seçimi ile yüksek uyum oranı elde etme olanağının oluşacağını gösterir.

4.1.8.3 s parametre analizi

$U_0(p,q,s)$ değeri farklı seviyeler sözkonusu olduğunda doğal olarak değişmektedir. Peki bu değişimin seviye artışı ile ilişkisi ne şekildedir? Bu bölümde, seviye artışına bağlı olarak gerçekleşen uyum oranı'ndaki değer değişikliği analiz edilecek, ve bu soruya cevap aranacaktır. Eğer seviye değişikliği ile uyum oranı arasında somut bir ilişki (orantı) kurulabilirse, bu durumda $s = 1$ için birazdan tanımlanacak olan algoritma kullanılarak kısa süre içinde uyum oranı değeri bulunarak seçilen sayıların $s = 1$ için olumlu olduğu kontrol edilecek, böyle olması durumunda $s > 1$ durumu içinde aynı durumun geçerli olduğu kabul edilebilecektir.

s parametresinin analizi, tasarlanacak olan şifre sisteminin bu temel parametresinin belirlenmesinde göz önünde tutulacak olan kriterlerin de belirlenmesine katkıda bulunacaktır. Böylece hiyerarşik seviye adedinin optimal olarak belirlenmesine ilişkin girdiler elde edileceği umulmaktadır.

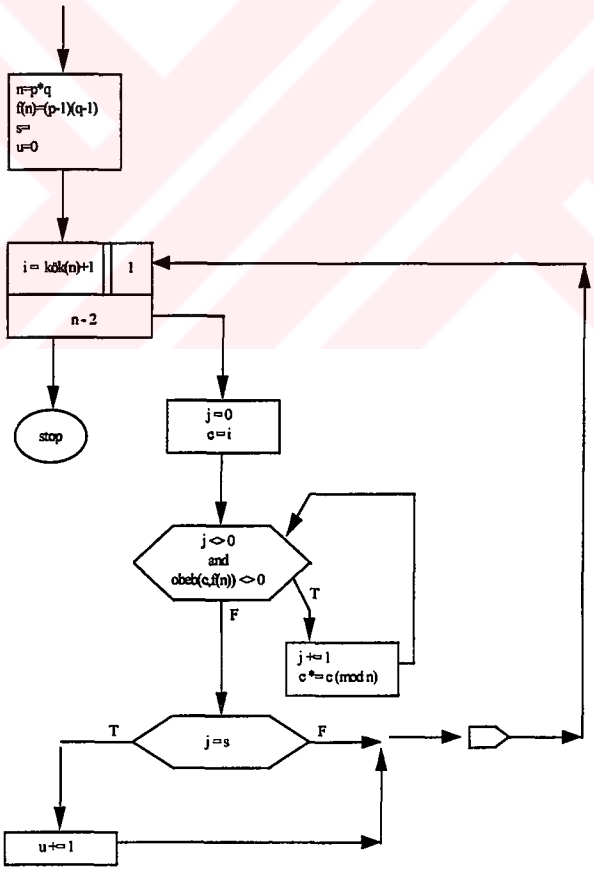


4.2 Uygun sayı bulma (USB) algoritması

Tasarlanmakta olan şifre sisteminin seçilen (p, q, s) parametrelerine bağlı olarak uygun sayılar, Şekil-4.1'de verilen algoritma kullanılarak bulunabilir. Bu algoritma tüm uygun sayıları bulduğu için bunların toplamları uyum adedini de verir.

```
p = ?
q = ?
n = p * q
s = ?
fi_of_n = ( p - 1 ) * ( q - 1 )
u = 0
for i = 2 to n-2 do
begin
   j = 0
   c = I
   while ( j <> s ) and ( obeb( c, fi_of_n ) <> 1 ) do
   begin
      j += 1
      c *= c mod n
   end
   if ( j = s ) then
      u += 1
end
```

Şekil 4.1 Uygun Sayı Bulma Algoritması



Şekil 4.2 Uygun Sayı Bulma Algoritması'nın Akış Diyagramı

Ek-A tablo kullanılarak yapılan hesaplamalarda bu yöntem kullanılmıştır. Bu amaçla $c \in [\lceil n^{1/2} \rceil .. n\text{-}2]$ arasındaki tüm c sayıları Denklem-4.1'deki eşitliği sağlama açısından bir döngü içinde test edilir; sağlayanlar uyum adedini bir artırır; tüm sayılar test edildiğinde de uyum adedi değeri bulunmuş olur. $s = 1$ olduğu durumda yalnızca [2..n-2] sayıları için birer kontrol yapılır ve eşitliği sağlayanların adedi, uyum adedini verir. $s > 1$ olduğu durumda ise, eşitliği sağlayan c sayılarının s-1 kez ardışık kare ($mod\ n$) değerleri de eşitliği sağlama açısından test edilir ve bunların ancak hepsinde eşitliği sağlayan c sayılarının adedi uyum adedi değerini verir.

4.3 Uyum Adedinin Hesaplanması

4.3.1 Uyum adedini bulma (UAB) algoritması

Az önce anlatılan algoritma, seçilen p, q, s değerlerine bağlı olarak mümkün tüm uygun sayıları bulduğu için bunların adedi de uyum oranını verecektir. Oysa yüksek bir uyum oranı olmasını isteyen bir şifre sistemi tasarımcısının, bu durumda bütün sayıların uygun olup olmadığını kontrol etmesi gerekmektedir, ki bu katlanılamayacak bir zaman maliyetini ortaya çıkarmaktadır. Bu durumda uyum adedinin hesaplanması için yeni bir yöntem belirlenmelidir.

n değerinin kanonik açılımı, aşağıdaki şekildedir:

$n = r_1^{s1} * r_2^{s2} * .. * r_m^{sm}$

Tasarlanan şifre sistemi ele alındığında $\phi(n)$ değerinin kanonik açılımı aşağıdaki şekilde olsun.

$n = r_1^{s_1} * r_2^{s_2} * \ldots * r_m^{s_m}$

Bu durumda $\phi(n)$ değeri aşağıda yeniden ifade edilen Denklem-2.5 kullanılarak bulunabilir.

$$\phi(n) = n * \left[\left(1 - \frac{1}{r_1}\right) * \left(1 - \frac{1}{r_2}\right) * \ldots * \left(1 - \frac{1}{r_m}\right) \right]$$

Tasarlanan şifre sistemi ele alındığında, $\phi(n)$ değerinin kanonik açılımı aşağıdaki şekilde olsun.

$$\phi(n) = r_1^{s_1} * r_2^{s_2} * \ldots * r_m^{s_m}$$

Bu durumda $\phi(n)$ değerinin indirgenmiş kalanlar kümesi, Denklem-2.5 kullanılarak aşağıdaki şekilde bulunabilir.

$$\phi(\phi(n)) = \phi(n) * \left[\left(1-\frac{1}{r_1}\right) * \left(1-\frac{1}{r_2}\right) * \ldots * \left(1-\frac{1}{r_m}\right)\right]$$

Bu eşitlik 1 seviye için [1..$\phi(n)$] arasındaki uygun c değerlerinin adedini verecektir. Oysa uyum adedini bulmak üzere, [1..n-1] arasındaki tüm uygun c değerlerinin adedi gerekmektedir. Bu nedenle birazdan tanımlanacak olan *UAB algoritması* kullanılacaktır. Bu amaçla öncelikle konu ile ilgili iki teorem verilecektir.

Teorem-4.1 : Seçilen asal p ve q sayılarının çarpımına eşit n sayısının Euler-Totient fonksiyonu olan $\phi(n)$ değerinin kanonik açılımı içinde yer alan herbir (asal) sayının kendileri ile bunların $\phi(n)$'den küçük-eşit tamsayı katları'nın $\phi(n)$ ile Ortak Bölenlerinin En Büyüğü değeri 1'den büyüktür.

$$Obeb(k * r, \phi(n)) > 1 \quad \Leftarrow \quad p, q \in P$$

$$\phi(n) = (p-1) * (q-1) = r_1^{s1} * r_2^{s2} * \ldots * r_m^{sm}$$

$$(k*r_i \le \phi(n) \Leftarrow (k \in Z^+) \wedge (r_i \mid \phi(n)) \wedge (1 \le i \le m) \wedge (r_i \in P)$$

İspat : İki bölümde yapılacaktır.

1. $k = 1$ olsun. Bu durumda $Obeb(r_i, \phi(n)) > 1$ önerilmiş olur.
   - [2..r-1] arasındaki bir sayı hem r'yi hem de $\phi(n)$'i bölse bile; r bu sayıdan daha büyük olduğundan, r'den küçük bir sayı *Obeb* değeri olamaz.
   - *Obeb* değeri r'den büyük bir sayı da olmayacağından, $Obeb(r,\phi(n)) = r > 1$ olduğu ortaya çıkar.
2. $k > 1$ olsun. Bu durumda $Obeb(k * r, \phi(n)) > 1$ önerilmiş olur. İki durum söz konusudur.
   - $k*r \mid \phi(n) \Rightarrow Obeb(k*r, \phi(n)) = k*r$

(birinci bölümdeki yargılama kullanılarak)

- $k^*r \nmid \phi(n) \Rightarrow r \mid \phi(n)$ olduğundan $Obeb(k^*r, \phi(n)) \geq r$. Çünkü $r \mid \phi(n)$ iken r'den küçük bir sayı Obeb değeri olamaz.

Teorem-4.2 :

Bu teorem, üç ayrı şekilde tanımlanabilir. İspat ise, yalnızca üçüncü tanım için yapılacaktır. İlk tanım, diğer tanımlardan daha geniş kapsamlıdır, fakat çalışmada bu geniş tanıma gerek olmayacaktır. İkinci ve üçüncü tanım ise kapsam olarak eştir.

1. Bir $x < \phi(n)$ sayısı ile $\phi(n)$'in *Obeb* değerlerinin 1'den büyük olması için x'in ya $\phi(n)$'in asal çarpanı, ya da $\phi(n)$'in asal çarpanlarından en az birisinin integer katı olması gerekir. Bu, $Obeb(x, \phi(n))>1$ için gerek ve yeter şarttır.
   $Obeb(x, \phi(n)) > 1 \Leftrightarrow ((x \in P) \Lambda (x \mid \phi(n))) \vee ((x \notin P) \Lambda ((x \mid r) \exists r \mid \phi(n)))$
2. Teorem-4.1'de belirtilen sayılar dışında kalan ve $[2..\phi(n)-2]$ içindeki tüm sayılar ile $\phi(n)$'in *Obeb* değerleri 1'e eşittir.
3. $\phi(n)$'in asal çarpanı ya da asal çarpanlarından en az birinin katı da olmayan tüm sayıların $\phi(n)$ ile *Obeb* değerleri 1'e eşittir.
   $Obeb(x, \phi(n)) = 1 \Leftarrow ((x \in P) \Lambda (x \nmid \phi(n))) \vee ((x \notin P) \Lambda ((r \nmid x) \forall r \mid \phi(n))) \quad x \in Z^+$

İspat : Aksi olsa idi, yani $Obeb(x,\phi(n)) > 1$ olsa idi:

- $(x \in P) \Rightarrow x$'in $[2..x-1]$ aralığında böleni olmayacağından, $Obeb(x, \phi(n))$ ancak x ya da 1'e eşit olabilir. $x \nmid \phi(n)$ verildiğinden $Obeb(x, \phi(n))=1$ olur.
- $(x \notin P) \Rightarrow x$'in; $\phi(n)$'in Kanonik Açılımı içinde yer alan hiçbir sayının katı olmadığı, buna karşın $Obeb(x, \phi(n)) > 1$ olduğu farzedildiğinde; x asal olmadığına göre x'in Kanonik Açılımı içinde bulunan (asal) sayılar, $\phi(n)$'in Kanonik Açılımı içinde yer almamaktadır. Tanımdan hatırlanacağı gibi; *Obeb*, iki sayının kanonik açılımları içinde yer alan ortak sayıların çarpımına eşittir. Bu durumda iki kanonik açılım içinde ortak sayı olmadığından, *Obeb* değeri 1'e eşittir.

UAB algoritması:

1. -1 ve $(n-1)$ değerlerinin uygun sayı olarak kabul edilmeyeceği, *uygun sayı* tanımında belirtilmişti. Dolayısı ile *uyum adedi* değeri başlangıç olarak eğer $\phi(n)$'in kanonik

açılımında yer alan herhangi bir asal çarpan *n*'yi bölüyor ise *n*-1-⌊√n⌋'e, aksi durumda *n*-2-⌊√n⌋'e eşitlenir.

2. $\phi(n)$'in Kanonik Açılımı içinde yer alan herbir r_k için (n div r_k) kadar $\phi(n)$ ile bağıl olarak asal olmayan sayı vardır; dolayısı ile bunlar *uyum adedi* değeri'nden çıkartılır.
3. Oysa iki r_k değerinin birden katı olan değerler, *uyum adedi* değeri'nden ikişer kez çıkartılmıştır. Dolayısı ile bunların birer adedi yeniden *uyum adedi* değeri'ne eklenmelidir.
4. Bu kez de üç r_k'nın çarpımı olan değerler ikişer kez çıkarılmış olmaktadır. Dolayısı ile bunların birer adedi yeniden *uyum adedi* değeri'ne eklenmelidir.
5. Madde 3 ile 4, asal çarpanların adedi kadar tekrarlanır ve her adımda oluşturulan çarpım değeri içine bir r_k daha eklenir.
6. Aynı işlem n yerine ⌊√n⌋ değeri kullanılarak yinelenir ve elde edilen sonuç, madde 5'te elde edilen sonuca eklenir.

Örnek-4.1 : Şimdi *UAB algoritması* bir örnek üzerinde uygulanacaktır.

$p = 7$

$q = 11$

$n = p * q = 7 * 11 = 77$

$\phi(n) = (p - 1) * (q - 1) = (7 - 1) * (11 - 1) = 60 = 2^2 * 3 * 5$

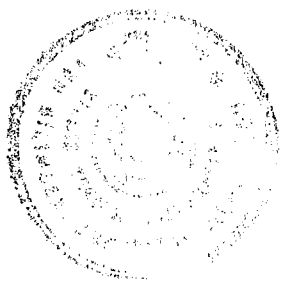
Teorem-4.2 gözönüne alındığında, aşağıdaki eşitsizlikler gerçekleşir:

$Obeb(k*2, \phi(n)) \neq 1 \ (\forall k \mid k*2 \leq n)$

$Obeb(k*3, \phi(n)) \neq 1 \ (\forall k \mid k*3 \leq n)$

$Obeb(k*5, \phi(n)) \neq 1 \ (\forall k \mid k*5 \leq n)$

Bu eşitsizlikleri sağlayan, dolayısı ile $\phi(n)$'e göre asal olmayan sayılar Tablo-4.1'de verilmiştir. Bu tabloda $\phi(n)$'in asal çarpanları olan { 2, 3, 5 } sayılarının katı olan ve $\phi(n)$'e göre asal olmayan her sayı, ilgili asal çarpanın satırında yer almaktadır. Tabloda görüldüğü (ve matematiksel olarak çok açık olduğu) üzere $\phi(n)$'in asal çarpanı olan (aynı zamanda $Obeb(k*r_i, \phi(n)) \neq 1$ eşitsizliğini sağlayan) bir r_i sayısının $\phi(n)$'den küçük integer katları adedi, $(\phi(n) \ div \ r_i)$ dir.



Tablo 4.1 $\phi(77)$'ye Göre Asal Olmayan Sayılar

r_i	$Obeb(k * r_i, \phi(n)) \neq 1$ olan sayılar
2	2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48 50 52 54 56 58 60 62 64 66 68 70 72 74 76
3	3 6 9 12 15 18 21 24 27 30 33 36 39 42 45 48 51 54 57 60 63 66 69 72 75
5	5 10 15 20 25 30 35 40 45 50 55 60 65 70 75

Tablo-4.1 içinde yer alan bazı sayılar iki ayrı asal çarpanın katı olarak görülmektedir. Bu sayılar, Tablo-4.2'de verilmiştir. Dikkat edilirse ele alınan r_i ve r_j değerlerinin her ikisinin katları olan sayılar, $k * (r_i * r_j) \leq n$ eşitliğini sağlayan sayılardır. Bunların adedi ise matematiksel olarak açık bir şekilde $n\ div\ (r_i * r_j)$ dir.

Tablo 4.2 İki ayrı bölenin birden katı olan Sayılar

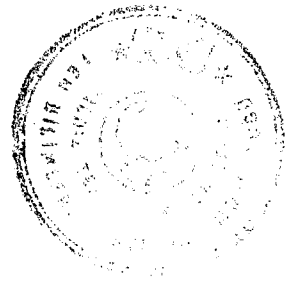
r_i	r_j	$Obeb(k * r_i * r_j, \phi(n)) \neq 1$ olan sayılar
2	3	6 12 18 24 30 36 42 48 54 60 66 72
3	5	15 30 45 60 75

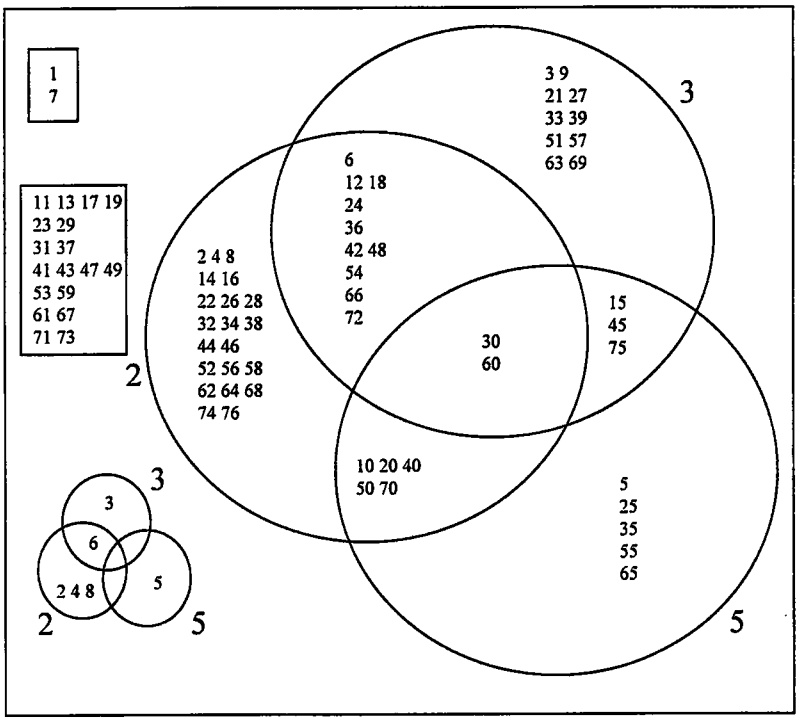
Yine Tablo-4.1'de yer alan bazı sayılar ise $\phi(n)$'in asal böleni olan her üç sayının katı olarak üç satırda da yer almıştır. Bu sayılar Tablo-4.3'de gösterilmiştir. Bu sayıların adedi ise $n\ div\ (r_i * r_j * r_k)$ dır.

Tablo 4.3 Üç ayrı bölenin birden katı olan sayılar

r_i	r_j	r_k	$Obeb(k * r_i * r_j * r_k, \phi(n)) \neq 1$ olan sayılar
2	3	5	30 60

Tablolarla gösterilen bu ilişkiler, küme gösterimi ile Şekil-4.3'de yeralmaktadır.





Şekil 4.3 $\phi(n)$'e Göre Asal Olan ve Olmayan Sayılar

Tüm bu irdelemelerden sonra *UAB algoritması* kullanılarak uyum adedi aşağıda anlatıldığı ve örneklendiği şekilde bulunacaktır.

Uyum adedi için önce *n* sayısı temel olarak alınacaktır.

adayuyumadedi = $n-1-\lfloor\sqrt{n}\rfloor = 68$

Bu sayılar içinden 1 ile çıkartılacaktır. Eğer n değerini, n'in asal çarpanlarından hiçbiri tam olarak bölmüyor ise, bu durumda n-1 gözönüne alınarak 2 çıkartılmalıdır.

adayuyumadedi = n-1-8 = 68

Bu sayılar içinden r_1, r_2, r_3'ün katları olan sayılar çıkartıldığında:

adayuyumadedi = $n-1-\lfloor\sqrt{n}\rfloor - ((n \text{ div } r_1) + (n \text{ div } r_2) + (n \text{ div } r_3))$

$= 68 - ((77 \text{ div } 2) + (77 \text{ div } 3) + (77 \text{ div } 5))$

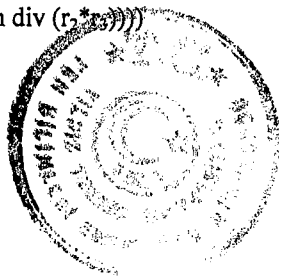
$= 68 - (38 + 25 + 15)$

$= -10$

Şimdi bu değere, ikişer kez çıkarılan ve Tablo-4.3'de yer alan sayıların adedi bir kez eklenecektir. Bu durumda:

adayuyumadedi = $n-1-\lfloor\sqrt{n}\rfloor - ((n \text{ div } r_1)+(n \text{ div } r_2)+(n \text{ div } r_3))+((n \text{ div } (r_1*r_2))+(n \text{ div } (r_1*r_3))+(n \text{ div } (r_2*r_3)))$

$= 68 - ((77 \text{ div } 2) + (77 \text{ div } 3) + (77 \text{ div } 5))$



$$+ ((77 \text{ div } (2*3))+ (77 \text{ div } (2*5))+ (77 \text{ div } (3*5)))$$
$$= 68 - (38 + 25 + 15) + (12 + 7 + 5)$$
$$= 14$$

Bu durumda da Tablo-4.3'de yer alan ve her üç bölenin integer katı olan sayılar ikişer kez eklenmiş olmaktadır. Sorunun çözümü, bu sayıların adedini bir kez daha adayuyumadedi'nden çıkarmaktır:

$$\text{adayuyumadedi} = n-1-\lfloor\sqrt{n}\rfloor - ((n \text{ div } r_1)+(n \text{ div } r_2)+(n \text{ div } r_3))$$
$$+((n \text{ div } (r_1*r_2))+(n \text{ div } (r_1*r_3))+(n \text{ div } (r_2*r_3))))$$
$$- (n \text{ div } (r_1*r_2*r_3))$$
$$= 76 - (38 + 25 + 15) + (12 + 7 + 5) - (2)$$
$$= 12$$

Aynı işlem $\lfloor\sqrt{n}\rfloor$ için tekrarlandığında r_1 = 2'nin (2,4,6,8), r_2 = 3'ün (6), r_3 = 5'in (5), r_1*r_2= 2*3'ün (6) değerlerini bölmeleri nedeni ile sonuca (4+1+1-1)=6 eklenmesi neticesinde uyumadedi = 12 + 6 = 18 olarak bulunur.

Bu safhada bulunan adayuyumadedi, uyumadedinin aranan değeridir. Bu çalışmadan görüleceği gibi içleme-dışlama algoritması $\phi(n)$'in asal böleni olan r_i'lerin adedi kadar safha hitamında s = 1 için uyum adedini vermektedir.

4.3.2 Yukarıya doğru tanımlanmış sistemde uyum adedinin hesaplanması

p ile q sayılarının daha önce tanımlanmış yöntem kullanılarak belirlenmesi durumunda n değeri şu şekilde oluşmaktadır:

$$p = 2p' + 1$$
$$q = 2q' + 1$$
$$n = p * q = (2p' + 1) * (2q' + 1)$$
$$\phi(n) = (p - 1) * (q - 1) = ((2p' + 1) - 1) * ((2q' + 1) - 1) = 4p' * q' = 2^2 * p' * q'$$

$$\phi(\phi(n)) = \phi(n) * \left[\left(1-\frac{1}{2}\right) * \left(1-\frac{1}{p'}\right) * \left(1-\frac{1}{q'}\right)\right]$$
$$= 4p'q'\left(\frac{1}{2}\right)\left(\frac{p'-1}{p'}\right)\left(\frac{q'-1}{q'}\right)$$
$$= 2(p'-1)(q'-1)$$

Bu durumda uyum adedinin bulunması kolaylaşacaktır:

$$
\begin{aligned}
u = n-1-\lfloor\sqrt{n}\rfloor-[(n\ div\ 2)+(n\ div\ p')+(n\ div\ q')] \\
+[(n\ div\ 2p')+(n\ div\ 2q')+(n\ div\ p'q')] \\
-[n\ div\ 2p'q'] \\
+\left[\left(\lfloor\sqrt{n}\rfloor div\ 2\right)+\left(\lfloor\sqrt{n}\rfloor div\ p'\right)+\left(\lfloor\sqrt{n}\rfloor div\ q'\right)\right] \\
-\left[\left(\lfloor\sqrt{n}\rfloor div\ 2p'\right)\right]
\end{aligned}
\qquad (4.2)
$$

$p' < q'$ olarak düşünülmüştür. Bu denklem, genel algoritmada kullanılan örnek üzerinde uygulandığında:

$u = 77 - 1 - 8 - (38 + 25 + 15)$
$+ (12 + 7 + 5)$
$- (2)$
$+ (4 + 2 + 1)$
$- (1)$
$= 18$

Uygulamada elde edilen sonucun genel algoritmadaki değer ile aynı olduğu görülmektedir.

4.3.3 Algoritmaların birlikte kullanılması

USB algoritması, seçilen p ve q sayılarına bağlı olarak bir c sayısının verilen herhangi bir seviyedeki ($s \geq 1$) sistem için uygun sayı olup olmadığını bulmada kullanılır. Tüm $c \in [2..n\text{-}2]$ sayılarının bu algoritma kullanılarak uygun sayı olup olmadığı test edildiğinde de *uyum adedi* elde edilmiş olur. *UAB algoritması* ise herhangi bir c sayısının uygun sayı olup olmadığını test etmede kullanılamaz, buna karşılık $U(p,q,s)$ değerinin hangi sayıların uygun sayı oldukları araştırılmaksızın hesaplanmasında kullanılabilir. *UAB algoritması* kullanılarak bulunan $U(p,q,s)$ değerini veren uygun sayıların hangi sayılar olduğu ise ancak *USB algoritması* kullanılarak bulunabilir. Dolayısı ile *UAB algoritması*, yalnızca $s = 1$ durumunu ele alıp uyum adedini bulması nedeni ile, $s \geq 1$ durumunu ele alıp uygun sayıları da bulan *USB algoritması*na oranla daha yeteneksizdir.

4.4 $\{P_{13}..P_{212}\}$ için uyum sayıları hesabı

Bu bölümde, $\{P_{13}..P_{212}\}$ asal sayı grubuna ilişkin yapılan hesaplamalar sonucunda oluşturulmuş tablo ve grafiklerin içerikleri ele alınmıştır. Bu tablo ile grafikler, çalışmanın eklerinde yer almaktadır. Yapılan hesaplamalar anlatılırken bu hesaplamalarda üretilen değerlerin hangi eklerde yer aldıkları da belirtilecektir. Herbir tablo, yapılacak analiz işlemini kolaylaştırmak amacı ile ayrıca bir grafik üzerine çizilmiş, ve bu grafikler de çalışmaya ek olarak konulmuştur.

4.4.1 Ek-C1 : $U_o(\{P_{13}..P_{212}\}, \{P_{13}..P_{212}\}, \{1..4\})$ tablosu

Yapılacak hesaplama ve analizlerde kullanmak üzere, $\{P_{13}..P_{212}\}$ asal sayılarını içeren uyum adedi ve uyum oranı değerleri hesaplanarak Ek-C1 grubu tablolar oluşturulmuştur. Bu grup, {C1-13..C1-212} olmak üzere 200 ayrı ek'ten oluşmaktadır. Herbir ek, asal sayılar kümesine ait $\{P_{13}..P_{212}\}$ listesi içindeki bir sayının p, listede bulunan diğer tüm sayıların ise q olarak seçilmeleri durumunda elde edilen değerleri içermektedir ve herbir ekin adı, o anda geçerli p sayısının liste içindeki sırası kullanılarak oluşturulmuştur. Örneğin C1-13 eki P_{13} sayısının, C1-212 eki ise P_{212} sayısının p olarak seçilmesi durumunda elde edilen değerleri içermektedir.

Ek-C1 grubu içindeki bilgilerin açıklamasını yapmak üzere, C1-13 eki örnek olarak kullanılacaktır. Bu ek içinde 200 satır, herbir satırda ise 4 ayrı sütun vardır. Herbir satır ile sütunda yeralan değerlerin açıklaması aşağıdadır.

- İlk satırda 4 ayrı değer bulunmaktadır:
  - 1. Sütun : $U_o(P_{13},P_{13},\mathbf{s=1})$
  - 2. Sütun : $U_o(P_{13},P_{13},\mathbf{s=2})$
  - 3. Sütun : $U_o(P_{13},P_{13},\mathbf{s=3})$
  - 4. Sütun : $U_o(P_{13},P_{13},\mathbf{s=4})$

  Herbir uyum oranı değerinin yanında, yine bu değerin ait olduğu uyum adedi değeri de mevcuttur. (uyum adedi, uyum oranı değerinin hesaplanması amacı dışında kullanılmayacaktır)
- Herbir satır, içinde yukarıda tanımlanan 4 ayrı sütun mevcut olmak üzere aşağıdaki değerleri içermektedir:

- 001. Satır : $U_o(P_{13}, q=P_{13+000}, \{1..4\})$
- 002. Satır : $U_o(P_{13}, q=P_{13+001}, \{1..4\})$
- .....
- 200. Satır : $U_o(P_{13}, q=P_{13+199}, \{1..4\})$

Ek-C1 grubu ekler, herbiri yukarıda ifade edilen 200 satırlık bilgiyi içermek üzere, aşağıda tanımlanan 200 ayrı tablodan oluşmaktadır:

- C1-13 : $U_o(p=P_{13+000}, \{P_{13}..P_{212}\}, \{1..4\})$
- C1-14 : $U_o(p=P_{13+001}, \{P_{13}..P_{212}\}, \{1..4\})$
- C1-15 : $U_o(p=P_{13+002}, \{P_{13}..P_{212}\}, \{1..4\})$
- ...
- C1-212 : $U_o(p=P_{13+199}, \{P_{13}..P_{212}\}, \{1..4\})$

4.4.2 Ek-C2 : Ek-C1 grafiği

Ek-C1 grubu tabloda yer alan bilgiler, Ek-C2 grubu grafiklerde çizilmiştir. Ek-C1 grubundaki herbir tabloya karşılık Ek-C2 grubunda bir grafik, ve herbir grafikte de (her seviye için bir adet olmak üzere) dört adet eğri vardır. Böylece örneğin Ek-C2-13 grafiği Ek-C1-13 tablosundaki, Ek-C2-212 grafiği ise Ek-C1-212 tablosundaki (dört sütunda yer alan) bilgilerin (dört ayrı) çizimlerini içermektedir.

4.4.3 Ek-C3 : $U_{oo}(\{P_{13}..P_{212}\}, [P_{13}..P_{212}], \{1..4\})$ tablosu

$U_{oo}(\{P_{13}..P_{212}\}, [P_{13}..P_{212}], \{1..4\})$ değerleri, Ek-C3 tablosunda yer almaktadır.

4.4.4 Ek-C4 : Ek-C3 grafiği

Ek-C3 tablosunda yer alan bilgiler, Ek-C4 grafiğinde çizilmiştir. Bu grafikte yatay eksen P_k'nin sırasını belirten k değerini, dikey eksen ise $U_{oo}(P_k)$ değerini göstermektedir. Bu grafiğin kolay analiz edilebilmesi amacı ile, ardışık her iki uyum oranı ortalaması ($U_{oo}(P_k)$ ile $U_{oo}(P_{k+1})$) düz bir çizgi ile birleştirilmiştir.

4.4.5 Ek-C5 : $U_{ooo}(\{P_{13}..P_{212}\}, [P_{13}..P_{212}], \{1..4\})$ tablosu

Ek-C4 grafikte yer alan uyum oranı ortalaması değerlerinin uzun vadede ortalama olarak değişip değişmediğini analiz etmek üzere $U_{ooo}(\{P_{13}..P_{212}\},[P_{13}..P_{212}],\{1..4\})$ tablosu Ek-C5'te oluşturulmuştur.

4.4.6 Ek-C6 : Ek-C5 grafiği

Ek-C5'te yer alan U_{ooo} değerleri kullanılarak Ek-C6 grafik çizilmiştir.

4.4.7 Ek-D : Ek-C1'in $U_o(\{P_{13}..P_{212}\}, \{P_{13}..P_{212}\}, 1)$ değerine göre sıralanmış hali

Seviye artışının analizini daha detaylı olarak yapmak üzere, ilk olarak Ek-C1 grubuna dahil 200 tablo tek tek ele alınarak herbir tablo içindeki 200 satır, bu satırlarda bulunan $U_o(p,q,s=1)$ değerine göre yeniden sıralanmıştır. Bu şekilde ortaya çıkan 200 adet tablo, Ek-D grubunu oluşturmuştur. Bu grup {D13..D212} eklerinden oluşmakta, ve Ek-D grubundaki her bir ek, Ek-C1 grubundaki ilgili ekin sıralanmış halini içermektedir. Örneğin Ek-D13, Ek-C1-13'ün sıralanmış halidir.

Bu tabloda sıralama $U_o(p,q,s=1)$ değerine göre yapılmış olduğuna göre, q değeri sıralı değildir. Tabloda q sütununa bakıldığında bu durum kolaylıkla görülebilir.

4.4.8 Ek-E : Ek-D grafiği

Ek-E içinde yeralan herbir grafik, Ek-D grubu içindeki bir tablonun gösterimidir. Ek-D grubu içindeki tablolarda $s \in \{1..4\}$ olmak üzere yer alan dört ayrı uyum oranı sütununun herbiri, Ek-E grubu içindeki grafiklerde ayrı bir eğri olarak yer almaktadır. Örneğin Ek-E13 grafiği, Ek-D13'de mevcut aşağıdaki değerlerin dördünün çizimini de içermektedir.

- $U_o(P_{13},\{P_{13}..P_{212}\},1)$
- $U_o(P_{13},\{P_{13}..P_{212}\},2)$
- $U_o(P_{13},\{P_{13}..P_{212}\},3)$
- $U_o(P_{13},\{P_{13}..P_{212}\},4)$

Ek-D tablosu q değerine göre sıralı olmadığı için, Ek-E tablosundaki yatay eksen de artık önceki grafikler gibi P_k değerinin k indeksini göstermemektedir; buna karşılık yalnızca tablodaki satırın sırasını göstermektedir.

4.5 $\{P_{13}..P_{212}\}$ için uyum analizi

Uyum sayıları hesaplamaları sonucunda oluşturulmuş olan her tabloya karşılık bir de grafik oluşturulduğu belirtilmişti. Yapılan sayısal analizlerde ilgili tablolar, görsel analizlerde ise bunların grafikleri kullanılmıştır.

4.5.1 q parametre analizi

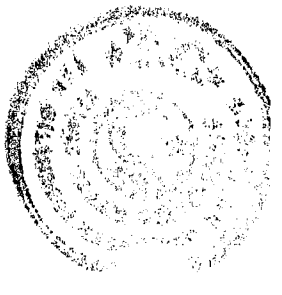
Ek-C1 ve Ek-C2 analizi

Uyum sayıları açısından araştırılması gereken önemli bir konu, p ve q (dolayısı ile n) değerleri arttıkça, uyum oranında ne gibi bir değişme olduğudur. Bu önemlidir; çünkü temel amaç p ve q olarak büyük sayılar kullanmak olduğuna göre, n değeri arttıkça uyum oranının azalması demek, şifre sistemi tasarımcısının daha az uygun sayı arasından bir seçim yapmak zorunda kalması demektir, ki bu da arzu edilir bir durum değildir. Bu nedenle sayılar büyüdükçe bu oranın azalmaması ümit edilmektedir. (Dikkat edilirse, sayılar büyüdükçe uyum adedinin artması doğaldır. Oysa uyum oranının da artması demek, şifre sistemi tasarımcısının sayıların artışı ile birlikte en azından doğru orantılı sayıda *uygun sayı*ya sahip olması demektir.)

Ek-C1-13 tablosunda yer alan ve Ek-C2-13 grafiğinde çizilen $U_o(P_{13},\{P_{13}..P_{212}\},1)$ değerleri analiz edildiğinde, şu bilgiler elde edilmektedir:

- Uyum oranı ortalaması, iki sınır değer arasında değişmektedir.
- Uyum oranı, sürekli artış ya da azalış içinde değildir.
- Uyum oranı hiçbir değerde sabit kalmamaktadır.
- Uyum oranı ortalama değer çevresinde değişmektedir.
- Değerlerin rassal olduğu göze çarpmaktadır.

Ek-C1 grubu tablo ve bağlı Ek-C2 grubu grafiklerin hepsi ayrı ayrı incelendiğinde, yukarıdaki üç maddelik gözlem hepsinde aynen görülmekte, yalnızca ilk maddede belirtilen



sınır değerleri değişmektedir. Dolayısı ile q değeri değiştikçe uyum oranında bir azalma görülmemektedir.

4.5.2 p parametre analizi

Ek-C3 ve Ek-C4 analizi

Ek-C3 tablo ve bağlı Ek-C4 grafikte göze çarpan önemli hususlar şunlardır:

- Uyum oranı ortalaması, iki sınır değer arasında değişmektedir.
- Uyum oranı ortalaması, sürekli artış ya da azalış içinde değildir.
- Uyum oranı ortalaması, hiçbir değerde sabit kalmamaktadır.
- Uyum oranı ortalaması, ortalama değer çevresinde değişmektedir.
- Değerlerin rassal olduğu göze çarpmaktadır.
- Üst sınır, alt sınırdan daha belirgindir.

Ek-C5 ve Ek-C6 analizi

Ek-C4 grafikte belirlenen "p büyüdükçe U_{oo}'nun azalmayacağı" ipucu'nun sağlam bir temele dayanıp dayanmadığını makro ölçüde analiz etmek üzere Ek-C6 grafiğe göz atılabilir. Eğrinin ilk kısımlarında bir dalgalanma mevcuttur. Bu dalgalanma ile oluşan eğri görünümü çizimin ortalarına yaklaştıkça bir *doğru* haline dönüşmektedir. Zaten P_{13} civarında ortaya çıkan U_{ooo} değerleri ile P_{212} civarındaki değerler birbirine çok yakındır.

Ek-C4 ve Ek-C6 grafikler birlikte incelendiğinde, p arttıkça uyum oranı değerinin azalmayacağı, ve uyum oranının, p'nin artışına bağlı olmaksızın rassal olarak belirlendiği ortaya çıkmaktadır. Bu durum şifre sisteminin tasarımını yaparken kolaylık sağlayacak, ve şifre kırıcının belirli özellikteki p üzerinde yoğunlaşarak avantaj kazanmasını önleyecek bir husustur.

4.5.3 s parametre analizi

Şifre sisteminde varolan seviye adedi; uyum adedi ve dolayısı ile uyum oranını direkt olarak etkilemektedir. Bu doğaldır, çünkü belirli bir seviye değerine göre uygun olan bir sayı, seviye adedi artırıldığı durumda artan seviye adedi kadar daha kare değerinin tersinin mevcudiyetini sağlaması gerekmektedir. Bir kısım uygun sayı yeni koşulları da sağlarak

uygun sayı olabilecektir; ama bazı uygun sayılar yeni durumda uygun sayı olmaktan çıkacaktır. Daha önce uygun sayı olmayan hiçbir sayı yeni durumda uygun sayı da olamayacağından dolayı, seviye adedi arttıkça uyum adedinin azalması doğaldır. Bir önceki konuda, $\{P_{13}..P_{212}\}$ sayılarının uyum oranları $\{1..4\}$ seviye adetleri için ayrı ayrı incelenmiş, ve bu değerlerin p ile q değerlerinin artışlarına bağlı olarak ne şekilde değiştiğinin analizi yapılmıştır. Bu bölümde ise uyum değerlerinin farklı seviyelere bağlı olarak değişimi konusu analiz edilecektir.

Ek-C1 ve Ek-C2 analizi

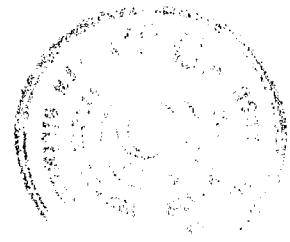
Uyum oranı değerlerinin seviye artışına bağlı olarak değişimi, aynı p ve q değerleri için her s değerine karşılık ayrı bir eğrinin yeraldığı Ek-C2 grubu grafiklerde incelenebilir. Bu grafiklerde önemli saptamalar vardır:

- $s = 1$ eğrisinde yeralan yükselme ve düşmeler, $s > 1$ eğrilerine de yansımıştır. Bu değişmeler, herbir p için geçerlidir. Dolayısı ile $U_o(p,q=P_{k+1},s)$ değeri $U_o(p,q=P_k,s)$ değerine göre artış gösteriyor ise bu artış $U_o(p,q=P_{k+1},s+1)$ ile $U_o(p,q=P_k,s+1)$ arasında da gerçekleşmektedir. Düşmelerde de aynı durum mevcuttur.
- Bu değişmeler genlik olarak ta benzer şekilde olmakta, $U_o(p,q=P_{k+1},s)$ ile $U_o(p,q=P_k,s)$ arasındaki artışın genliği fazlalaştıkça $U_o(p,q=P_k,s+1)$ ile $U_o(p,q=P_{k-1},s+1)$ arasında da yüksek genlikte bir artış gözlenmektedir.

Ek-D ve Ek-E analizi

Önceden tanımlandığı üzere Ek-D tablosu, Ek-C1 tablosunun $U_o(p,q,s=1)$ değerine göre sıralanmış halidir. Dolayısı ile Ek-E grafikte $U_o(p_l) \leq U_o(p_{l+1})$ garanti edilmiştir. Dikkat edilirse $s \in \{2..4\}$ için bu durum garanti altına alınmamıştır. Burada k yerine l kullanılmasının nedeni, k değerinin kullanılması durumunda P_k ile P_{k+1} değerlerinin P asal sayılar kümesinde iki ardışık sayıyı sembolize ediyor izlenimi vermesinden dolayıdır. Oysa Ek-E grafikte yatay eksendeki iki ardışık asal sayı, Ek-D tablodaki satırların $U_o(p,q,s=1)$ değerine göre sıralanması sonucunda yanyana gelen sayılar olmaktadır ve bu sayıların P asal sayılar kümesindeki indeksi ile ilgili hiç bir ipucu bu aşamada mevcut değildir.

Bu tablo ve grafiklerin tümünde göze çarpan bazı özellikler vardır.



- $U_o(p,q,s=1)$ eğrisine ait U_o değerleri p_l ile p_{l+1} arasında sürekli artış içindedir, ki bu durum sıralama yapılarak garanti altına alınmış idi.
- $U_o(p,q,s\in\{2,3,4\})$ eğrisine ait U_o değerleri de bir önceki gözleme yakın sonuçlar vermektedir. Bu eğrilerde uyum oranları bazen önceki değerlerden düşük olduğu halde büyük düşüş yaşanmamaktadır, ve zaten genel bir yükseliş eğilimi de mevcuttur.
- $s = 1$ eğrisi her noktada diğer eğrilerin üzerinde yer almaktadır. Bu durum $s\in\{2,3,4\}$ eğrilerinin herbiri için gerçekleşmektedir.
- Eğriler arasında bir kesişme söz konusu değildir. Her eğri (aynı eksenlere bağlı olarak çizildikleri halde) birbirinden tamamen bağımsız olarak yer almıştır.

Herbir grafikteki dört ayrı eğri kendi içinde incelendiğinde, bu eğriler içinde ortak noktalar göze çarpmaktadır. Hatırlanacağı gibi Ek-D grubu tablolar, $U_o(p,q,s=1)$ değerlerine göre küçükten büyüğe sıraya sokulduğundan, bu tabloda peşpeşe yer alan iki uyum oranı içinden sonra yer alan uyum oranı, önce yer alan uyum oranı'ndan hiçbir zaman küçük olamaz. Bu durumun grafikteki $s = 1$ eğrisinde görülmesi de bu nedenle doğaldır. Oysa $s\in\{2,3,4\}$ durumuna ait eğrilerde de q değeri arttıkça uyum oranı değerlerinin de artmakta olduğu farkedilmektedir. Bu artış, $s = 1$ eğrisinde olduğu gibi mutlak değildir; yine de bu eğriler için artış durumu gözlenmektedir. Bu, çok önemli bir olaydır; $s = 1$ için yüksek uyum oranı değeri veren p ve q sayıları, $s > 1$ durumunda da yüksek değerler oluşturmaktadır. $s = 1$ için düşük uyum oranı değeri veren p ile q sayıları ise yine $s > 1$ için de düşük değerler oluşturmaktadır.

5. SONUÇ VE ÖNERİLER

5.1 Sonuçlar

Bu çalışmada, başlangıç bölümlerinde tanımlanan hiyerarşik grupsal kurumlarda kullanılacak güvenli bir şifre sisteminin tasarımı yapılmaktadır. *Hiyerarşik Grupsal Kurum Modeli*'nde kurumların gruplardan oluştuğu, herbir grupta bir ya da daha fazla seviyeli gizlilik seviyelerinin bulunabileceği, etkin bir şifre sisteminde hem grupsal, hem de hiyerarşik bölünmenin dikkate alınması gerektiği belirtilmiştir. Bir seviyedeki kişilerin kendi seviyelerine ilişkin bilgilere erişimlerinin mümkün olması yanında, kendilerinden daha alt seviyedeki kişilere ilişkin bilgilere erişmelerinin de olanaklı kılınmasının gerekli olduğu vurgulanmış, üst seviyeye ilişkin bilgilere erişmelerinin ise engellenmesi gerektiği belirtilmiştir.

Tasarlanan şifre sisteminde p, q asal sayıları ile bunların çarpımından oluşan bir n sayısı temel olarak kullanılmaktadır. Her elemana, bağlı olduğu grubun şifre çözme anahtarı ile birlikte bulunduğu seviyenin şifre çözme anahtarının verileceği, bu anahtarların karşılıkları olan şifreleme anahtarları ile p ile q sayılarının gizli kalacağı, n sayısının ise açık olarak yayınlanacağı belirtilmiştir. Kurum içinde yayınlanacak olan bir mesajın önce grup şifreleme anahtarı, daha sonra da seviye şifreleme anahtarı ile şifrelenerek kurum içinde yayınlanacağı, yetkili kullanıcıların ise öncelikle ellerinde mevcut seviye şifre çözme anahtarını, daha sonra da grup şifre çözme anahtarını kullanarak iki kez şifre çözme işlemi uygulamak yolu ile şifrelenmiş mesajın özgün halini bulabilecekleri teorik olarak açıklanmıştır. Grup şifreleme algoritmasında ayrıca bir a sayısı kullanılarak *ayrık logaritma* probleminin sisteme dahil edilmesi sağlanmıştır. Önerilen modelde hem *ayrık logaritma*, hem de *çarpanlara ayırma* zor problemleri temel alınarak şifrelenmiş mesajın şifre kırıcılar tarafından polinom zamanda kırılmaları engellenmiştir.

Eğer verilen bir c sayısı için $c^{-1} \bmod \phi(n)$ değeri, yani c'nin $\phi(n)$'e göre tersi mevcut ise bu c sayısı 1. seviyede kullanılabilir bir sayı olmaktadır. Bunun gerçekleşmesi için ise obeb(c, $\phi(n)$) = 1 olmalıdır. c'nin $\phi(n)$'e göre tersi, $c^{-1} \bmod \phi(n) = c^{-\phi(\phi(n))-1} \bmod \phi(n)$ eşitliği ile bulunabilir. Kurum içinde eğer s adet seviye mevcut ise, bu şartın yanında c'nin s-1 kere

alınacak kare değerlerinin de $\phi(n)$'e göre tersleri mevcut olmalıdır. Bu şartı sağlayan c sayısına *uygun sayı* denilmektedir.

Şifre sisteminin tasarımında p ile q asal sayılarının çarpımından oluşan n sayısı sözkonusu olduğunda bir c sayısının $\phi(n)$'e göre tersinin az önce verilen denklem kullanılarak bulunması için $\phi(n)$'in asal çarpanlarına ayrılması gerekmektedir. $\phi(n)$ değeri n değerine nispeten daha küçük bir sayı olmasına ve bu nedenle $\phi(\phi(n))$ değerinin hesaplanması, şifre kırıcının yapması gerekli olan n değerinin asal çarpanlarına ayrılması problemine göre çok daha az zaman almasına rağmen çalışmada $\phi(\phi(n))$ değerinin hesaplanmasına gerek kalmaması için bir yöntem tanımlanmıştır.

Şifre tasarımcısının harcayacağı süreyi en alt düzeye indirmek amacı ile p ile q değerleri belirlenirken $\phi(n)$ değerinin bulunmasının kolay olması gözetilebilir. Bu amaçla örneğin öncelikle asal bir p' sayısı kullanılarak $2*p'+1$ sayısının asal olma durumu kontrol edilmiş, bu sayının asal olması durumunda $p=2*p'+1$ asal sayısı elde edilmiştir. q' asal sayısı kullanılarak $q=2*q'+1$ asal sayısı da belirlendiğinde $n=p*q$; $\phi(n)=(p-1)*(q-1)$; $\phi(\phi(n))=2^2*p'*q'$değerleri kolaylıkla hesaplanabilmektedir, ki bu durumda çarpanlara ayırma problemine gerek kalmamaktadır. Bu durumda uyum adedi değeri, Denklem-4.2 kullanılarak hesaplanabilir. Bu şekilde yapılacak işlemlerde, kullanılacak olan asal sayıların, açık olarak yayınlanmış listelerde bulunmaması gerekmektedir. Çünkü böyle bir durumda sistemin kırılması kolaylaşacaktır. Dolayısı ile bu gibi bir belirlemede, işlemin nasıl yapıldığının şifre kırıcıların bilmemeleri konusu önem kazanmaktadır.

Bir kişinin elindeki $(c^m)^2$ değerini kullanarak c^m değerini elde etmesinin önlenmesi için $(c^m)^2 > n$ şartının gerçekleşmesi gerektiği, bu nedenle uygun sayı aramasının $[\lceil\sqrt{n}\rceil..n-2]$ arasında yapılması gerektiği belirtilmiştir.

Uygun sayılar, şifre sisteminde ilk hiyerarşik seviyede şifre çözme anahtarı olarak, bunun tersi ise yine ilk seviyede şifre çözme anahtarı olarak kullanılmıştır. Uygun sayının ardışık kare değerleri, ilgili üst seviyelere dağıtılmış, bunların $\phi(n)$'e göre tersleri ise şifreleme anahtarı olarak kullanılmıştır. Çalışmada da belirtildiği gibi bir seviyedeki kişi,

kendisinden daha alt seviyeye gönderilmiş bir mesajı çözme amacı ile elindeki şifre çözme anahtarının karesini alarak kullanabilmektedir. Böylece bir kişinin yalnızca bir grup ve bir seviye anahtarını muhafaza etmesi yeterli olmakta, alt seviyeye ilişkin anahtarı ise basit kare alma işlemi ile üretebilmektedir. Üst seviye anahtarını üretme ise *quadratik residue* probleminin çözülmesini gerektirdiğinden polinom zamanda mümkün değildir.

Önerilen sistemde güvenilirliğin sağlanması için anahtar seçiminde p ile q sayılarının uzunluklarının birbirine yakın olması; (p-1) ile (q-1)'in büyük asal sayıları içermesi; obeb(p-1,q-1)'in küçük bir sayı olması gerektiği ayrıca belirtilmiştir.

Tasarlanan şifre sistemi, şu nedenlerle özgün bir çalışmadır:

1. Tanımlanan grupsal hiyerarşik model için öngörülen ilk çözüm olması.
2. Bir kişinin elinde bulunan seviye anahtarını kullanarak kendisine göre alt seviyenin anahtarını basit kare alma işlemi ile üretebilmesi; üst seviye anahtarı üretiminin ise NP problem kullanımı yoluyla engellenmiş olması.
3. Alt seviye anahtarının kolaylıkla üretilebilmesi sağlandığından, bir kişinin kendisine göre alt seviyedeki tüm anahtarları elinde tutma gereksiniminin ortadan kalkmış olması.

Kurum içinde iki ya da daha fazla grup ve iki ya da daha fazla hiyerarşik seviye mevcut olduğunda, bu çalışmada tasarlanan şifre sistemi güvenli bir şekilde kullanılabilir. Eğer tek bir grup mevcut ise bu durumda grupsal olarak şifreleme, artık yalnızca ikinci bir şifreleme olanağı tanır, fazladan bir güvenlik sağlasa da zaten hiyerarşik seviye şifrelemesi yeterli güvenlik tesis edeceğinden, grupsal şifrelemeye gerek kalmaz. Hiyerarşik olarak tek bir seviye mevcut olduğunda ise artık şifre sisteminin temel kullanım nedeni ortadan kalkmış olur. Bu durumda sistemin güvenliği, RSA algoritması ile sağlanan güvenlik kadar olur.

Tasarlanan şifre sisteminde kullanılan algoritmalar, çalışmanın başlangıç bölümünde tanımlanan NP problemlere dayandığından, kırılamaz. Hiyerarşik şifreleme bölümünde kullanılan algoritma, RSA algoritmasında da kullanılan *bölenlere ayırma* problemine dayanmaktadır. Grupsal şifreleme algoritması ise El Gamal algoritmasında kullanılan *ayrık logaritma* problemine dayanmaktadır. Her iki algoritmanın avantaj ve dezavantajları, aynı

problemler kullanıldığından dolayı burada da geçerlidir, ve bu dezavantajların yokedilmesi ile ilgili özel bir çalışma yapılmamıştır.

Kurum, iki ve daha büyük seviye içerdiğinde şifre sistemi tasarımcısı öncelikle yüksek uyum oranı veren bir sistem tasarlayabilmek amacı ile belirleyeceği p' ve q' değerlerini kullanarak uyum adedi ve oranını hesaplayacak, uyum oranı düşük olduğu sürece yeni p' ve q' değerleri ile işlemi tekrarlayacaktır. Tatmin edici bir değer elde ettiği zaman ise belirlediği sayılara göre bir uygun sayı arayacaktır. Bu sayıyı da bulduğunda artık sistem sayıları ile hiyerarşik şifre alt sistemi sayıları belirlenmiş olmaktadır. Grup sayıları da belirlediğinde şifre sistemi sayıları tamamen belirlenmiş olmaktadır.

Şifre sisteminin oluşturulması için üç grup sayının belirlenmesi gerekmektedir: sistem sayıları, hiyerarşik seviye sayıları ve grup sayıları.

Sistem sayılarının belirlenmesi için asal bir p' seçilmekte, ve $p = 2p' + 1$ sayısının asal olup olmadığı kontrol edilecektir. Bu şekilde asal bir sayı bulunduğu zaman aynı işlem $q = 2q' + 1$ için de yinelenerek asal bir sayı elde etmeye çalışılacaktır. Bu şekilde asal p ve q sayıları bulunduğunda $n = p * q$ olmak üzere sistem sayıları elde edilmiş olacaktır. Bunun sonucunda elde edilecek bazı değerler aşağıdaki gibidir:

$p = 2p' + 1$

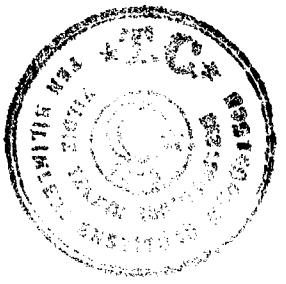
$q = 2q' + 1$

$n = p * q = (2p' + 1) * (2q' + 1)$

$\phi(n) = (p - 1) * (q - 1) = ((2p' + 1) - 1) * ((2q' + 1) - 1) = 4p' * q' = 2^2 * p' * q'$

$\phi(\phi(n)) = 2(p' - 1)(q' - 1)$

Çalışma içinde, p, q, n, $\phi(n)$ değerlerinin belirlenmesine örnek teşkil etmek üzere uygulamalar yapılmıştır. Bu uygulamalar dört ayrı grup asal sayılar kullanılarak yapılmıştır. İlk uygulamalar $P_{13}..P_{212}$, ikinci uygulamalar $P_1..P_{1,000,000}$, üçüncü uygulamalar {10, 20, 30, 40, 50, 60} basamaklı sayılar, son uygulamalar ise 130 .. 250 basamaklı sayılar kullanılarak yinelenmiş, ve her durumda şifre sisteminin doğru olarak çalıştığı örnekler üzerinde de görülmüştür.



Bir alt seviye anahtarının üretilmesi için yalnızca kare alma işlemi ile sınırlı kalınmadığı, istendiğinde daha başka bir üs değerinin de kullanılabileceği belirtilmiştir. Böyle bir durumda şifre çözücülerin de bu işlemi bilmeleri gerektiği, doğaldır.

Tasarlanan şifre sistemine ait uygulamalar, 15 seviye ve 250 basamaklı n değeri kullanılarak yapılmış, ve elde edilen değerler, çalışmanın ekinde verilmiştir.

Tanımlanmış olan UAB algoritması kullanılarak, bu sistem sayılarının kullanılması durumunda elde edilecek olan uyum adedi bulunarak, tatmin edici bir sonuç elde edilip edilmediği kontrol edilebilir. Gerektiğinde de yeni sistem sayılarının belirlenmesi amacı ile işlemler yinelenebilir.

Dördüncü bölümde, uygun sayı, uyum adedi, uyum oranı, uyum oranı ortalaması tanımları yapılmıştır:

- *Uyum adedi*, uygun sayılar kümesi'nde bulunan elemanların adedidir:

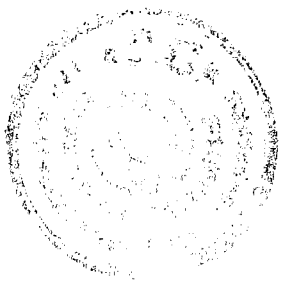
$U(p, q, s) = |u(p,q,s)|$

- Uyum oranı, *uyum adedi*'nin n'ye ondalık sayı olarak bölünüp 10,000 ile çarpılması ve en yakın tamsayıya yuvarlanması sonucu bulunan tamsayı değeridir ve bu değer, onbinde olarak oran ifade eder.

$$U_o(p,q,s) = \left[10{,}000 * \left(\frac{U(p,q,s)}{n} \right) \right]$$

- Uyum oranı ortalaması: P_k sayısının p, liste içindeki diğer tüm sayıların sırası ile q olarak seçilmesi durumunda ve önceden belirtilmiş olan seviye adedine göre hesaplanacak olan $|\{P_L..P_R\}| = R\text{-}L+1$ adet uyum oranı'nın aritmetik ortalaması olarak tanımlanmış ve bulunması için gerekli formül verilmiştir:

$$U_{oo}(P_k, [P_L..P_R], s) = \frac{\sum_{i=L}^{R} U_o(p_k, p_i, s)}{|\{P_L..P_R\}|}$$



- Uyum oranı ortalamalarının ortalaması, Bir P_k sayısı için $[P_L..P_R]$ sayılarının uyum oranı ortalaması değerlerinin aritmetik ortalamasıdır.

$$U_{ooo}(P_k,[P_L..P_R],s)=\frac{\sum_{i=L}^{k}U_{oo}(P_i,q\in[P_L..P_R],s)}{k}$$

Çalışmanın dördüncü bölümünün kalan kısmında, uyum sayıları hesaplama ve analizleri yer almaktadır. Bu amaçla öncelikle [P_{13} .. P_{212}] sayıları ele alınarak bu sayılardan herbirisinin sırası ile *p*, diğerinin de *q* olarak seçilmesi durumunda elde edilecek 200 * 200 adet uyum adedi ve uyum oranı değerleri hesaplanmış ve elde edilen değerlerin örnekleri çalışmanın Ek-C1 ekine konulmuştur. Daha sonra herbir *p* değeri için bulunan değerler ayrı bir sayfada olmak üzere Ek-C2 grubu grafikler çizilmiştir. Bu grafikler üzerinde yapılmış olan analizler sonucunda şu gözlemler edinilmiştir:

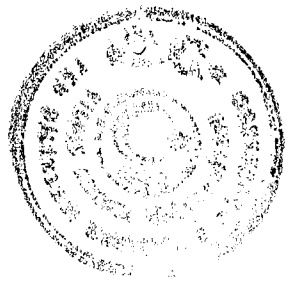
- Uyum oranı, iki sınır değer arasında değişmektedir.
- Uyum oranı, sürekli artış ya da azalış içinde değildir.
- Uyum oranı hiçbir değerde sabit kalmamaktadır.
- Uyum oranı ortalama değer çevresinde değişmektedir.

Bir sonraki aşamada [P_{13} .. P_{212}] arasındaki sayıların herbirisi için elde edilen uyum oranlarının ortalamaları alınarak elde edilen uyum oranları Ek-C3 grubu ekine konulmuş, grafiği ise Ek-C4'te çizilmiştir. Bu değerlerin kümülatif ortalamaları olan uyum oranları ortalamaları Ek-C5'e konulmuş, grafiğ ise Ek-C6'da çizilmiştir.

Ek-C4'de yapılan incelemeler sonucunda, Ek-C2 grubu grafiklerde elde edilen gözlemler burada da görülmüştür.

Ek-C6'da yapılan incelemeler sonucunda ise uyum oranının *p* ile *q* değerlerinin artışı ile düşmediği gözlenmiştir.

Şifre sistemi için uygulamalar, 60-130 basamaklı *p* ile *q* sayıları kullanılarak uygulanmış, elde edilen uygun sayı örnekleri ve şifreleme-şifre çözme uygulaması Ek-I'da yer almıştır.



5.2 Öneriler

Aşağıdaki konularda destekleyici çalışmalar yapılabilir.

- Kullanılacak olan c sayısının bazı özellikleri, şifre sisteminin şifre kırıcı tarafından kırılmasını kolaylaştırıp zorlaştırabilir. Varsa c sayısının seçimine etki edebilecek olan bu kriterler ortaya konulabilir. Bu özelliklerin bir kısmı, bu çalışmada belirtilmiştir. Yine de ek girdiler bulunabilir.

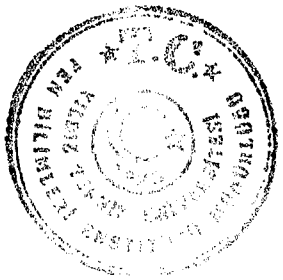
- Kullanılacak p', p, q', q ve dolayısı ile n sayılarının bazı özellikleri de şifre sisteminin şifre kırıcı tarafından kırılmasını kolaylaştırıp zorlaştırabilir. Bu özellik p sayısının özelliğine dayanabilir; ya da eşleşeceği q sayısı ile ilgili olabilir. Varsa p ile q değerlerinin seçimine etki edebilecek olan bu kriterlerin ortaya konulabilir.

- Sistemde şifreleme yalnızca bir grup ve bir minimum erişim seviyesi hedef alınarak hazırlandığından, örneğin iki ayrı grubun okuması gereken mesajların iki grup için ayrı ayrı şifrelenmesi, ve dolayısı ile bir mesaj için iki ayrı şifrelenmiş mesaj'ın hazırlanması gereği vardır. Varsa bu durumda iki ayrı grup için iki ayrı şifreleme gereksinimini ortadan kaldırabilecek ya da bu konudaki gayreti azaltacak olan yeni bir sistem ortaya konulabilir. Bu sistem değişik gruplama kombinasyonları için de geliştirilebilir.

- Hiyerarşik ve grupsal, yine de bu çalışmada ele alındığından farklı bir şekilde olabilecek bir başka organizasyon yapısı için sistemin geliştirilmesi.

- Sistem içinde *MD* tarafından yapıldığı belirtilen, şekli hakkında yeni bir metod öngörülmeyen; anahtar üretim, dağıtım ve depolama konuları hakkında yeni metodlar geliştirilebilir.

- Erişim seviye anahtarının karesi yerine bir başka üssü alınarak bir alt seviye anahtarı üretildiğinde sistemin ne şekilde etkilediği araştırılabilir. Bu durumda problem, *computing square-root* yerine *discrete logarithm* algoritmasına dayanmış olur. Bu



durumda uyum adedinin artıp artmayacağı ve çalışmada yapılmış olan analizleri değiştirip değiştirmeyeceği araştırılabilir.

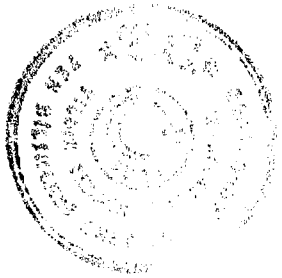
- s değeri arttıkça, uyum oranı düşük seviyelere inmektedir. Uyum oranı azaldıkça da p ve q sayılarını seçme, dolayısı ile şifre sistemi oluşturma işlemi zorlaşmaktadır. Buna karşın şifre kırma işlemi kolaylaşmaktadır. Bu durumda yüksek seviye adedinde de bu protokolün kullanılmasını daha güvenli duruma getirecek bir yöntemin bulunması önem kazanmaktadır.

- Uyum adedi (dolayısı ile oranı) hesaplamalarda $U(p,q,s)$ olarak tanımlanmış ve kullanılmıştır. Oysa $U(p,q,s)=U(p*q,s)=U(n,s)$ anlamına da gelmektedir. Dolayısı ile her iki kullanım da aynı anlamı ifade eder. Oysa analizde bu durum değişir. Bu çalışmada yapılan analizlerde p ile q ayrı ayrı kullanılmış, ve bu şekilde p'nin artışına bağlı olarak ortaya çıkacak olan durum analiz edilebilmiştir. n kullanılması durumunda ise, p ile q birlikte değerlendirilmiş olmaktadır. Bu analiz örneğin $n_1..n_2$ arasında yüksek uyum oranı oluştuğuna karar verirse, bu durum yalnızca p ile q'nun $n_1..n_2$ değerini oluşturacak şekilde seçiminin uygun olduğu görülmüş olur. Bu yaklaşımın iyi sonuç verip vermeyeceği ise analiz yapılmasını gerektiren bir durumdur.

- Belirlenmiş olan p ile q değerlerine göre oluşacak olan *uyum adedi* değerinin bu çalışmada belirtilen algoritmalar dışında bir hesaplama yöntemi kullanılarak bulunmasına çalışılabilir.

- Bölüm-4.4.4.1'de anlatılan konu ile ilişkili olarak, belirlenmiş bir p (ya da p ve q) için uyum oranı alt-üst sınırı bulmak için çalışmalar yapılabilir.

- Bir şifre sisteminin güvenli olması için belirli bir en az uyum oranı değeri var ise ve bu değerler başka kriterlere bağlı ise, bunların bulunması için çalışmalar yapılabilir.



KAYNAKLAR

Adleman. L. M., Pomerance, C. ve Rumely, R. S., (1983), "On distinguishing prime numbers from composite numbers", Annals of Mathematics., Cilt 117, Sayfa 173-206.

AKL, S.G. ve TAYLOR, P.D., (1983), "Cryptographic solution to a problem of access control in a hierarchy", ACM Transactions on Computer Systems, Cilt 1, No 3.

Ayoub, F. ve Singh, K., (1984), "Cryptographic techniques and network security", IEE Proceedings, Cilt 131, Pt.F, No 7.

Blakley, B. ve Blakley, G.R.,(1978), "Security of number theoretic public key cryptosystems against random attack", Cryptologia Bölüm 1, Cilt 2, No 4, Sayfa 305-321.

Blakley, B. ve Blakley, G.R., (1979), "Security of number theoretic public key cryptosystems against random attack", Cryptologia Bölüm 2, Cilt 2, No 4, Sayfa 305-321.

Blakley, G.R. ve Borosh, I., (1979), "Rivest-Shamir-Adleman public key cryptosystems do not always conceal messages", Comp. & Math. with applications, Cilt 5, Sayfa 169-178.

Beth, T., Frisch, M. ve Simmons, G.S., (1992), Lecture notes in computer science, public-key cryptology: State of the art and future directions, Springer-Verlag.

Bressoud, D.M., (1989), Factorization and primality testing, Springer-Verlag.

Brickell, E.F. ve Odlyzko, A.M., (1988), Cryptanalysis : A survey of recent results, Proceedings of the IEEE, Cilt 76, No 5.

Chang, C.C. ve Lee, H.C., (1993), "A new generalized group-oriented cryptoscheme without trusted centers", IEEE Journal on Selected Areas in Communications, Cilt 11, No 5.

Chapra, S.C. ve Canale, R.P., (1988), Numerical methods for engineers, McGraw-Hill.

Cohen, H. ve Lenstra, A. K., (1987), "Implementation of a new primality test", Math. Comput., Cilt 48, No 177, Sayfa 103-121.

Cohen, H. ve Lenstra, H. W., (1984), "Primality testing and Jacobi sums", Math. Comput., Cilt 42, No 165, Sayfa 297-330.

Cormen, T.H., Leiserson, Charles E. ve Rivest, R.L., (1988), Introduction to algorithms, McGraw-Hill.

Davies, D., (1981), Tutorial : The Security of data in networks, IEEE Computer Society.

Denning, D.E., (1993), Cryptography and Data Security, ikinci baskı, Addison-Wesley.

Diffie, W. ve Hellman, M.E., (1976), "New directions in cryptography", IEEE Transactions on Information Theory IT-22, Sayfa 644-654.

El Gamal, T., (1985), "A public-key cryptosistem and a signature ccheme based on discrete logarithms", Advances in Cryptology: Proceedings of CRYPTO 84, Springer-Verlag.

Fabrykowski, J., (1994), "On quadratic residues and nonResidues in difference sets modulo m", Proceedings of the American Mathematical Society, Cilt 122, No 2.

Hwang, T., (1992), "Protocols for group oriented secret writing, Information processing letters", No 42, Sayfa 179-182.

Johnsonbaugh, R., (1993), Discrete Mathematics, Mac Millan.

Karakaş, H. İ. ve Aliyev, İ., (1996), Sayılar teorisinde ilginç olimpiyat problemleri ve çözümleri, TUBİTAK.

Kemmerer, R. A., (1988), "Analyzing encription protocols using formal verification techniques", IEEE Journal on selected areas in communications, Cilt 7, No 4.

Knuth, D. E., (1981), "The art of computer programming", ikinci baskı, Addison-Wesley.

Koblitz, N., (1987), A course in number theory and cryptography, Springer-Verlag.

Kranakis, E., (1986), Primality and cryptography, John Wiley & Sons.

Lehmann, D. J., (1982), "On primality tests", SIAM J. Comput., Cilt 11, No 2, Sayfa 374-375.

Lu, W.P. ve Sundareshan, M.K., (1992), "Enhanced protocols for hierarchical encryption key management for secure communication in internet environments", IEEE Transactions on Communications, Cilt 40, No 4.

Massey, J. L. (1988), "An introduction to contemporary cryptology", Proceedings of the IEEE, Cilt 76, No 5.

Miller, G. L., (1976), "Riemann's hypothesis and tests for primality", J. Comput. Syst. Sci., Cilt 13, No 3, Sayfa 300-317.

Niven, I., Zuckerman, H.S. ve Montgomery, H.L., (1991), "An introduction to the theory of numbers", John Wiley & Sons.

Pohlig, S. C. ve Hellman, M. E., (1978) "An improved algorithm for computing logarithms over GF(p) and its cryptographic significance", IEEE Transactions on Information Theory , Cilt IT-24, No 1, Sayfa 106-110.

Rabin, M.O., (1980), "Probabilistic algorithms for testing primality", J. Number Theory, No 12, Sayfa 128-138.

Rose, K.H. ve Wright, C. R. B., (1995), Discrete mathematics, ikinci baskı, Prentice-Hall.

Rivest, R. L., Shamir, A. ve Adleman, L.M., (1978), "A method for obtaining digital signatures and public key cryptosystems", Communications of the ACM, Cilt 21, Sayfa 120-126.

Salomaa, A., (1990), Public-Key Cryptography, Springer-Verlag.

Salomaa, A., (1985), Computation and automata, Cambridge University Press.

Schneier, B., (1996), Applied cryptography, ikinci baskı, Wiley.

Schumely, Z., "Composite Diffie-Hellman public-key generating systems are hard to break", Technion-Israel Institute of Technology, Technical Report #356

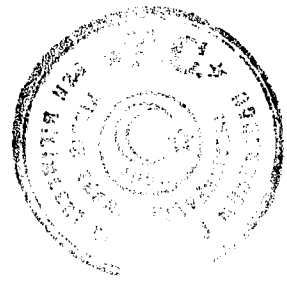
Seberry, J. ve Pieprzyk, J., (1989), Cryptography: An introduction to computer security, Prentice Hall.

Simmons, G. J., (1979), "Symmetric and asymmetric encryption", ACM Comput. Surveys, Cilt 11, No 4, Sayfa 305-330.

Stinson, D.R., (1996), Cryptography, CRC Press.

Turing, A., (1936), "On computable numbers, with an application to the Entscheidungs-problem", Proc. London Math. Soc. Ser. 2, Cilt 42 Sayfa 230-265.

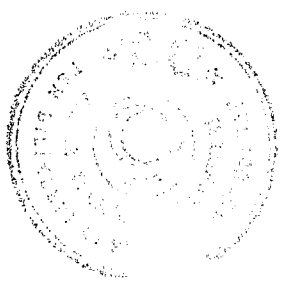
Wilf, H.S., (1992), Algorithms and complexity, Prentice-Hall



Ek-A
p=7 q=11 n=77 $\phi(n)=60$
Ardışık kareler ve tersleri mod $\phi(n)$

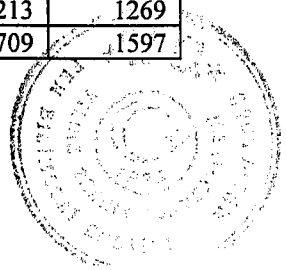
c	c^{-1}	c^{2}	c^{-2}	c^{4}	c^{-4}	c^{8}	c^{-8}
2							
3							
4							
5							
6							
7							
8							
9							
10							
11	11						
12							
13	37						
14							
15							
16							
17	53						
18							
19	19	53	17	37	13		
20							
21							
22							
23	47	67	43	23	47	67	43
24							
25							
26							
27							
28							
29	29	71	11				
30							
31	31	37	13				
32							
33							
34							
35							
36							
37	13						
38							

c	c^{-1}	c^{2}	c^{-2}	c^{4}	c^{-4}	c^{8}	c^{-8}
39							
40							
41	41						
42							
43	7						
44							
45							
46							
47	23	53	17	37	13		
48							
49	49						
50							
51							
52							
53	17	37	13				
54							
55							
56							
57							
58							
59	59						
60							
61	1						
62							
63							
64							
65							
66							
67	43	23	47	67	43	23	47
68							
69							
70							
71	11						
72							
73	37						
74							
75							

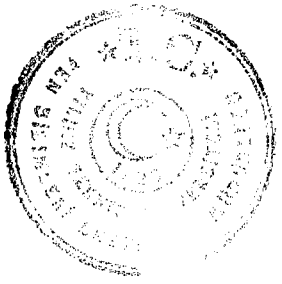


Ek-B
u(p=47, q=53, s=4)

Sıra No	c	c^{-1}	c^{2}	c^{-2}	c^{4}	c^{-4}	c^{8}	c^{-8}
1	81	945	1579	1883	2241	697	225	1297
2	111	431	2357	205	519	1143	333	941
3	177	473	1437	1861	2421	165	2409	985
4	205	2357	2169	1137	1553	1129	521	1561
5	227	843	1709	1597	1229	1341	895	1943
6	257	121	1283	1251	2029	1509	1709	1597
7	303	1271	2133	157	1123	2179	683	795
8	363	883	2237	1821	2241	697	225	1297
9	369	1841	1647	1615	2401	1329	627	763
10	383	687	2211	859	1179	211	63	1215
11	407	335	1243	2163	629	1061	2063	887
12	449	1497	2321	977	1499	75	119	2191
13	459	1011	1437	1861	2421	165	2409	985
14	491	1291	1945	1097	1687	95	1247	727
15	511	543	2057	1985	1531	1603	2421	165
16	519	1143	333	941	1285	981	2183	103
17	571	155	2211	859	1179	211	63	1215
18	579	1731	1447	2311	1369	2233	929	2065
19	595	1395	303	1271	2133	157	1123	2179
20	605	1965	2339	1715	685	653	917	613
21	617	1857	2057	1985	1531	1603	2421	165
22	625	1041	2029	1509	1709	1597	1229	1341
23	641	153	2357	205	519	1143	333	941
24	711	471	2339	1715	685	653	917	613
25	735	1471	2169	1137	1553	1129	521	1561
26	745	777	2023	551	2307	2195	1473	2025
27	783	1335	303	1271	2133	157	1123	2179
28	815	2031	1619	1835	629	1061	2063	887
29	821	1853	1471	735	1653	2269	2273	201
30	927	2103	2425	145	1865	817	789	861
31	945	81	1247	727	625	1041	2029	1509
32	971	2291	1243	2163	629	1061	2063	887
33	979	2155	1897	1585	1605	1389	331	1467
34	1021	1237	1203	171	2429	1293	1353	937
35	1089	1889	205	2357	2169	1137	1553	1129
36	1121	2089	1177	2329	333	941	1285	981
37	1141	1109	1579	1883	2241	697	225	1297
38	1177	2329	333	941	1285	981	2183	103
39	1203	171	2429	1293	1353	937	2215	1919
40	1215	63	1553	1129	521	1561	2413	1253
41	1243	2163	629	1061	2063	887	1341	1229
42	1247	727	625	1041	2029	1509	1709	1597
43	1279	879	1745	1257	1023	159	309	1525
444	1283	1251	2029	1509	1709	1597	1229	1341
45	1323	1083	1647	1615	2401	1329	627	763
46	1421	101	1531	1603	2421	165	2409	985
47	1423	2039	2237	1821	2241	697	225	1297
48	1447	2311	1369	2233	929	2065	1155	1371
49	1483	1171	2227	2363	2439	967	213	1269
50	1529	2137	1283	1251	2029	1509	1709	1597



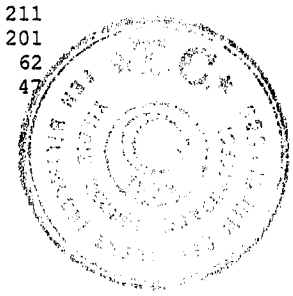
51	1591	1087	425	1953	1273	233	1379	1379
52	1619	1835	629	1061	2063	887	1341	1229
53	1627	1307	1687	95	1247	727	625	1041
54	1639	1223	1023	159	309	1525	823	1895
55	1671	1055	2321	977	1499	75	119	2191
56	1687	95	1247	727	625	1041	2029	1509
57	1699	107	2023	551	2307	2195	1473	2025
58	1715	2339	1845	1325	1319	1935	1043	555
59	1745	1257	1023	159	309	1525	823	1895
60	1779	1475	1271	303	1273	233	1379	1379
61	1845	1325	1319	1935	1043	555	1773	541
62	1853	821	1011	459	811	1867	97	1233
63	1927	607	1739	1707	47	967	2209	2209
64	1941	1973	1089	1889	205	2357	2169	1137
65	1945	1097	1687	95	1247	727	625	1041
66	1987	2203	2425	145	1865	817	789	861
67	2029	1509	1709	1597	1229	1341	895	1943
68	2057	1985	1531	1603	2421	165	2409	985
69	2075	83	1177	2329	333	941	1285	981
70	2081	1769	1203	171	2429	1293	1353	937
71	2169	1137	1553	1129	521	1561	2413	1253
72	2177	89	1447	2311	1369	2233	929	2065
73	2193	601	1619	1835	629	1061	2063	887
74	2201	2129	1897	1585	1605	1389	331	1467
75	2219	1355	1745	1257	1023	159	309	1525
76	2227	2363	2439	967	213	1269	531	955
77	2341	469	81	945	1579	1883	2241	697
78	2357	205	519	1143	333	941	1285	981
79	2371	1139	1945	1097	1687	95	1247	727
80	2423	463	2133	157	1123	2179	683	795
81	2437	1701	425	1953	1273	233	1379	1379



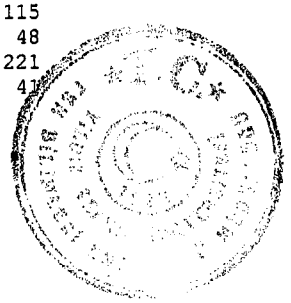
Ek-C1-13

$U(p,q,s)$ ve $U_o(p,q,s)$; $p=P_{13}$, $q \in \{P_{13}..P_{212}\}$, $s \in \{1..4\}$

				s							
				1		2		3		4	
p	q	n	fiofn	U	Uo	U	Uo	U	Uo	U	Uo
41	41	1681	1600	656	3902	245	1457	99	588	38	226
41	43	1763	1680	393	2229	92	521	25	141	8	45
41	47	1927	1840	719	3731	265	1375	93	482	37	192
41	53	2173	2080	786	3617	281	1293	84	386	36	165
41	59	2419	2320	915	3782	369	1525	152	628	64	264
41	61	2501	2400	652	2606	157	627	40	159	8	31
41	67	2747	2640	653	2377	153	556	34	123	10	36
41	71	2911	2800	979	3363	319	1095	114	391	45	154
41	73	2993	2880	783	2616	208	694	55	183	23	76
41	79	3239	3120	783	2417	174	537	44	135	7	21
41	83	3403	3280	1306	3837	496	1457	215	631	107	314
41	89	3649	3520	1304	3573	455	1246	162	443	58	158
41	97	3977	3840	1043	2622	267	671	64	160	12	30
41	101	4141	4000	1630	3936	623	1504	269	649	107	258
41	103	4223	4080	1044	2472	235	556	55	130	11	26
41	107	4387	4240	1696	3865	641	1461	240	547	69	157
41	109	4469	4320	1174	2626	313	700	95	212	25	55
41	113	4633	4480	1565	3377	501	1081	157	338	59	127
41	127	5207	5040	1172	2250	250	480	53	101	13	24
41	131	5371	5200	1955	3639	722	1344	269	500	97	180
41	137	5617	5440	2086	3713	774	1377	292	519	105	186
41	139	5699	5520	1434	2516	365	640	68	119	19	33
41	149	6109	5920	2347	3841	862	1411	302	494	112	183
41	151	6191	6000	1629	2631	393	634	97	156	31	50
41	157	6437	6240	1563	2428	399	619	96	149	34	52
41	163	6683	6480	1760	2633	477	713	121	181	37	55
41	167	6847	6640	2672	3902	1028	1501	410	598	166	242
41	173	7093	6880	2738	3860	1043	1470	430	606	192	270
41	179	7339	7120	2868	3907	1140	1553	459	625	196	267
41	181	7421	7200	1955	2634	530	714	165	222	60	80
41	191	7831	7600	2934	3746	1046	1335	370	472	122	155
41	193	7913	7680	2087	2637	549	693	134	169	45	56
41	197	8077	7840	2737	3388	924	1143	325	402	104	128
41	199	8159	7920	1955	2396	434	531	90	110	13	15
41	211	8651	8400	1956	2261	409	472	102	117	30	34
41	223	9143	8880	2348	2568	579	633	130	142	25	27
41	227	9307	9040	3651	3922	1421	1526	547	587	208	223
41	229	9389	9120	2347	2499	581	618	153	162	41	43
41	233	9553	9280	3652	3822	1386	1450	525	549	212	221
41	239	9799	9520	3131	3195	959	978	288	293	83	84
41	241	9881	9600	2608	2639	676	684	154	155	35	35
41	251	10291	10000	4076	3960	1636	1589	623	605	265	257
41	257	10537	10240	4173	3960	1614	1531	632	599	267	253
41	263	10783	10480	4238	3930	1658	1537	649	601	256	237
41	269	11029	10720	4304	3902	1647	1493	633	573	236	213
41	271	11111	10800	2934	2640	742	667	185	166	49	44
41	277	11357	11040	2869	2526	737	648	194	170	53	46
41	281	11521	11200	3914	3397	1314	1140	419	363	141	122
41	283	11603	11280	3001	2586	794	684	185	159	34	29
41	293	12013	11680	4696	3909	1812	1508	755	628	310	258
41	307	12587	12240	3129	2485	781	620	197	156	60	47
41	311	12751	12400	4892	3836	1861	1459	718	563	299	234
41	313	12833	12480	3131	2439	731	569	174	135	27	21
41	317	12997	12640	5087	3913	1984	1526	786	604	316	243
41	331	13571	13200	3260	2402	786	579	174	128	30	22
41	337	13817	13440	3130	2265	728	526	170	123	37	26
41	347	14227	13840	5610	3943	2203	1548	885	622	364	255
41	349	14309	13920	3652	2552	911	636	221	154	65	45
41	353	14473	14080	5219	3606	1863	1287	684	472	306	211
41	359	14719	14320	5806	3944	2206	1498	828	562	296	201
41	367	15047	14640	3915	2601	993	659	291	193	94	62
41	373	15293	14880	3914	2559	1027	671	268	175	73	47



41	379	15539	15120	3523	2267	793	510	188	120	36	23
41	383	15703	15280	6198	3947	2422	1542	907	577	346	220
41	389	15949	15520	6264	3927	2388	1497	872	546	304	190
41	397	16277	15840	3915	2405	963	591	232	142	70	43
41	401	16441	16000	6525	3968	2595	1578	999	607	355	215
41	409	16769	16320	4176	2490	1032	615	251	149	63	37
41	419	17179	16720	5872	3418	2028	1180	768	447	302	175
41	421	17261	16800	3916	2268	903	523	183	106	31	17
41	431	17671	17200	6853	3878	2560	1448	957	541	344	194
41	433	17753	17280	4699	2646	1262	710	367	206	81	45
41	439	17999	17520	4699	2610	1171	650	301	167	77	42
41	443	18163	17680	6265	3449	2135	1175	701	385	239	131
41	449	18409	17920	6265	3403	2092	1136	701	380	215	116
41	457	18737	18240	4699	2507	1123	599	283	151	83	44
41	461	18901	18400	7179	3798	2705	1431	1024	541	404	213
41	463	18983	18480	3915	2062	763	401	148	77	25	13
41	467	19147	18640	7570	3953	2972	1552	1183	617	476	248
41	479	19639	19120	7766	3954	3001	1528	1190	605	457	232
41	487	19967	19440	5286	2647	1354	678	360	180	101	50
41	491	20131	19600	6853	3404	2352	1168	824	409	308	152
41	499	20459	19920	5353	2616	1401	684	366	178	80	39
41	503	20623	20080	8158	3955	3205	1554	1266	613	478	231
41	509	20869	20320	8224	3940	3198	1532	1202	575	468	224
41	521	21361	20800	7833	3666	2835	1327	1011	473	362	169
41	523	21443	20880	5482	2556	1384	645	348	162	91	42
41	541	22181	21600	5875	2648	1539	693	379	170	82	36
41	547	22427	21840	4698	2094	975	434	225	100	55	24
41	557	22837	22240	9009	3944	3526	1543	1408	616	583	255
41	563	23083	22480	9139	3959	3554	1539	1366	591	507	219
41	569	23329	22720	9140	3917	3598	1542	1378	590	507	217
41	571	23411	22800	5874	2509	1470	627	359	153	86	36
41	577	23657	23040	6267	2649	1629	688	397	167	89	37
41	587	24067	23440	9531	3960	3766	1564	1452	603	569	236
41	593	24313	23680	9402	3867	3566	1466	1368	562	527	216
41	599	24559	23920	8618	3509	2968	1208	1023	416	351	142
41	601	24641	24000	6529	2649	1694	687	428	173	102	41
41	607	24887	24240	6530	2623	1673	672	404	162	113	45
41	613	25133	24480	6268	2493	1590	632	391	155	103	40
41	617	25297	24640	7834	3096	2387	943	735	290	200	79
41	619	25379	24720	6661	2624	1742	686	458	180	109	42
41	631	25871	25200	5877	2271	1279	494	289	111	61	23
41	641	26281	25600	10447	3975	4151	1579	1626	618	644	245
41	643	26363	25680	6923	2626	1871	709	488	185	135	51
41	647	26527	25840	9403	3544	3295	1242	1158	436	436	164
41	653	26773	26080	10578	3950	4177	1560	1590	593	643	240
41	659	27019	26320	9012	3335	3091	1144	1007	372	346	128
41	661	27101	26400	6529	2409	1529	564	366	135	93	34
41	673	27593	26880	6270	2272	1414	512	325	117	85	30
41	677	27757	27040	10187	3670	3754	1352	1378	496	513	184
41	683	28003	27280	9796	3498	3454	1233	1217	434	433	154
41	691	28331	27600	7182	2535	1805	637	438	154	105	37
41	701	28741	28000	9796	3408	3334	1160	1164	404	370	128
41	709	29069	28320	7575	2605	1975	679	518	178	143	49
41	719	29479	28720	11689	3965	4540	1540	1715	581	594	201
41	727	29807	29040	7184	2410	1670	560	401	134	101	33
41	733	30053	29280	7838	2608	2048	681	575	191	159	52
41	739	30299	29520	7836	2586	2079	686	517	170	117	38
41	743	30463	29680	10189	3344	3386	1111	1181	387	409	134
41	751	30791	30000	8163	2651	2079	675	512	166	128	41
41	757	31037	30240	7053	2272	1608	518	387	124	99	31
41	761	31201	30400	11757	3768	4378	1403	1644	526	621	199
41	769	31529	30720	8360	2651	2205	699	600	190	181	57
41	773	31693	30880	12540	3956	4930	1555	1877	592	711	224
41	787	32267	31440	8492	2631	2294	710	635	196	210	65
41	797	32677	31840	12932	3957	5096	1559	1970	602	804	246
41	809	33169	32320	13064	3938	5143	1550	2039	614	741	223
41	811	33251	32400	8817	2651	2307	693	603	181	148	44
41	821	33661	32800	13065	3881	5168	1535	2084	619	888	263
41	823	33743	32880	8885	2633	2299	681	586	173	143	42
41	827	33907	33040	11365	3351	3810	1123	1242	366	390	115
41	829	33989	33120	8622	2536	2171	638	603	177	164	48
41	839	34399	33520	13652	3968	5289	1537	2029	589	762	221
41	853	34973	34080	9147	2615	2455	701	671	191	146	41

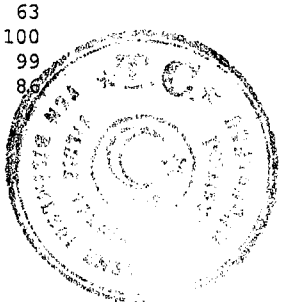


41	857	35137	34240	13850	3941	5376	1530	2088	594	834	237
41	859	35219	34320	7838	2225	1761	500	383	108	83	23
41	863	35383	34480	14045	3969	5562	1571	2207	623	888	250
41	877	35957	35040	9408	2616	2492	693	667	185	156	43
41	881	36121	35200	13065	3617	4704	1302	1694	468	626	173
41	883	36203	35280	8232	2273	1924	531	432	119	80	22
41	887	36367	35440	14437	3969	5747	1580	2279	626	928	255
41	907	37187	36240	9801	2635	2567	690	683	183	184	49
41	911	37351	36400	11759	3148	3629	971	1100	294	341	91
41	919	37679	36720	9407	2496	2253	597	538	142	114	30
41	929	38089	37120	14633	3841	5592	1468	2118	556	826	216
41	937	38417	37440	9408	2448	2348	611	614	159	174	45
41	941	38581	37600	15028	3895	5814	1506	2271	588	879	227
41	947	38827	37840	13721	3533	4848	1248	1692	435	622	160
41	953	39073	38080	12544	3210	4071	1041	1343	343	434	111
41	967	39647	38640	8621	2174	1792	451	376	94	77	19
41	971	39811	38800	15681	3938	6182	1552	2466	619	1018	255
41	977	40057	39040	15682	3914	6129	1530	2398	598	979	244
41	983	40303	39280	16008	3971	6313	1566	2594	643	1065	264
41	991	40631	39600	9800	2411	2305	567	553	136	156	38
41	997	40877	39840	10716	2621	2808	686	742	181	218	53
41	1009	41369	40320	9408	2274	2069	500	494	119	139	33
41	1013	41533	40480	14375	3461	4992	1201	1709	411	602	144
41	1019	41779	40720	16596	3972	6634	1587	2652	634	1089	260
41	1021	41861	40800	10453	2497	2652	633	619	147	131	31
41	1031	42271	41200	16663	3941	6469	1530	2464	582	903	213
41	1033	42353	41280	10977	2591	2818	665	730	172	162	38
41	1039	42599	41520	11240	2638	2906	682	726	170	184	43
41	1049	43009	41920	16991	3950	6659	1548	2605	605	1061	246
41	1051	43091	42000	9802	2274	2206	511	525	121	139	32
41	1061	43501	42400	16991	3905	6606	1518	2554	587	921	211
41	1063	43583	42480	11371	2609	2920	669	734	168	180	41
41	1069	43829	42720	11502	2624	2982	680	806	183	193	44
41	1087	44567	43440	11764	2639	3049	684	764	171	213	47
41	1091	44731	43600	17645	3944	7005	1566	2763	617	1051	234
41	1093	44813	43680	9409	2099	2021	450	421	93	83	18
41	1097	44977	43840	17775	3952	6986	1553	2830	629	1208	268
41	1103	45223	44080	16469	3641	5977	1321	2147	474	748	165
41	1109	45469	44320	18036	3966	7125	1567	2858	628	1117	245
41	1117	45797	44640	11762	2568	3079	672	805	175	227	49
41	1123	46043	44880	10456	2270	2363	513	530	115	131	28
41	1129	46289	45120	12024	2597	3062	661	752	162	159	34
41	1151	47191	46000	17973	3808	6803	1441	2567	543	947	200
41	1153	47273	46080	12549	2654	3326	703	878	185	242	51
41	1163	47683	46480	16078	3371	5442	1141	1889	396	617	129
41	1171	48011	46800	11763	2450	2915	607	726	151	179	37
41	1181	48421	47200	18954	3914	7372	1522	2890	596	1072	221
41	1187	48667	47440	19345	3974	7724	1587	3124	641	1307	268
41	1193	48913	47680	19347	3955	7683	1570	3066	626	1304	266
41	1201	49241	48000	13071	2654	3447	700	933	189	259	52
41	1213	49733	48480	13073	2628	3447	693	906	182	237	47
41	1217	49897	48640	18824	3772	7077	1418	2608	522	907	181
41	1223	50143	48880	18040	3597	6514	1299	2410	480	879	175
41	1229	50389	49120	19999	3968	7852	1558	3145	624	1233	244
41	1231	50471	49200	13071	2589	3358	665	803	159	200	39
41	1237	50717	49440	13334	2629	3558	701	967	190	287	56
41	1249	51209	49920	12550	2450	3045	594	720	140	177	34
41	1259	51619	50320	18826	3647	6956	1347	2607	505	967	187
41	1277	52357	51040	18302	3495	6482	1238	2328	444	803	153
41	1279	52439	51120	13726	2617	3513	669	892	170	243	46
41	1283	52603	51280	20917	3976	8290	1575	3278	623	1280	243
41	1289	52849	51520	17255	3264	5667	1072	1905	360	646	122
41	1291	52931	51600	13725	2592	3577	675	953	180	243	45
41	1297	53177	51840	14118	2654	3756	706	967	181	242	45
41	1301	53341	52000	19609	3676	7281	1364	2703	506	1000	187

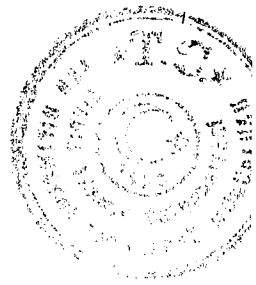
Ek-C1-50

$U(p,q,s)$ ve $U_0(p,q,s)$; $p=P_{50}$, $q \in \{P_{13}..P_{212}\}$, $s \in \{1..4\}$

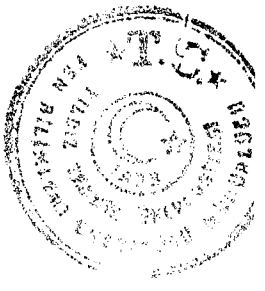
				s							
				1		2		3		4	
p	q	n	fiofn	U	Uo	U	Uo	U	Uo	U	Uo
229	41	9389	9120	2347	2499	581	618	153	162	41	43
229	43	9847	9576	2639	2680	700	710	186	188	50	50
229	47	10763	10488	3218	2989	961	892	290	269	78	72
229	53	12137	11856	3506	2888	1008	830	250	205	56	46
229	59	13511	13224	4083	3021	1192	882	349	258	93	68
229	61	13969	13680	3499	2504	889	636	216	154	53	37
229	67	15343	15048	4370	2848	1241	808	353	230	90	58
229	71	16259	15960	3493	2148	733	450	160	98	35	21
229	73	16717	16416	5238	3133	1589	950	475	284	141	84
229	79	18091	17784	5235	2893	1531	846	451	249	119	65
229	83	19007	18696	5813	3058	1703	895	495	260	175	92
229	89	20381	20064	5812	2851	1687	827	526	258	168	82
229	97	22213	21888	6968	3136	2159	971	661	297	198	89
229	101	23129	22800	5803	2508	1435	620	375	162	104	44
229	103	23587	23256	6965	2952	2089	885	601	254	184	78
229	107	24503	24168	7543	3078	2254	919	670	273	183	74
229	109	24961	24624	7832	3137	2445	979	825	330	287	114
229	113	25877	25536	6960	2689	1859	718	528	204	147	56
229	127	29083	28728	7825	2690	2089	718	517	177	127	43
229	131	29999	29640	6956	2318	1531	510	314	104	62	20
229	137	31373	31008	9271	2955	2721	867	815	259	254	80
229	139	31831	31464	9561	3003	2895	909	833	261	240	75
229	149	34121	33744	10426	3055	3158	925	995	291	330	96
229	151	34579	34200	8688	2512	2241	648	597	172	143	41
229	157	35953	35568	10425	2899	2994	832	878	244	278	77
229	163	37327	36936	11726	3141	3628	971	1081	289	302	80
229	167	38243	37848	11870	3103	3684	963	1141	298	334	87
229	173	39617	39216	12157	3068	3685	930	1093	275	347	87
229	179	40991	40584	12736	3107	3846	938	1171	285	343	83
229	181	41449	41040	10418	2513	2556	616	608	146	147	35
229	191	43739	43320	10996	2514	2745	627	689	157	183	41
229	193	44197	43776	13891	3142	4327	979	1351	305	433	97
229	197	45113	44688	12153	2693	3263	723	812	179	191	42
229	199	45571	45144	13022	2857	3683	808	1072	235	325	71
229	211	48319	47880	10415	2155	2222	459	478	98	107	22
229	223	51067	50616	15621	3058	4786	937	1417	277	395	77
229	227	51983	51528	16199	3116	4983	958	1508	290	477	91
229	229	52441	51984	16488	3144	5182	988	1636	311	522	99
229	233	53357	52896	16198	3035	4988	934	1558	291	455	85
229	239	54731	54264	13883	2536	3541	646	902	164	222	40
229	241	55189	54720	13882	2515	3476	629	855	154	213	38
229	251	57479	57000	14459	2515	3600	626	905	157	243	42
229	257	58853	58368	18507	3144	5843	992	1845	313	627	106
229	263	60227	59736	18797	3121	5876	975	1786	296	498	82
229	269	61601	61104	19084	3098	5899	957	1877	304	604	98
229	271	62059	61560	15616	2516	4017	647	1046	168	269	43
229	277	63433	62928	19085	3008	5812	916	1740	274	491	77
229	281	64349	63840	13878	2156	3057	475	659	102	149	23
229	283	64807	64296	19952	3078	6094	940	1801	277	523	80
229	293	67097	66576	20817	3102	6470	964	2173	323	685	102
229	307	70303	69768	20817	2961	6093	866	1801	256	504	71
229	311	71219	70680	17346	2435	4371	613	1121	157	311	43
229	313	71677	71136	20816	2904	5976	833	1696	236	475	66
229	317	72593	72048	22551	3106	6974	960	2187	301	649	89
229	331	75799	75240	17345	2288	3889	513	859	113	201	26
229	337	77173	76608	20812	2696	5590	724	1524	197	406	52
229	347	79463	78888	24860	3128	7725	972	2402	302	755	95
229	349	79921	79344	24282	3038	7395	925	2233	279	686	85
229	353	80837	80256	23125	2860	6570	812	1790	221	517	63
229	359	82211	81624	25727	3129	8167	993	2603	316	828	100
229	367	84043	83448	26013	3095	8163	971	2618	311	837	99
229	373	85417	84816	26014	3045	7884	923	2395	280	741	86



229	379	86791	86184	23411	2697	6345	731	1713	197	480	55
229	383	87707	87096	27458	3130	8671	988	2756	314	857	97
229	389	89081	88464	27747	3114	8578	962	2594	291	767	86
229	397	90913	90288	26011	2861	7443	818	2056	226	550	60
229	401	91829	91200	23121	2517	5789	630	1406	153	368	40
229	409	93661	93024	27746	2962	8148	869	2413	257	699	74
229	419	95951	95304	27456	2861	7781	810	2205	229	644	67
229	421	96409	95760	20809	2158	4427	459	941	97	201	20
229	431	98699	98040	24276	2459	5871	594	1456	147	386	39
229	433	99157	98496	31213	3147	9702	978	3017	304	933	94
229	439	100531	99864	31212	3104	9549	949	2981	296	917	91
229	443	101447	100776	27743	2734	7578	746	2088	205	574	56
229	449	102821	102144	27743	2698	7451	724	2019	196	564	54
229	457	104653	103968	32946	3148	10385	992	3336	318	1090	104
229	461	105569	104880	25433	2409	6096	577	1448	137	347	32
229	463	106027	105336	26009	2453	6461	609	1556	146	378	35
229	467	106943	106248	33524	3134	10485	980	3310	309	1035	96
229	479	109691	108984	34390	3135	10670	972	3286	299	1064	96
229	487	111523	110808	35112	3148	11109	996	3451	309	1035	92
229	491	112439	111720	24275	2158	5242	466	1079	95	226	20
229	499	114271	113544	35544	3110	11068	968	3428	299	1085	94
229	503	115187	114456	36123	3136	11405	990	3779	328	1287	111
229	509	116561	115824	36412	3123	11352	973	3479	298	1022	87
229	521	119309	118560	27742	2325	6454	540	1455	121	313	26
229	523	119767	119016	36412	3040	11066	923	3361	280	1049	87
229	541	123889	123120	31210	2519	7839	632	2043	164	559	45
229	547	125263	124488	31209	2491	7848	626	1957	156	478	38
229	557	127553	126768	39877	3126	12316	965	3838	300	1150	90
229	563	128927	128136	40456	3137	12736	987	4037	313	1317	102
229	569	130301	129504	40455	3104	12470	957	3878	297	1230	94
229	571	130759	129960	32943	2519	8333	637	2194	167	564	43
229	577	132133	131328	41612	3149	12935	978	3927	297	1224	92
229	587	134423	133608	42190	3138	13231	984	4150	308	1314	97
229	593	135797	134976	41611	3064	12687	934	3889	286	1175	86
229	599	137171	136344	38142	2780	10607	773	2952	215	827	60
229	601	137629	136800	34677	2519	8664	629	2204	160	570	41
229	607	139003	138168	43344	3118	13513	972	4224	303	1283	92
229	613	140377	139536	41609	2964	12348	879	3615	257	1079	76
229	617	141293	140448	34675	2454	8486	600	2105	148	551	38
229	619	141751	140904	44211	3118	13951	984	4379	308	1390	98
229	631	144499	143640	31207	2159	6694	463	1461	101	320	22
229	641	146789	145920	36987	2519	9358	637	2337	159	591	40
229	643	147247	146376	45944	3120	14350	974	4453	302	1414	96
229	647	148163	147288	43921	2964	13135	886	3930	265	1141	77
229	653	149537	148656	46811	3130	14691	982	4669	312	1445	96
229	659	150911	150024	39877	2642	10379	687	2788	184	727	48
229	661	151369	150480	34675	2290	7973	526	1827	120	416	27
229	673	154117	153216	41609	2699	10988	712	2788	180	724	46
229	677	155033	154128	45076	2907	13076	843	3824	246	1112	71
229	683	156407	155496	43343	2771	11972	765	3390	216	921	58
229	691	158239	157320	38144	2410	9109	575	2158	136	510	32
229	701	160529	159600	34674	2159	7440	463	1562	97	324	20
229	709	162361	161424	50277	3096	15612	961	4863	299	1530	94
229	719	164651	163704	51722	3141	16169	982	5046	306	1594	96
229	727	166483	165528	47676	2863	13702	823	3959	237	1102	66
229	733	167857	166896	52010	3098	16031	955	4836	288	1520	90
229	739	169231	168264	52011	3073	16034	947	4962	293	1533	90
229	743	170147	169176	45076	2649	11874	697	3181	186	854	50
229	751	171979	171000	43342	2520	10948	636	2846	165	748	43
229	757	173353	172368	46810	2700	12791	737	3513	202	956	55
229	761	174269	173280	43920	2520	11000	631	2756	158	710	40
229	769	176101	175104	55478	3150	17494	993	5581	316	1803	102
229	773	177017	176016	55478	3134	17247	974	5464	308	1669	94
229	787	180223	179208	56344	3126	17708	982	5561	308	1738	96
229	797	182513	181488	57211	3134	18006	986	5695	312	1808	99
229	809	185261	184224	57789	3119	17956	969	5720	308	1852	99
229	811	185719	184680	46810	2520	11716	630	2914	156	723	38
229	821	188009	186960	46230	2458	11361	604	2889	153	743	39
229	823	188467	187416	58943	3127	18608	987	5765	305	1756	93
229	827	189383	188328	50276	2654	13156	694	3437	181	925	48
229	829	189841	188784	57211	3013	17270	909	5287	278	1650	86
229	839	192131	191064	60390	3143	18824	979	5933	308	1880	97
229	853	195337	194256	60679	3106	18969	971	5935	303	1837	94



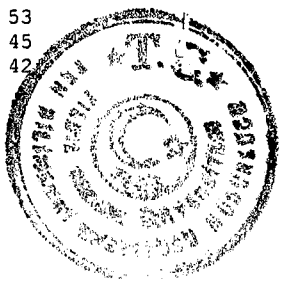
229	857	196253	195168	61257	3121	19215	979	6069	309	1994	101
229	859	196711	195624	52009	2643	13761	699	3650	185	962	48
229	863	197627	196536	62124	3143	19521	987	6143	310	1953	98
229	877	200833	199728	62413	3107	19240	958	6045	300	1948	96
229	881	201749	200640	46232	2291	10570	523	2320	114	525	26
229	883	202207	201096	54611	2700	14704	727	3944	195	1064	52
229	887	203123	202008	63858	3143	20147	991	6436	316	2071	101
229	907	207703	206568	65012	3130	20392	981	6259	301	1870	90
229	911	208619	207480	41608	1994	8261	395	1653	79	335	16
229	919	210451	209304	62411	2965	18415	875	5426	257	1611	76
229	929	212741	211584	64725	3042	19681	925	6017	282	1906	89
229	937	214573	213408	62411	2908	18033	840	5265	245	1514	70
229	941	215489	214320	53165	2467	13083	607	3247	150	794	36
229	947	216863	215688	60679	2798	16944	781	4793	221	1349	62
229	953	218237	217056	55477	2542	14059	644	3505	160	884	40
229	967	221443	220248	57212	2583	14766	666	3852	173	954	43
229	971	222359	221160	55477	2494	13808	620	3447	155	868	39
229	977	223733	222528	69348	3099	21285	951	6536	292	1931	86
229	983	225107	223896	70791	3144	22205	986	6987	310	2178	96
229	991	226939	225720	52010	2291	11997	528	2723	119	611	26
229	997	228313	227088	71082	3113	22150	970	6875	301	2167	94
229	1009	231061	229824	62413	2701	16873	730	4523	195	1227	53
229	1013	231977	230736	63567	2740	17396	749	4839	208	1313	56
229	1019	233351	232104	73392	3145	23049	987	7123	305	2197	94
229	1021	233809	232560	55477	2372	13236	566	3194	136	782	33
229	1031	236099	234840	58946	2496	14740	624	3642	154	921	39
229	1033	236557	235296	72816	3078	22176	937	6575	277	1944	82
229	1039	237931	236664	74548	3133	23416	984	7385	310	2296	96
229	1049	240221	238944	75126	3127	23391	973	7197	299	2219	92
229	1051	240679	239400	52010	2160	11330	470	2435	101	518	21
229	1061	242969	241680	60101	2473	14724	606	3642	149	898	36
229	1063	243427	242136	75417	3098	23417	961	7254	297	2224	91
229	1069	244801	243504	76282	3116	23883	975	7557	308	2391	97
229	1087	248923	247608	78016	3134	24387	979	7708	309	2451	98
229	1091	249839	248520	62412	2498	15437	617	3767	150	923	36
229	1093	250297	248976	62413	2493	15467	617	3790	151	945	37
229	1097	251213	249888	78594	3128	24598	979	7716	307	2446	97
229	1103	252587	251256	76862	3042	23499	930	7135	282	2136	84
229	1109	253961	252624	79751	3140	24789	976	7531	296	2291	90
229	1117	255793	254448	78016	3049	23801	930	7286	284	2237	87
229	1123	257167	255816	69346	2696	18564	721	4958	192	1281	49
229	1129	258541	257184	79751	3084	24655	953	7636	295	2413	93
229	1151	263579	262200	63568	2411	15387	583	3736	141	917	34
229	1153	264037	262656	83218	3151	26191	991	8254	312	2645	100
229	1163	266327	264936	71082	2668	18818	706	4964	186	1277	47
229	1171	268159	266760	62411	2327	14634	545	3404	126	787	29
229	1181	270449	269040	67036	2478	16623	614	4133	152	1045	38
229	1187	271823	270408	85529	3146	26751	984	8297	305	2605	95
229	1193	273197	271776	85529	3130	26585	973	8254	302	2489	91
229	1201	275029	273600	69348	2521	17460	634	4290	155	1038	37
229	1213	277777	276336	86686	3120	27056	974	8507	306	2578	92
229	1217	278693	277248	87841	3151	27682	993	8781	315	2802	100
229	1223	280067	278616	79752	2847	22612	807	6448	230	1915	68
229	1229	281441	279984	88420	3141	27943	992	8661	307	2692	95
229	1231	281899	280440	69349	2460	17018	603	4089	145	965	34
229	1237	283273	281808	88419	3121	27499	970	8524	300	2607	92
229	1249	286021	284544	83218	2909	24331	850	7034	245	1981	69
229	1259	288311	286824	83219	2886	24177	838	6915	239	1931	66
229	1277	292433	290928	80907	2766	22467	768	6252	213	1744	59
229	1279	292891	291384	91021	3107	28165	961	8687	296	2703	92
229	1283	293807	292296	92463	3147	28995	986	8952	304	2752	93
229	1289	295181	293664	76283	2584	19604	664	5010	169	1291	43
229	1291	295639	294120	72816	2463	17912	605	4405	148	1099	37
229	1297	297013	295488	93621	3152	29376	989	9283	312	2891	97
229	1301	297929	296400	69347	2327	16025	537	3651	122	840	28



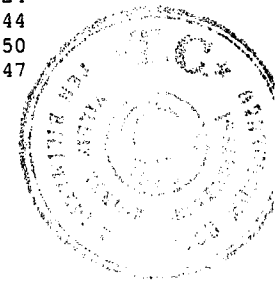
Ek-C1-100

$U(p,q,s)$ ve $U_0(p,q,s)$; $p=P_{100}$, $q \in \{P_{13}..P_{212}\}$, $s \in \{1..4\}$

				s							
				1		2		3		4	
p	q	n	fiofn	U	Uo	U	Uo	U	Uo	U	Uo
541	41	22181	21600	5875	2648	1539	693	379	170	82	36
541	43	23263	22680	5281	2270	1214	521	294	126	64	27
541	47	25427	24840	6444	2534	1692	665	457	179	123	48
541	53	28673	28080	7016	2446	1665	580	395	137	93	32
541	59	31919	31320	8171	2559	2018	632	514	161	123	38
541	61	33001	32400	8751	2651	2320	703	548	166	130	39
541	67	36247	35640	8741	2411	2117	584	526	145	135	37
541	71	38411	37800	8734	2273	2002	521	460	119	106	27
541	73	39493	38880	10478	2653	2716	687	691	174	187	47
541	79	42739	42120	10469	2449	2642	618	694	162	196	45
541	83	44903	44280	11626	2589	2968	660	776	172	202	44
541	89	48149	47520	11620	2413	2764	574	646	134	146	30
541	97	52477	51840	13932	2654	3690	703	936	178	234	44
541	101	54641	54000	14507	2654	3821	699	1008	184	230	42
541	103	55723	55080	13926	2499	3526	632	906	162	231	41
541	107	57887	57240	15082	2605	3782	653	966	166	266	45
541	109	58969	58320	15660	2655	4203	712	1134	192	287	48
541	113	61133	60480	13917	2276	3232	528	741	121	182	29
541	127	68707	68040	15644	2276	3587	522	830	120	218	31
541	131	70871	70200	17379	2452	4157	586	976	137	231	32
541	137	74117	73440	18533	2500	4716	636	1193	160	294	39
541	139	75199	74520	19111	2541	4821	641	1197	159	310	41
541	149	80609	79920	20840	2585	5400	669	1432	177	407	50
541	151	81691	81000	21708	2657	5775	706	1525	186	421	51
541	157	84937	84240	20834	2452	5152	606	1325	155	340	40
541	163	88183	87480	23436	2657	6254	709	1612	182	409	46
541	167	90347	89640	23723	2625	6350	702	1716	189	472	52
541	173	93593	92880	24299	2596	6335	676	1664	177	401	42
541	179	96839	96120	25452	2628	6504	671	1639	169	410	42
541	181	97921	97200	26029	2658	6919	706	1790	182	468	47
541	191	103331	102600	26022	2518	6513	630	1616	156	446	43
541	193	104413	103680	27757	2658	7429	711	1944	186	501	47
541	197	106577	105840	24285	2278	5404	507	1271	119	313	29
541	199	107659	106920	26020	2416	6419	596	1598	148	399	37
541	211	114151	113400	26014	2278	5896	516	1338	117	277	24
541	223	120643	119880	31211	2587	8047	667	2078	172	565	46
541	227	122807	122040	32366	2635	8522	693	2273	185	595	48
541	229	123889	123120	31210	2519	7839	632	2043	164	559	45
541	233	126053	125280	32363	2567	8222	652	2051	162	515	40
541	239	129299	128520	27737	2145	5986	462	1246	96	264	20
541	241	130381	129600	34672	2659	9378	719	2527	193	660	50
541	251	135791	135000	36112	2659	9705	714	2618	192	670	49
541	257	139037	138240	36977	2659	9871	709	2512	180	653	46
541	263	142283	141480	37554	2639	9861	693	2588	181	665	46
541	269	145529	144720	38127	2619	10003	687	2609	179	715	49
541	271	146611	145800	38994	2659	10415	710	2813	191	764	52
541	277	149857	149040	38125	2544	9670	645	2483	165	642	42
541	281	152021	151200	34658	2279	7848	516	1798	118	376	24
541	283	153103	152280	39856	2603	10333	674	2711	177	713	46
541	293	158513	157680	41586	2623	10869	685	2972	187	815	51
541	307	166087	165240	41581	2503	10426	627	2633	158	683	41
541	311	168251	167400	43313	2574	10936	649	2763	164	673	39
541	313	169333	168480	41581	2455	10238	604	2534	149	646	38
541	317	171497	170640	45044	2626	11905	694	3103	180	818	47
541	331	179071	178200	43307	2418	10494	586	2603	145	639	35
541	337	182317	181440	41575	2280	9427	517	2117	116	480	26
541	347	187727	186840	49657	2645	12927	688	3341	177	841	44
541	349	188809	187920	48501	2568	12516	662	3218	170	827	43
541	353	190973	190080	46190	2418	11273	590	2682	140	647	33
541	359	194219	193320	51385	2645	13689	704	3661	188	1036	53
541	367	198547	197640	51960	2617	13506	680	3498	176	903	45
541	373	201793	200880	51960	2574	13242	656	3374	167	863	42



541	379	205039	204120	46762	2280	10701	521	2488	121	582	28
541	383	207203	206280	54845	2646	14534	701	3781	182	983	47
541	389	210449	209520	55420	2633	14376	683	3765	178	992	47
541	397	214777	213840	51954	2418	12741	593	3175	147	783	36
541	401	216941	216000	57726	2660	15486	713	4196	193	1148	52
541	409	221269	220320	55415	2504	13695	618	3383	152	812	36
541	419	226679	225720	51950	2291	11784	519	2695	118	616	27
541	421	227761	226800	51950	2280	11884	521	2638	115	556	24
541	431	233171	232200	60606	2599	15655	671	4026	172	1055	45
541	433	234253	233280	62338	2661	16576	707	4388	187	1243	53
541	439	237499	236520	62337	2624	16325	687	4275	180	1093	46
541	443	239663	238680	55410	2311	12786	533	2941	122	694	28
541	449	242909	241920	55408	2281	12666	521	2900	119	648	26
541	457	247237	246240	62334	2521	15586	630	3921	158	962	38
541	461	249401	248400	63487	2545	16383	656	4225	169	1069	42
541	463	250483	249480	51943	2073	10827	432	2214	88	458	18
541	467	252647	251640	66950	2649	17836	705	4795	189	1286	50
541	479	259139	258120	68680	2650	18261	704	4763	183	1277	49
541	487	263467	262440	70120	2661	18514	702	4909	186	1280	48
541	491	265631	264600	60598	2281	13831	520	3154	118	753	28
541	499	269959	268920	70985	2629	18786	695	4899	181	1310	48
541	503	272123	271080	72139	2650	19062	700	5055	185	1341	49
541	509	275369	274320	72714	2640	19229	698	5112	185	1386	50
541	521	281861	280800	69248	2456	17037	604	4280	151	1089	38
541	523	282943	281880	72713	2569	18650	659	4870	172	1286	45
541	541	292681	291600	77904	2661	20540	701	5523	188	1448	49
541	547	295927	294840	62322	2105	13165	444	2742	92	540	18
541	557	301337	300240	79633	2642	21060	698	5618	186	1502	49
541	563	304583	303480	80787	2652	21584	708	5800	190	1540	50
541	569	307829	306720	80785	2624	20999	682	5541	180	1436	46
541	571	308911	307800	77901	2521	19697	637	4930	159	1146	37
541	577	312157	311040	83092	2661	22219	711	6003	192	1627	52
541	587	317567	316440	84245	2652	22310	702	6010	189	1633	51
541	593	320813	319680	83091	2590	21559	672	5662	176	1507	46
541	599	324059	322920	76166	2350	17948	553	4287	132	977	30
541	601	325141	324000	86552	2661	23155	712	6266	192	1675	51
541	607	328387	327240	86550	2635	22695	691	5992	182	1578	48
541	613	331633	330480	83089	2505	20810	627	5303	159	1344	40
541	617	333797	332640	69240	2074	14308	428	2954	88	612	18
541	619	334879	333720	88281	2636	23291	695	6196	185	1660	49
541	631	341371	340200	77894	2281	17792	521	4023	117	895	26
541	641	346781	345600	92317	2662	24478	705	6427	185	1632	47
541	643	347863	346680	91739	2637	24082	692	6317	181	1650	47
541	647	350027	348840	83085	2373	19685	562	4622	132	1149	32
541	653	353273	352080	93470	2645	24480	692	6477	183	1722	48
541	659	356519	355320	79621	2233	17629	494	3932	110	925	25
541	661	357601	356400	86546	2420	20771	580	4955	138	1202	33
541	673	364093	362880	83082	2281	19041	522	4348	119	1025	28
541	677	366257	365040	90006	2457	22128	604	5401	147	1310	35
541	683	369503	368280	86545	2342	20332	550	4753	128	1088	29
541	691	373831	372600	95198	2546	24178	646	6028	161	1517	40
541	701	379241	378000	86542	2281	19795	521	4520	119	1081	28
541	709	383569	382320	100388	2617	26250	684	6819	177	1804	47
541	719	388979	387720	103272	2654	27227	699	7156	183	1913	49
541	727	393307	392040	95194	2420	22899	582	5457	138	1330	33
541	733	396553	395280	103847	2618	27086	683	7109	179	1876	47
541	739	399799	398520	103847	2597	27138	678	7047	176	1897	47
541	743	401963	400680	90000	2239	20098	499	4521	112	1048	26
541	751	406291	405000	108175	2662	28734	707	7549	185	1999	49
541	757	409537	408240	93463	2282	21257	519	4838	118	1091	26
541	761	411701	410400	103846	2522	26030	632	6488	157	1617	39
541	769	416029	414720	110769	2662	29575	710	8052	193	2168	52
541	773	418193	416880	110770	2648	29246	699	7759	185	1996	47
541	787	425767	424440	112498	2642	29779	699	7976	187	2092	49
541	797	431177	429840	114229	2649	30130	698	7840	181	2052	47
541	809	437669	436320	115379	2636	30083	687	7859	179	2018	46
541	811	438751	437400	116823	2662	30810	702	8073	183	2069	47
541	821	444161	442800	115380	2597	29839	671	7584	170	1881	42
541	823	445243	443880	117689	2643	31187	700	8215	184	2111	47
541	827	447407	446040	100379	2243	22526	503	5058	113	1114	24
541	829	448489	447120	114227	2546	29494	657	7609	169	1984	44
541	839	453899	452520	120571	2656	32133	707	8594	189	2304	50
541	853	461473	460080	121146	2625	31673	686	8207	177	2176	47

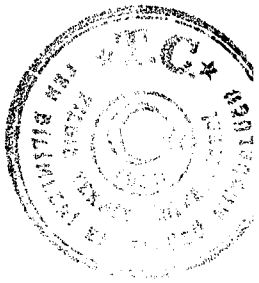


541	857	463637	462240	122299	2637	32643	704	8716	187	2366	51
541	859	464719	463320	103840	2234	23284	501	5180	111	1176	25
541	863	466883	465480	124032	2656	33292	713	8931	191	2368	50
541	877	474457	473040	124606	2626	32632	687	8515	179	2177	45
541	881	476621	475200	115377	2420	27902	585	6838	143	1716	36
541	883	477703	476280	109030	2282	24778	518	5539	115	1240	25
541	887	479867	478440	127491	2656	33750	703	8960	186	2386	49
541	907	490687	489240	129798	2645	34322	699	9035	184	2309	47
541	911	492851	491400	103837	2106	21820	442	4524	91	919	18
541	919	497179	495720	124605	2506	31245	628	7964	160	1981	39
541	929	502589	501120	129219	2571	33030	657	8314	165	2090	41
541	937	506917	505440	124603	2458	30579	603	7602	149	1937	38
541	941	509081	507600	132679	2606	34694	681	9108	178	2380	46
541	947	512327	510840	121141	2364	28546	557	6718	131	1570	30
541	953	515573	514080	110759	2148	23711	459	5012	97	1039	20
541	967	523147	521640	114220	2183	25127	480	5653	108	1252	23
541	971	525311	523800	138447	2635	36730	699	9687	184	2562	48
541	977	528557	527040	138447	2619	36249	685	9606	181	2456	46
541	983	531803	530280	141332	2657	37733	709	9932	186	2666	50
541	991	536131	534600	129792	2420	31392	585	7516	140	1778	33
541	997	539377	537840	141906	2630	37220	690	9711	180	2609	48
541	1009	545869	544320	124601	2282	28393	520	6545	119	1422	26
541	1013	548033	546480	126907	2315	29378	536	6934	126	1594	29
541	1019	551279	549720	146521	2657	38934	706	10388	188	2792	50
541	1021	552361	550800	138445	2506	34613	626	8623	156	2127	38
541	1031	557771	556200	147097	2637	39004	699	10469	187	2823	50
541	1033	558853	557280	145368	2601	37745	675	9878	176	2591	46
541	1039	562099	560520	148828	2647	39428	701	10480	186	2794	49
541	1049	567509	565920	149980	2642	39408	694	10329	182	2722	47
541	1051	568591	567000	129791	2282	29612	520	6651	116	1484	26
541	1061	574001	572400	149980	2612	38936	678	10252	178	2685	46
541	1063	575083	573480	150557	2618	39442	685	10361	180	2706	47
541	1069	578329	576720	152288	2633	40136	693	10557	182	2820	48
541	1087	588067	586440	155748	2648	41240	701	10907	185	2903	49
541	1091	590231	588600	155747	2638	40866	692	10679	180	2756	46
541	1093	591313	589680	124599	2107	26398	446	5478	92	1111	18
541	1097	593477	591840	156900	2643	41308	696	10790	181	2777	46
541	1103	596723	595080	145363	2436	35270	591	8527	142	2034	34
541	1109	599969	598320	159208	2653	41914	698	10997	183	2905	48
541	1117	604297	602640	155746	2577	40216	665	10331	170	2683	44
541	1123	607543	605880	138440	2278	31661	521	7172	118	1575	25
541	1129	610789	609120	159207	2606	41528	679	10956	179	2843	46
541	1151	622691	621000	158629	2547	40124	644	10239	164	2591	41
541	1153	623773	622080	166129	2663	44650	715	12015	192	3228	51
541	1163	629183	627480	141901	2255	31712	504	7154	113	1626	25
541	1171	633511	631800	155746	2458	38126	601	9246	145	2180	34
541	1181	638921	637200	167281	2618	43701	683	11436	178	2954	46
541	1187	642167	640440	170742	2658	45156	703	11986	186	3227	50
541	1193	645413	643680	170742	2645	45100	698	11890	184	3116	48
541	1201	649741	648000	173049	2663	46276	712	12484	192	3352	51
541	1213	656233	654480	173048	2636	45693	696	12055	183	3208	48
541	1217	658397	656640	166126	2523	41826	635	10501	159	2591	39
541	1223	661643	659880	159205	2406	38341	579	9167	138	2238	33
541	1229	664889	663120	176510	2654	46858	704	12570	189	3338	50
541	1231	665971	664200	173049	2598	44759	672	11574	173	2995	44
541	1237	669217	667440	176508	2637	46506	694	12281	183	3144	46
541	1249	675709	673920	166126	2458	40786	603	10013	148	2484	36
541	1259	681119	679320	166125	2439	40451	593	9922	145	2432	35
541	1277	690857	689040	161508	2337	37752	546	8899	128	2061	29
541	1279	691939	690120	181699	2625	47985	693	12612	182	3252	46
541	1283	694103	692280	184584	2659	49298	710	13177	189	3468	49
541	1289	697349	695520	152279	2183	33170	475	7260	104	1678	24
541	1291	698431	696600	181700	2601	47204	675	12219	174	3187	45
541	1297	701677	699840	186890	2663	49576	706	13170	187	3536	50
541	1301	703841	702000	173046	2458	42245	600	10206	145	2495	35

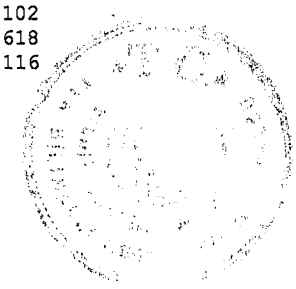
Ek-C1-150

$U(p,q,s)$ ve $U_o(p,q,s)$; $p=P_{150}$, $q \in \{P_{13}..P_{212}\}$, $s \in \{1..4\}$

				s							
				1		2		3		4	
p	q	n	fiofn	U	Uo	U	Uo	U	Uo	U	Uo
863	41	35383	34480	14045	3969	5562	1571	2207	623	888	250
863	43	37109	36204	10522	2835	2944	793	847	228	259	69
863	47	40561	39652	19257	4747	9082	2239	4214	1038	1969	485
863	53	45739	44824	20962	4582	9605	2099	4546	993	2122	463
863	59	50917	49996	24414	4794	11700	2297	5606	1101	2693	528
863	61	52643	51720	13944	2648	3759	714	1021	193	281	53
863	67	57821	56892	17407	3010	5311	918	1642	283	543	93
863	71	61273	60340	20873	3406	7069	1153	2421	395	893	145
863	73	62999	62064	20867	3312	6714	1065	2162	343	682	108
863	79	68177	67236	20848	3057	6344	930	1925	282	579	84
863	83	71629	70684	34728	4848	16823	2348	8172	1140	3930	548
863	89	76807	75856	34706	4518	15644	2036	6979	908	3053	397
863	97	83711	82752	27742	3314	9170	1095	3023	361	1014	121
863	101	87163	86200	34666	3977	13735	1575	5460	626	2191	251
863	103	88889	87924	27728	3119	8643	972	2662	299	812	91
863	107	92341	91372	45045	4878	21915	2373	10656	1153	5147	557
863	109	94067	93096	31180	3314	10284	1093	3399	361	1130	120
863	113	97519	96544	41562	4261	17787	1823	7591	778	3245	332
863	127	109601	108612	31147	2841	8662	790	2477	226	701	63
863	131	113053	112060	41522	3672	15031	1329	5453	482	2003	177
863	137	118231	117232	55347	4681	25978	2197	12094	1022	5554	469
863	139	119957	118956	38047	3171	12154	1013	3893	324	1251	104
863	149	128587	127576	62236	4839	30087	2339	14519	1129	6964	541
863	151	130313	129300	34573	2653	9284	712	2510	192	652	50
863	157	135491	134472	41478	3061	12707	937	4003	295	1278	94
863	163	140669	139644	46655	3316	15439	1097	5197	369	1723	122
863	167	144121	143092	70839	4915	34717	2408	17175	1191	8507	590
863	173	149299	148264	72555	4859	35183	2356	17088	1144	8173	547
863	179	154477	153436	75999	4919	37433	2423	18393	1190	9006	582
863	181	156203	155160	41452	2653	10924	699	2907	186	747	47
863	191	164833	163780	62165	3771	23437	1421	8868	537	3402	206
863	193	166559	165504	55254	3317	18368	1102	6245	374	2128	127
863	197	170011	168952	72515	4265	30875	1816	13280	781	5738	337
863	199	171737	170676	51795	3015	15598	908	4658	271	1352	78
863	211	182093	181020	41427	2275	9441	518	2223	122	506	27
863	223	192449	191364	62129	3228	20276	1053	6605	343	2239	116
863	227	195901	194812	96640	4933	47513	2425	23459	1197	11483	586
863	229	197627	196536	62124	3143	19521	987	6143	310	1953	98
863	233	201079	199984	96632	4805	46663	2320	22471	1117	10869	540
863	239	206257	205156	82820	4015	33237	1611	13516	655	5541	268
863	241	207983	206880	55213	2654	14653	704	3896	187	1090	52
863	251	216613	215500	86259	3982	34390	1587	13603	627	5437	251
863	257	221791	220672	110404	4977	55131	2485	27568	1242	13698	617
863	263	226969	225844	112122	4939	55170	2430	26953	1187	13212	582
863	269	232147	231016	113840	4903	55415	2387	27089	1166	13313	573
863	271	233873	232740	62093	2654	16402	701	4352	186	1104	47
863	277	239051	237912	75886	3174	24031	1005	7545	315	2345	98
863	281	242503	241360	82782	3413	28322	1167	9703	400	3363	138
863	283	244229	243084	79331	3248	25947	1062	8477	347	2728	111
863	293	252859	251704	124161	4910	61021	2413	30041	1188	14879	588
863	307	264941	263772	82765	3123	26082	984	8093	305	2487	93
863	311	268393	267220	103453	3854	40014	1490	15472	576	6003	223
863	313	270119	268944	82761	3063	25360	938	7836	290	2386	88
863	317	273571	272392	134484	4915	65900	2408	32502	1188	16069	587
863	331	285653	284460	68959	2414	16597	581	3975	139	985	34
863	337	290831	289632	82748	2845	23525	808	6633	228	1840	63
863	347	299461	298252	148250	4950	73691	2460	36628	1223	18077	603
863	349	301187	299976	96532	3205	30746	1020	9870	327	3185	105
863	353	304639	303424	137901	4526	62335	2046	28322	929	12841	421
863	359	309817	308596	153411	4951	75846	2448	37469	1209	18700	603
863	367	316721	315492	103418	3265	33642	1062	10865	343	3536	111
863	373	321899	320664	103415	3212	33311	1034	10698	332	3409	105



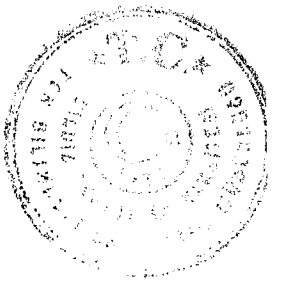
863	379	327077	325836	93070	2845	26333	805	7612	232	2136	65
863	383	330529	329284	163734	4953	80795	2444	40023	1210	19770	598
863	389	335707	334456	165453	4928	81607	2430	40263	1199	19750	588
863	397	342611	341352	103404	3018	31249	912	9611	280	2974	86
863	401	346063	344800	137870	3983	54844	1584	21948	634	8863	256
863	409	352967	351696	110291	3124	34449	975	10788	305	3364	95
863	419	361597	360316	155093	4289	66347	1834	28459	787	12147	335
863	421	363323	362040	82715	2276	18851	518	4372	120	1031	28
863	431	371953	370660	144747	3891	56261	1512	21607	580	8405	225
863	433	373679	372384	124068	3320	41128	1100	13567	363	4362	116
863	439	378857	377556	124065	3274	40418	1066	13063	344	4190	110
863	443	382309	381004	165418	4326	71354	1866	30683	802	13128	343
863	449	387487	386176	165413	4268	70245	1812	29776	768	12767	329
863	457	394391	393072	124058	3145	39011	989	12211	309	3847	97
863	461	397843	396520	151624	3811	57961	1456	22032	553	8410	211
863	463	399569	398244	103379	2587	26784	670	7005	175	1802	45
863	467	403021	401692	199864	4959	98629	2447	48455	1202	23678	587
863	479	413377	412036	205026	4959	101418	2453	49977	1208	24617	595
863	487	420281	418932	139553	3320	46390	1103	15456	367	5195	123
863	491	423733	422380	144719	3415	49287	1163	16970	400	5891	139
863	499	430637	429276	141272	3280	46166	1072	15087	350	4953	115
863	503	434089	432724	215350	4960	106990	2464	53134	1224	26292	605
863	509	439267	437896	217071	4941	107306	2442	52646	1198	25793	587
863	521	449623	448240	165383	3678	60637	1348	22129	492	8081	179
863	523	451349	449964	144709	3206	46366	1027	14859	329	4658	103
863	541	466883	465480	124032	2656	33292	713	8931	191	2368	50
863	547	472061	470652	124029	2627	32386	686	8400	177	2198	46
863	557	480691	479272	237719	4945	117391	2442	57969	1205	28608	595
863	563	485869	484444	241161	4963	119499	2459	59007	1214	29145	599
863	569	491047	489616	241159	4911	118331	2409	58097	1183	28508	580
863	571	492773	491340	124024	2516	31355	636	7985	162	2013	40
863	577	497951	496512	165364	3320	54594	1096	17988	361	5942	119
863	587	506581	505132	251486	4964	124930	2466	62172	1227	30923	610
863	593	511759	510304	248039	4846	120171	2348	58217	1137	28078	548
863	599	516937	515476	227367	4398	100138	1937	44300	856	19738	381
863	601	518663	517200	137798	2656	36518	704	9637	185	2563	49
863	607	523841	522372	172246	3288	56440	1077	18400	351	5997	114
863	613	529019	527544	165354	3125	51853	980	16281	307	5070	95
863	617	532471	530992	206690	3881	80177	1505	31245	586	11937	224
863	619	534197	532716	175688	3288	57373	1074	18772	351	6167	115
863	631	544553	543060	124012	2277	28129	516	6539	120	1492	27
863	641	553183	551680	220462	3985	87718	1585	34764	628	13871	250
863	643	554909	553404	182570	3290	60137	1083	19624	353	6472	116
863	647	558361	556852	248019	4441	110184	1973	48835	874	21583	386
863	653	563539	562024	279018	4951	138207	2452	68376	1213	33944	602
863	659	568717	567196	237680	4179	99320	1746	41739	733	17601	309
863	661	570443	568920	137786	2415	33260	583	8071	141	1994	34
863	673	580799	579264	165340	2846	47113	811	13391	230	3813	65
863	677	584251	582712	268676	4598	123499	2113	56733	971	26087	446
863	683	589429	587884	258340	4382	113096	1918	49478	839	21512	364
863	691	596333	594780	151559	2541	38657	648	9952	166	2569	43
863	701	604963	603400	206668	3416	70248	1161	23968	396	8279	136
863	709	611867	610296	199778	3265	65380	1068	21571	352	7133	116
863	719	620497	618916	308274	4968	153043	2466	75827	1222	37465	603
863	727	627401	625812	189441	3019	56964	907	17111	272	5161	82
863	733	632579	630984	206662	3266	67357	1064	21915	346	7161	113
863	739	637757	636156	206661	3240	67175	1053	21767	341	7022	110
863	743	641209	639604	268657	4189	112556	1755	47472	740	19681	306
863	751	648113	646500	172215	2657	45618	703	12068	186	3189	49
863	757	653291	651672	185992	2847	52859	809	15056	230	4344	66
863	761	656743	655120	247987	3776	93780	1427	35448	539	13595	207
863	769	663647	662016	220432	3321	72934	1098	24111	363	7791	117
863	773	667099	665464	330646	4956	163681	2453	81162	1216	40337	604
863	787	679181	677532	223872	3296	73983	1089	24401	359	8101	119
863	797	687811	686152	340972	4957	168758	2453	83849	1219	41453	602
863	809	698167	696496	344412	4933	169738	2431	83362	1194	41043	587
863	811	699893	698220	185983	2657	49268	703	13267	189	3601	51
863	821	708523	706840	275526	3888	107282	1514	41898	591	16311	230
863	823	710249	708564	234198	3297	77119	1085	25136	353	8281	116
863	827	713701	712012	299634	4198	125496	1758	52347	733	21854	306
863	829	715427	713736	227308	3177	71913	1005	22724	317	7298	102
863	839	724057	722356	359903	4970	179029	2472	89560	1236	44806	618
863	853	736139	734424	241081	3274	78821	1070	25939	352	8557	116



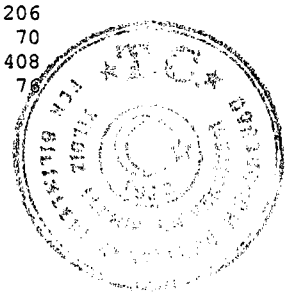
Ek-C1-200

$U(p,q,s)$ ve $U_o(p,q,s)$; $p=P_{200}$, $q \in \{P_{13}..P_{212}\}$, $s \in \{1..4\}$

				s							
				1		2		3		4	
p	q	n	fiofn	U	Uo	U	Uo	U	Uo	U	Uo
1223	41	50143	48880	18040	3597	6514	1299	2410	480	879	175
1223	43	52589	51324	13515	2569	3464	658	950	180	276	52
1223	47	57481	56212	24733	4302	10692	1860	4594	799	1962	341
1223	53	64819	63544	29165	4499	13199	2036	5900	910	2544	392
1223	59	72157	70876	31354	4345	13574	1881	5870	813	2551	353
1223	61	74603	73320	17908	2400	4367	585	1049	140	267	35
1223	67	81941	80652	22355	2728	6039	736	1631	199	442	53
1223	71	86833	85540	26805	3086	8330	959	2598	299	768	88
1223	73	89279	87984	26796	3001	8062	903	2440	273	717	80
1223	79	96617	95316	29003	3001	8672	897	2583	267	823	85
1223	83	101509	100204	44594	4393	19710	1941	8650	852	3727	367
1223	89	108847	107536	44564	4094	18285	1679	7557	694	3142	288
1223	97	118631	117312	35622	3002	10704	902	3274	275	962	81
1223	101	123523	122200	44511	3603	15923	1289	5725	463	2099	169
1223	103	125969	124644	35604	2826	10051	797	2810	223	774	61
1223	107	130861	129532	57836	4419	25518	1950	11290	862	4997	381
1223	109	133307	131976	40036	3003	11952	896	3636	272	1120	84
1223	113	138199	136864	53365	3861	20415	1477	7778	562	2983	215
1223	127	155321	153972	39991	2574	10297	662	2677	172	651	41
1223	131	160213	158860	57752	3604	20512	1280	7348	458	2627	163
1223	137	167551	166192	71061	4241	30063	1794	12753	761	5419	323
1223	139	169997	168636	48850	2873	14121	830	4146	243	1243	73
1223	149	182227	180856	79902	4384	34932	1916	15195	833	6554	359
1223	151	184673	183300	44388	2403	10712	580	2523	136	578	31
1223	157	192011	190632	57691	3004	17360	904	5362	279	1634	85
1223	163	199349	197964	59898	3004	17971	901	5353	268	1608	80
1223	167	204241	202852	90947	4452	40365	1976	17895	876	8078	395
1223	173	211579	210184	93148	4402	40842	1930	17780	840	7739	365
1223	179	218917	217516	97569	4456	43861	2003	19849	906	8939	408
1223	181	221363	219960	53215	2403	12827	579	3119	140	751	33
1223	191	233593	232180	79807	3416	27390	1172	9442	404	3264	139
1223	193	236039	234624	70936	3005	21015	890	6229	263	1875	79
1223	197	240931	239512	93095	3863	36177	1501	14001	581	5475	227
1223	199	243377	241956	66494	2732	18204	747	4969	204	1373	56
1223	211	258053	256620	53181	2060	10948	424	2351	91	513	19
1223	223	272729	271284	79758	2924	23348	856	6786	248	1967	72
1223	227	277621	276172	124061	4468	55459	1997	24669	888	11038	397
1223	229	280067	278616	79752	2847	22612	807	6448	230	1915	68
1223	233	284959	283504	124051	4353	53960	1893	23347	819	10156	356
1223	239	292297	290836	106321	3637	38491	1316	14093	482	5131	175
1223	241	294743	293280	70877	2404	17009	577	4161	141	1063	36
1223	251	306973	305500	110731	3607	39829	1297	14477	471	5187	168
1223	257	314311	312832	141727	4509	63661	2025	28679	912	13001	413
1223	263	321649	320164	143931	4474	64240	1997	28770	894	12948	402
1223	269	328987	327496	146136	4441	64761	1968	28591	869	12542	381
1223	271	331433	329940	79709	2404	19245	580	4628	139	1095	33
1223	277	338771	337272	97416	2875	27824	821	8019	236	2336	68
1223	281	343663	342160	106269	3092	32986	959	10345	301	3277	95
1223	283	346109	344604	104051	3006	31144	899	9266	267	2718	78
1223	293	358339	356824	159385	4447	71170	1986	31570	881	14088	393
1223	307	375461	373932	106244	2829	30197	804	8658	230	2476	65
1223	311	380353	378820	132802	3491	46459	1221	16199	425	5573	146
1223	313	382799	381264	115092	3006	34638	904	10449	272	3096	80
1223	317	387691	386152	172633	4452	76669	1977	34018	877	15085	389
1223	331	404813	403260	88519	2186	19215	474	4165	102	883	21
1223	337	412151	410592	106220	2577	27134	658	6967	169	1822	44
1223	347	424381	422812	190299	4484	85436	2013	38516	907	17511	412
1223	349	426827	425256	123915	2903	36105	845	10602	248	3104	72
1223	353	431719	430144	177016	4100	72404	1677	29452	682	12025	278
1223	359	439057	437476	196923	4485	88321	2011	39453	898	17592	400
1223	367	448841	447252	132751	2957	39067	870	11512	256	3368	75
1223	373	456179	454584	132747	2909	38489	843	11050	242	3162	69

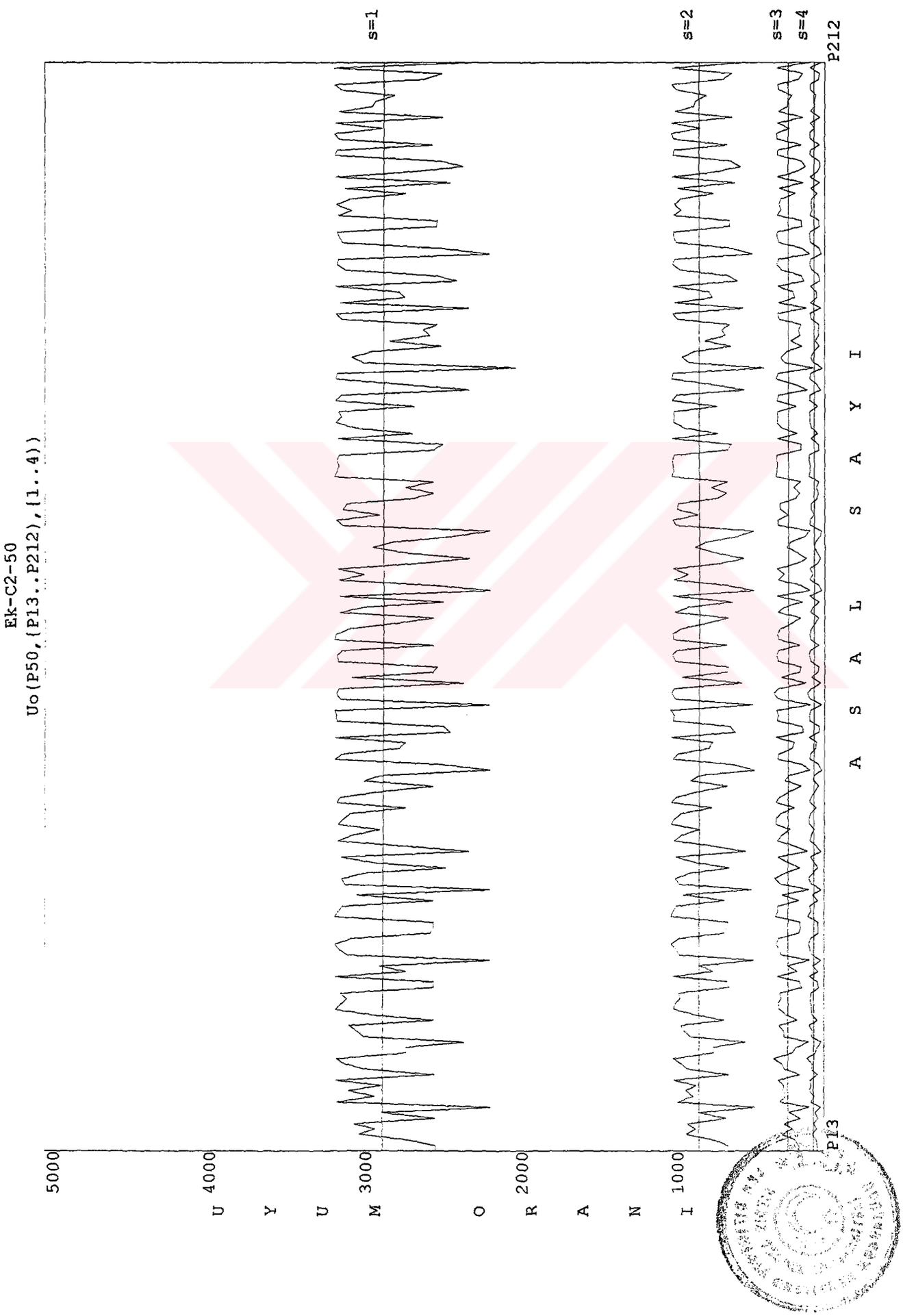


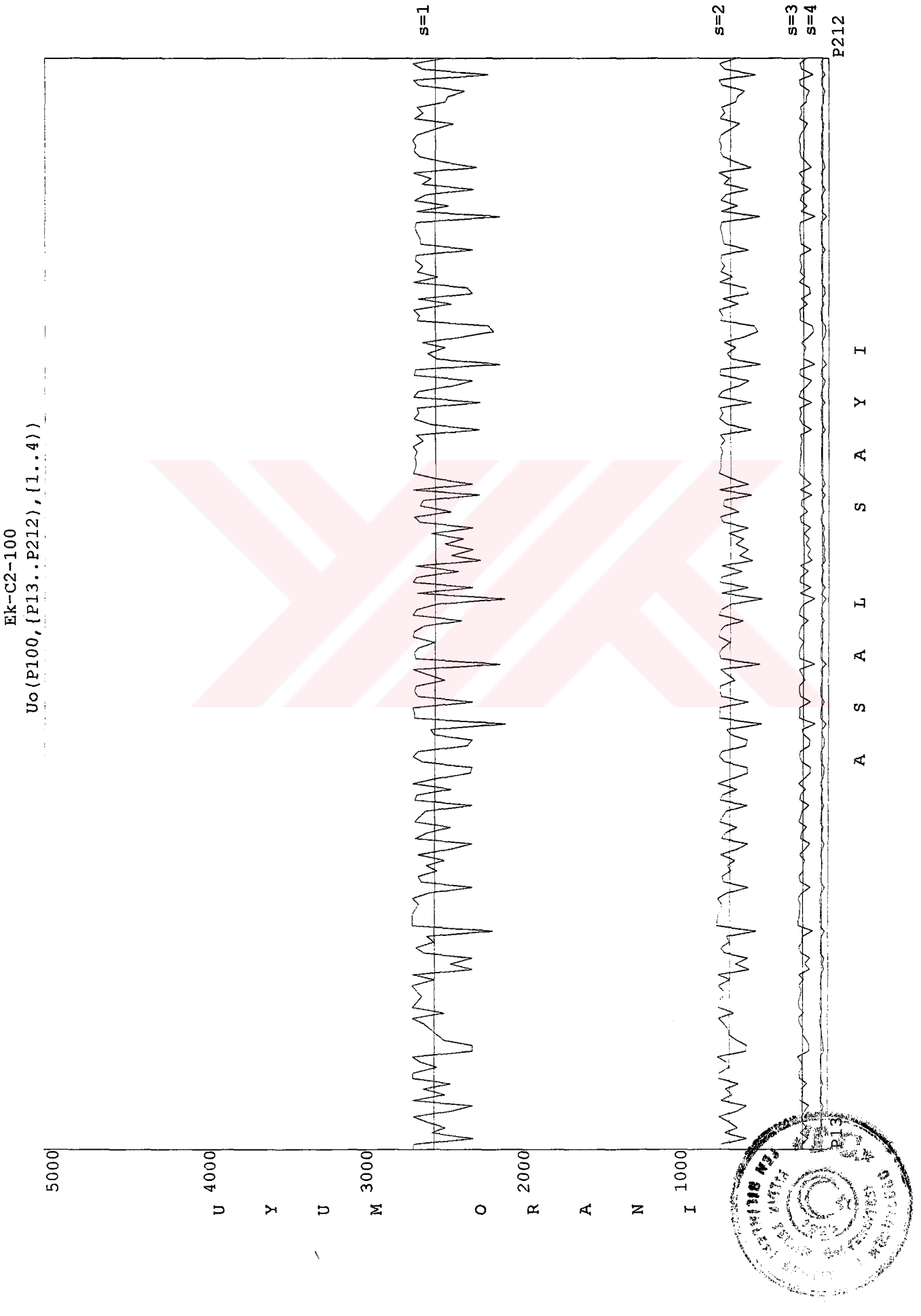
1223	379	463517	461916	119468	2577	30774	663	7875	169	1979	42
1223	383	468409	466804	210172	4486	94426	2015	42183	900	18877	403
1223	389	475747	474136	212380	4464	95138	1999	42785	899	19480	409
1223	397	485531	483912	132733	2733	36015	741	9847	202	2749	56
1223	401	490423	488800	176973	3608	63820	1301	23190	472	8443	172
1223	409	500207	498576	141575	2830	40022	800	11422	228	3330	66
1223	419	512437	510796	199081	3884	77497	1512	30316	591	11628	226
1223	421	514883	513240	106175	2062	22006	427	4612	89	935	18
1223	431	527113	525460	185797	3524	65343	1239	22850	433	7925	150
1223	433	529559	527904	159253	3007	47845	903	14471	273	4407	83
1223	439	536897	535236	159251	2966	47149	878	14000	260	4183	77
1223	443	541789	540124	230026	4245	97497	1799	41237	761	17456	322
1223	449	549127	547456	212328	3866	81720	1488	31473	573	12113	220
1223	457	558911	557232	159241	2849	45406	812	12891	230	3553	63
1223	461	563803	562120	194625	3452	67261	1192	23185	411	8107	143
1223	463	566249	564564	132696	2343	31284	552	7316	129	1709	30
1223	467	571141	569452	256546	4491	115611	2024	52280	915	23632	413
1223	479	585817	584116	263172	4492	117991	2014	52844	902	23651	403
1223	487	595601	593892	179129	3007	53773	902	16144	271	4839	81
1223	491	600493	598780	185761	3093	57339	954	17675	294	5544	92
1223	499	610277	608556	181335	2971	53666	879	15812	259	4625	75
1223	503	615169	613444	276423	4493	124249	2019	55939	909	25028	406
1223	509	622507	620776	278629	4475	124779	2004	56020	899	25136	403
1223	521	637183	635440	229972	3609	82938	1301	30037	471	10982	172
1223	523	639629	637884	185745	2903	53735	840	15579	243	4542	71
1223	541	661643	659880	159205	2406	38341	579	9167	138	2238	33
1223	547	668981	667212	172469	2578	44402	663	11362	169	2830	42
1223	557	681211	679432	305132	4479	136610	2005	60783	892	26976	396
1223	563	688549	686764	309548	4495	138983	2018	62283	904	27697	402
1223	569	695887	694096	309545	4448	137650	1978	61336	881	27307	392
1223	571	698333	696540	159195	2279	36410	521	8262	118	1843	26
1223	577	705671	703872	212255	3007	63748	903	19078	270	5637	79
1223	587	717901	716092	322800	4496	144905	2018	65116	907	29155	406
1223	593	725239	723424	318375	4389	139807	1927	61458	847	26801	369
1223	599	732577	730756	316161	4315	136080	1857	58327	796	24991	341
1223	601	735023	733200	176872	2406	42608	579	10349	140	2491	33
1223	607	742361	740532	221088	2978	65635	884	19665	264	5892	79
1223	613	749699	747864	212241	2831	59817	797	16915	225	4755	63
1223	617	754591	752752	265299	3515	93326	1236	32994	437	11698	155
1223	619	757037	755196	225505	2978	67326	889	19944	263	5951	78
1223	631	771713	769860	159177	2062	32852	425	6857	88	1418	18
1223	641	783943	782080	282976	3609	101809	1298	36475	465	12880	164
1223	643	786389	784524	234340	2979	69635	885	20546	261	6110	77
1223	647	791281	789412	318345	4023	128429	1623	51478	650	20713	261
1223	653	798619	796744	358136	4484	160529	2010	71847	899	32083	401
1223	659	805957	804076	311710	3867	120599	1496	46802	580	18205	225
1223	661	808403	806520	176857	2187	38639	477	8492	105	1857	22
1223	673	823079	821184	212223	2578	54795	665	13901	168	3412	41
1223	677	827971	826072	373599	4512	168397	2033	75675	913	34039	411
1223	683	835309	833404	331596	3969	131749	1577	52226	625	20620	246
1223	691	845093	843180	194532	2301	44954	531	10392	122	2434	28
1223	701	857323	855400	265271	3094	81667	952	25080	292	7520	87
1223	709	867107	865176	256423	2957	75616	872	22387	258	6655	76
1223	719	879337	877396	395682	4499	178272	2027	80125	911	35813	407
1223	727	889121	887172	243155	2734	66543	748	18446	207	5010	56
1223	733	896459	894504	265257	2958	78354	874	23147	258	6836	76
1223	739	903797	901836	265257	2934	77966	862	22943	253	6820	75
1223	743	908689	906724	344833	3794	130774	1439	49590	545	18767	206
1223	751	918473	916500	221045	2406	53546	582	12931	140	3119	33
1223	757	925811	923832	238726	2578	61515	664	15929	172	4138	44
1223	761	930703	928720	318299	3419	108709	1168	37127	398	12866	138
1223	769	940487	938496	282931	3008	84880	902	25639	272	7729	82
1223	773	945379	943384	424395	4489	190491	2014	85339	902	38335	405
1223	787	962501	960492	287348	2985	85572	889	25530	265	7568	78
1223	797	974731	972712	437647	4489	196287	2013	87707	899	39456	404
1223	809	989407	987376	442064	4467	197355	1994	88299	892	39408	398
1223	811	991853	989820	238714	2406	57592	580	14008	141	3415	34
1223	821	1004083	1002040	353648	3522	124416	1239	43902	437	15596	155
1223	823	1006529	1004484	300599	2986	89479	888	26832	266	7920	78
1223	827	1011421	1009372	384588	3802	145794	1441	55313	546	20897	206
1223	829	1013867	1011816	291756	2877	83881	827	24343	240	7135	70
1223	839	1026097	1024036	461945	4501	207929	2026	93413	910	41893	408
1223	853	1043219	1041144	309431	2966	91864	880	27070	259	7970	78

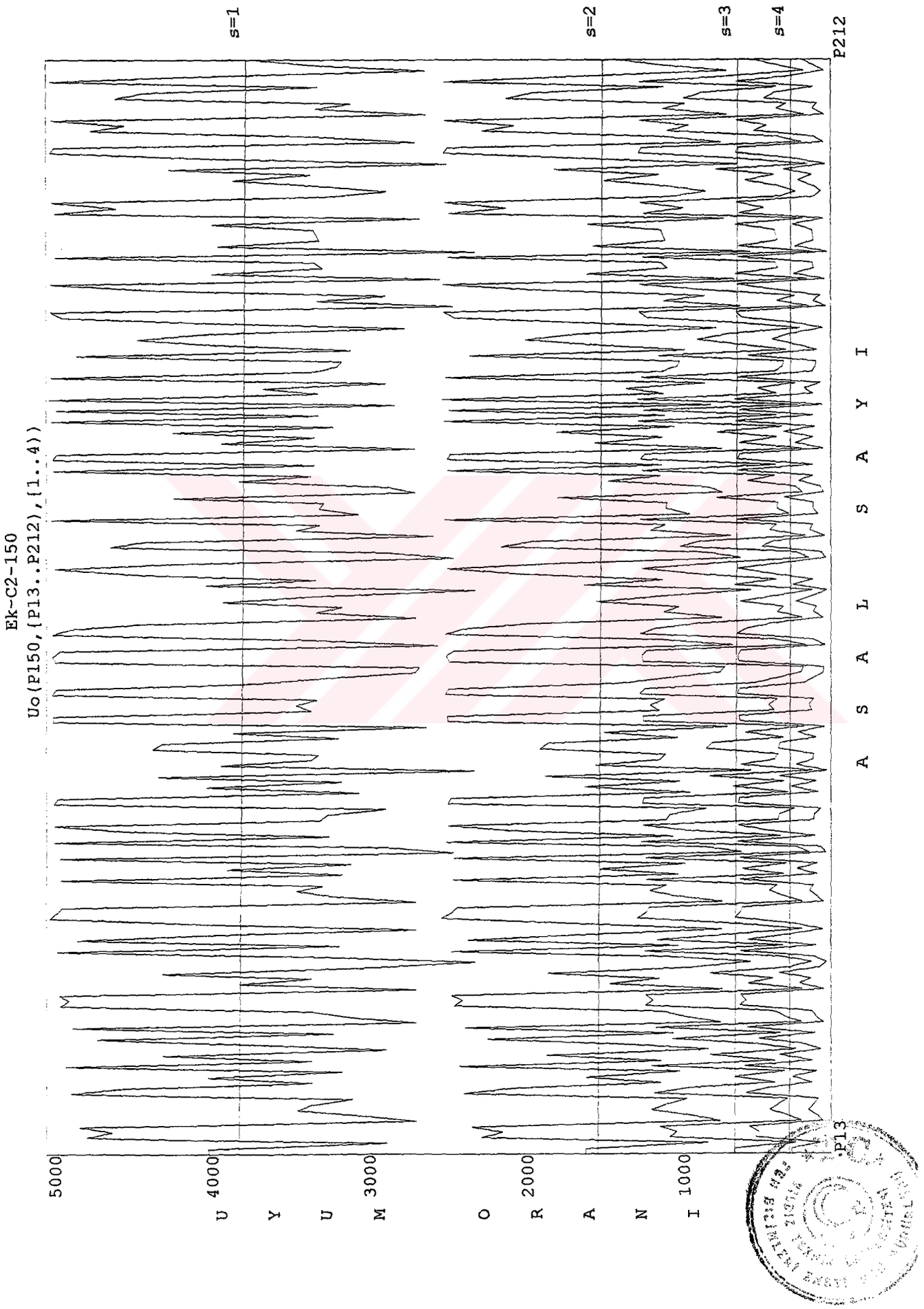


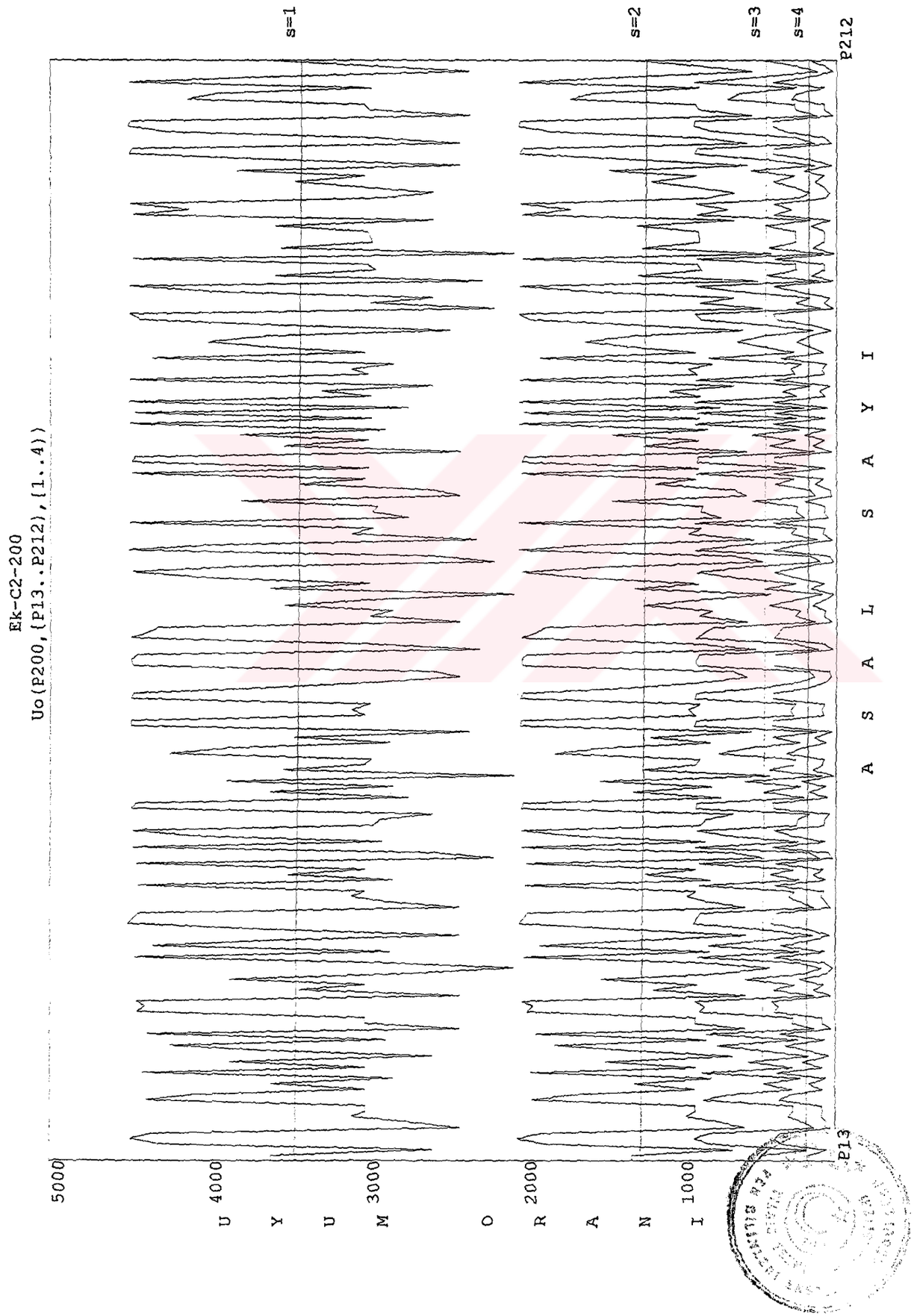
1223	857	1048111	1046032	468568	4470	209376	1997	93961	896	42198	402
1223	859	1050557	1048476	287327	2734	78636	748	21685	206	5949	56
1223	863	1055449	1053364	475197	4502	214059	2028	96430	913	43491	412
1223	877	1072571	1070472	318267	2967	94233	878	27826	259	8197	76
1223	881	1077463	1075360	353630	3282	115885	1075	37623	349	12103	112
1223	883	1079909	1077804	278482	2578	71591	662	18363	170	4726	43
1223	887	1084801	1082692	488449	4502	219577	2024	98577	908	44244	407
1223	907	1109261	1107132	331520	2988	99249	894	29754	268	8815	79
1223	911	1114153	1112020	344781	3094	106528	956	32819	294	10291	92
1223	919	1123937	1121796	318257	2831	89992	800	25441	226	7104	63
1223	929	1136167	1134016	495065	4357	215567	1897	93764	825	40863	359
1223	937	1145951	1143792	344774	3008	103720	905	31350	273	9458	82
1223	941	1150843	1148680	415499	3610	149798	1301	53794	467	19147	166
1223	947	1158181	1156012	464119	4007	186273	1608	74617	644	29852	257
1223	953	1165519	1163344	424333	3640	154327	1324	56232	482	20453	175
1223	967	1182641	1180452	291729	2466	71699	606	17886	151	4453	37
1223	971	1187533	1185340	424334	3573	151460	1275	54171	456	19275	162
1223	977	1194871	1192672	530411	4439	235322	1969	104067	870	45900	384
1223	983	1202209	1200004	541460	4503	243733	2027	109509	910	49262	409
1223	991	1211993	1209780	265201	2188	58004	478	12596	103	2723	22
1223	997	1219331	1217112	362442	2972	107700	883	32132	263	9654	79
1223	1009	1234007	1231776	318241	2578	82156	665	21276	172	5558	45
1223	1013	1238899	1236664	486200	3924	190862	1540	74981	605	29590	238
1223	1019	1246237	1243996	561339	4504	252461	2025	113185	908	50779	407
1223	1021	1248683	1246440	282879	2265	63603	509	14480	115	3345	26
1223	1031	1260913	1258660	450836	3575	160995	1276	57483	455	20516	162
1223	1033	1263359	1261104	371276	2938	109454	866	32336	255	9520	75
1223	1039	1270697	1268436	380115	2991	113430	892	33728	265	10119	79
1223	1049	1282927	1280656	574591	4478	257677	2008	115594	901	51816	403
1223	1051	1285373	1283100	265193	2063	54604	424	11407	88	2448	19
1223	1061	1297603	1295320	459671	3542	162738	1254	57465	442	20044	154
1223	1063	1300049	1297764	384529	2957	114019	877	33989	261	10172	78
1223	1069	1307387	1305096	388948	2975	115682	884	34552	264	10375	79
1223	1087	1329401	1327092	397784	2992	118623	892	35437	266	10557	79
1223	1091	1334293	1331980	477342	3577	171376	1284	61572	461	22120	165
1223	1093	1336739	1334424	344747	2579	88599	662	22693	169	5732	42
1223	1097	1341631	1339312	601097	4480	269473	2008	120942	901	54523	406
1223	1103	1348969	1346644	556898	4128	230072	1705	95311	706	39545	293
1223	1109	1356307	1353976	609932	4497	273753	2018	122994	906	55152	406
1223	1117	1366091	1363752	397781	2911	115525	845	33684	246	9700	71
1223	1123	1373429	1371084	353577	2574	91196	664	23488	171	6115	44
1223	1129	1380767	1378416	415457	3008	124602	902	37437	271	11291	81
1223	1151	1407673	1405300	486170	3453	167843	1192	58133	412	20095	142
1223	1153	1410119	1407744	424294	3008	127650	905	38277	271	11426	81
1223	1163	1422349	1419964	543624	3822	207183	1456	79003	555	29955	210
1223	1171	1432133	1429740	344736	2407	82832	578	19855	138	4841	33
1223	1181	1444363	1441960	512682	3549	182229	1261	64664	447	23285	161
1223	1187	1451701	1449292	654110	4505	294942	2031	132828	914	59977	413
1223	1193	1459039	1456624	654109	4483	292700	2006	131053	898	58710	402
1223	1201	1468823	1466400	353572	2407	84899	578	20340	138	4869	33
1223	1213	1483499	1481064	441962	2979	131184	884	39066	263	11583	78
1223	1217	1488391	1485952	636425	4275	271720	1825	115791	777	49242	330
1223	1223	1495729	1493284	675096	4513	304093	2033	137039	916	61724	412
1223	1229	1503067	1500616	676199	4498	304622	2026	137382	914	62081	413
1223	1231	1505513	1503060	353568	2348	82868	550	19436	129	4504	29
1223	1237	1512851	1510392	450798	2979	134495	889	40038	264	11869	78
1223	1249	1527527	1525056	459636	3009	138300	905	41567	272	12485	81
1223	1259	1539757	1537276	636419	4133	262690	1706	108655	705	45066	292
1223	1277	1561771	1559272	618735	3961	245244	1570	97014	621	38523	246
1223	1279	1564217	1561716	464049	2966	137745	880	40659	259	12099	77
1223	1283	1569109	1566604	707124	4506	318809	2031	143613	915	64466	410
1223	1289	1576447	1573936	583374	3700	215686	1368	80159	508	29881	189
1223	1291	1578893	1576380	371238	2351	86809	549	20151	127	4727	29
1223	1297	1586231	1583712	477306	3009	143539	904	43212	272	12953	81
1223	1301	1591123	1588600	574534	3610	207614	1304	75081	471	26905	169


Uo(P13,{P13..P212),{1..4))
s=1
s=2
s=3
s=4
P212
P13
5000
4000
3000
2000
1000
UYUMORANI
ASALSAYI


Ek-C2-50
Uo(P50,{P13..P212),{1..4))
s=1
s=2
s=3
s=4
P212
P13
5000
4000
3000
2000
1000
U Y U M O R A N I
A S A L S A Y I


Ek-C2-100
Uo(P100,(P13..P212),(1..4))
s=1
s=2
s=3
s=4
P212
P13
5000
4000
3000
2000
1000
U Y U M O R A N I
A S A L S A Y I

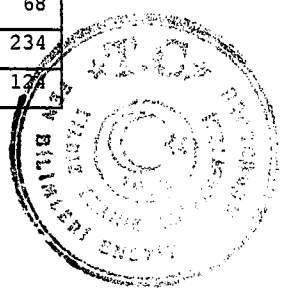

Ek-C2-150
Uo(P150,{P13..P212),{1..4))
s=1
s=2
s=3
s=4
P212
P13
5000
4000
3000
2000
1000
UYUMORANI
ASALSAYI


Ek-C2-200
Uo(P200,{P13..P212},{1..4})
s=1
s=2
s=3
s=4
P212
P13
5000
4000
3000
2000
1000
U Y U M O R A N I
A S A L S A Y I

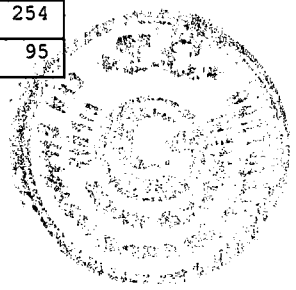
Ek-C3

$U_{00}(p,q,s)$; $p \in \{P_{13}..P_{212}\}$, $q \in [P_{13}..P_{212}]$, $s \in \{1..4\}$

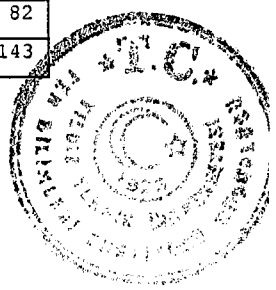
i	Pi	Seviye			
		1	2	3	4
13	41	3148	1026	348	123
14	43	2608	682	180	49
15	47	3585	1341	525	213
16	53	3476	1261	480	190
17	59	3618	1368	541	223
18	61	2507	627	158	40
19	67	2732	751	209	59
20	71	2767	793	236	73
21	73	2980	910	278	85
22	79	2772	772	222	61
23	83	3670	1421	575	242
24	89	3445	1250	475	182
25	97	2980	911	278	84
26	101	3158	1050	360	127
27	103	2805	812	231	68
28	107	3680	1435	582	245
29	109	2977	910	278	85
30	113	3291	1141	413	153
31	127	2612	694	188	50
32	131	2933	908	288	95
33	137	3540	1331	520	211
34	139	2852	835	242	70
35	149	3642	1415	1415	240
36	151	2512	640	161	40
37	157	2780	785	221	65
38	163	2988	910	278	83
39	167	3706	1455	1455	598
40	173	3671	1425	1427	244
41	179	2712	1455	594	254
42	181	2502	640	158	39
43	191	3001	948	309	102
44	193	2982	910	277	83
45	197	3290	1145	408	151
46	199	2741	760	765	60
47	211	2199	489	108	23
48	223	2902	860	254	77
49	227	3720	1466	600	257
50	229	2836	812	235	68
51	233	3636	1393	558	234
52	239	3116	1020	348	124



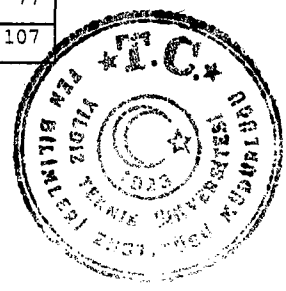
53	241	2516	639	160	40
54	251	3166	1051	359	128
55	257	3761	1489	617	263
56	263	3732	1467	601	257
57	269	3701	1447	589	251
58	271	2512	638	160	40
59	277	2870	832	241	72
60	281	2774	804	239	74
61	283	2929	871	261	77
62	293	3712	1451	591	253
63	307	2822	809	231	68
64	311	3063	982	328	110
65	313	2774	781	221	62
66	317	3709	1453	589	251
67	331	2303	536	120	28
68	337	2620	695	181	49
69	347	3734	1470	605	259
70	349	2888	848	249	74
71	353	3445	1252	471	188
72	359	3734	1473	608	259
73	367	2937	878	259	81
74	373	2799	850	249	75
75	379	2617	694	183	49
76	383	3735	1474	606	258
77	389	2716	1460	593	253
78	397	2736	761	211	61
79	401	3164	1051	359	127
80	409	2824	811	229	64
81	419	3273	1129	404	149
82	421	2201	488	102	21
83	431	3097	1002	331	116
84	433	2981	908	271	83
85	439	2948	882	260	77
86	443	3294	1149	411	154
87	449	3293	1142	408	155
88	457	2837	818	231	67
89	461	3029	966	314	105
90	463	2401	584	139	31
91	467	3739	1480	606	281
92	479	3741	1477	602	258
93	487	2984	909	273	83
94	491	2779	805	237	73
95	499	2952	888	262	79
96	503	3742	1478	605	259
97	509	3728	1469	594	254
98	521	2949	904	284	95



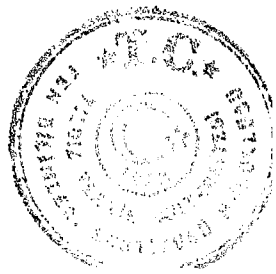
99	523	2890	847	248	72
100	541	2518	636	161	41
101	547	2438	599	148	37
102	557	3732	1462	599	254
103	563	3745	1474	607	259
104	569	3706	1443	587	248
105	571	2392	573	137	33
106	577	2990	904	275	85
107	587	3746	1474	607	260
108	593	3659	1406	565	236
109	599	3350	1177	432	164
110	601	2519	636	161	40
111	607	2961	886	268	82
112	613	2826	808	233	67
113	617	3023	956	315	107
114	619	2962	887	268	82
115	631	2210	488	108	23
116	641	3167	1045	357	126
117	643	2963	888	269	82
118	647	3373	1195	443	170
119	653	3736	1466	601	256
120	659	3229	1092	385	140
121	661	2310	535	124	29
122	673	2624	693	185	49
123	677	3494	1282	491	195
124	683	3338	1170	428	162
125	691	2415	585	142	34
126	701	2779	802	239	74
127	709	2941	874	263	80
128	719	3749	1477	608	260
129	727	2743	760	212	60
130	733	2943	875	263	80
131	739	2920	862	257	77
132	743	3236	1096	387	141
133	751	2519	636	161	41
134	757	2624	694	185	49
135	761	3009	943	307	103
136	769	2991	905	276	85
137	773	3740	1469	603	257
138	787	2969	892	270	82
139	797	3741	1470	604	258
140	809	3723	1456	596	253
141	811	2519	636	161	41
142	821	3092	997	334	115
143	823	2970	892	270	82
144	827	3243	1102	390	143



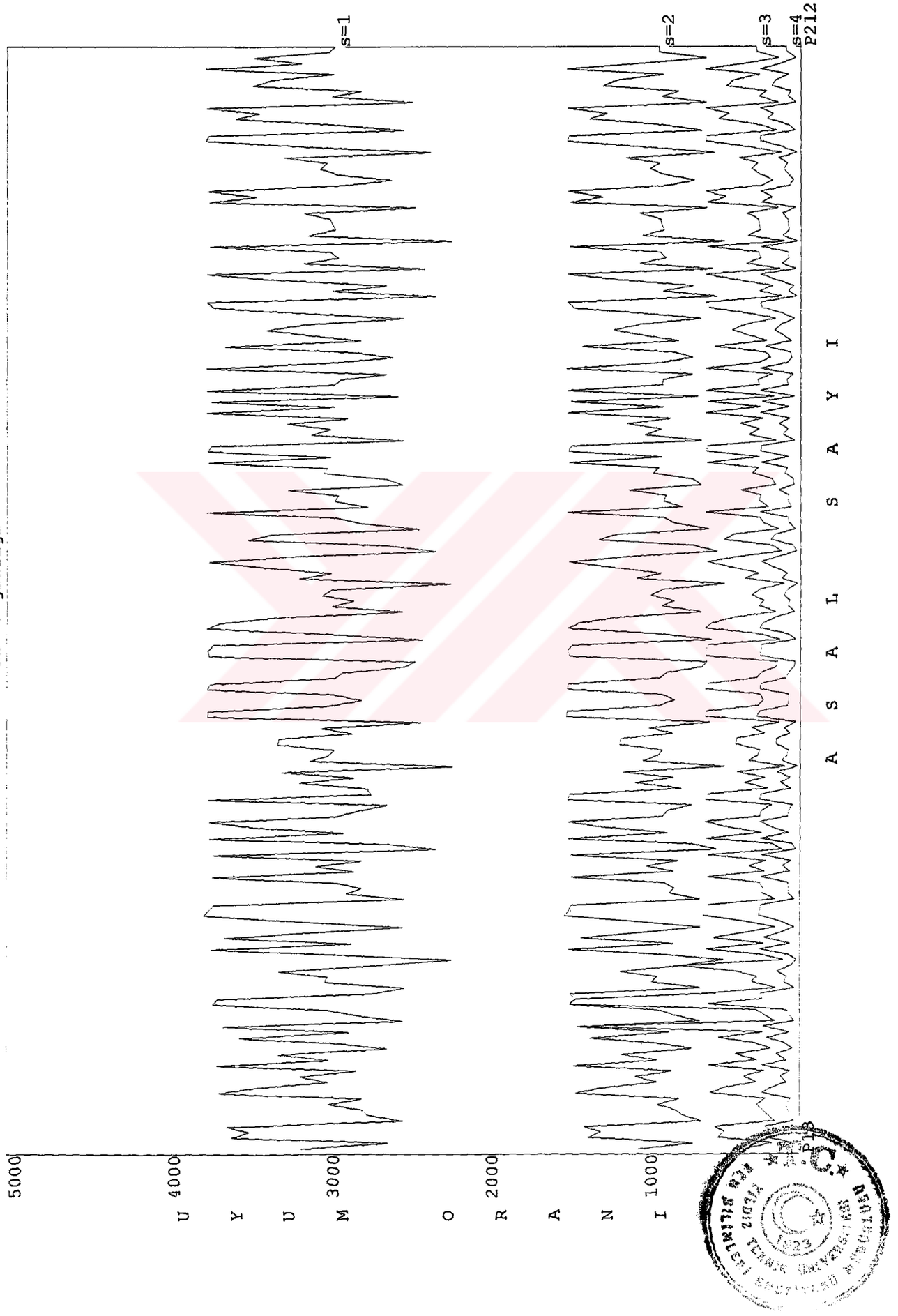
145	829	2868	831	244	72
146	839	3751	1478	609	261
147	853	2950	880	265	81
148	857	3725	1458	597	254
149	859	2550	657	171	45
150	863	3751	1478	609	260
151	877	2951	881	266	81
152	881	2905	879	276	89
153	883	2624	695	185	49
154	887	3753	1482	609	260
155	907	2972	893	271	83
156	911	2584	693	192	55
157	919	2827	808	233	68
158	929	3636	1389	554	230
159	937	2780	780	219	62
160	941	3103	1004	337	117
161	947	3370	1193	441	169
162	953	3116	1017	346	122
163	967	2517	638	163	42
164	971	3139	1024	348	121
165	977	3700	1438	585	247
166	983	3753	1480	610	261
167	991	2311	535	124	28
168	997	2957	884	267	81
169	1009	2626	691	183	47
170	1013	3307	1148	416	157
171	1019	3753	1480	610	261
172	1021	2381	568	136	32
173	1031	3138	1027	349	122
174	1033	2924	865	258	78
175	1039	2975	895	272	83
176	1049	3732	1464	600	255
177	1051	2211	489	108	24
178	1061	3110	1008	339	117
179	1063	2942	875	263	79
180	1069	2959	885	268	81
181	1087	2976	895	272	83
182	1091	3140	1028	349	122
183	1093	2440	600	148	37
184	1097	3734	1464	601	256
185	1103	3439	1256	477	185
186	1109	3747	1475	607	259
187	1117	2898	849	251	75
188	1123	2593	680	180	48
189	1129	2924	870	259	77
190	1151	3038	962	316	107



191	1153	2992	906	277	85
192	1163	3260	1113	396	146
193	1171	2341	549	127	28
194	1181	3116	1012	341	119
195	1187	3755	1482	611	262
196	1193	3736	1467	602	257
197	1201	2520	637	161	41
198	1213	2963	888	269	82
199	1217	3572	1341	526	214
200	1223	3423	1230	462	180
201	1229	3749	1477	608	260
202	1231	2460	607	150	37
203	1237	2964	888	269	82
204	1249	2782	782	222	63
205	1259	3460	1258	478	188
206	1277	3335	1168	428	162
207	1279	2951	881	266	81
208	1283	3755	1481	611	262
209	1289	3152	1050	361	130
210	1291	3452	608	148	36
211	1297	2979	904	277	85
212	1301	2946	905	288	94



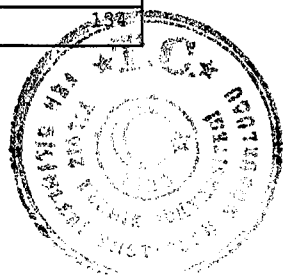
Ek-C4
Ek-C3 grafigi



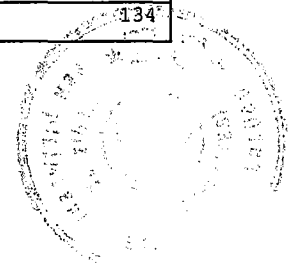
Ek-C5

$U_{000}(p, q, s)$ $p \in \{P_{13}..P_{212}\}$, $q \in [P_{13}..P_{212}]$, $s \in \{1..4\}$

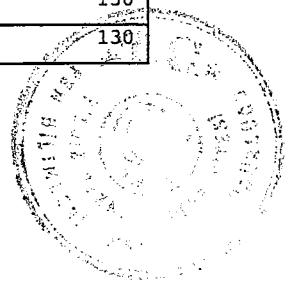
i	Pi	Seviye			
		1	2	3	4
13	41	3148	1026	348	123
14	43	2878	854	264	86
15	47	3114	1016	351	128
16	53	3204	1077	383	144
17	59	3287	1136	415	160
18	61	3157	1051	372	140
19	67	3096	1008	349	128
20	71	3055	981	335	121
21	73	3047	973	328	117
22	79	3019	953	318	112
23	83	3078	996	341	123
24	89	3109	1017	352	128
25	97	3099	1009	347	125
26	101	3103	1012	347	125
27	103	3083	998	340	121
28	107	3121	1026	355	129
29	109	3112	1019	350	126
30	113	3122	1026	354	128
31	127	3095	1008	345	124
32	131	3087	1003	342	122
33	137	3109	1019	351	127
34	139	3097	1010	346	124
35	149	3121	1028	392	129
36	151	3095	1012	383	125
37	157	3083	1003	376	123
38	163	3079	999	372	121
39	167	3102	1016	412	139
40	173	3123	1031	449	143
41	179	3109	1045	454	147
42	181	3088	1032	444	143
43	191	3085	1029	440	142
44	193	3082	1025	434	140
45	197	3089	1029	434	140
46	199	3078	1021	443	138
47	211	3053	1006	434	135
48	223	3049	1002	429	133
49	227	3067	1014	433	136
50	229	3061	1009	428	135
51	233	3076	1019	432	137
52	239	3077	1019	429	137
53	241	3063	1010	423	134



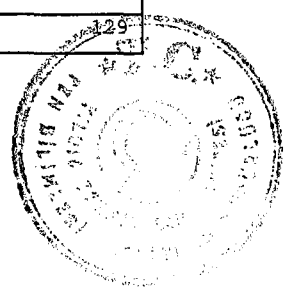
54	251	3066	1011	421	134
55	257	3082	1022	426	137
56	263	3097	1032	430	140
57	269	3110	1041	433	142
58	271	3097	1032	427	140
59	277	3092	1028	424	139
60	281	3086	1023	420	137
61	283	3082	1020	416	136
62	293	3095	1029	420	139
63	307	3090	1025	416	137
64	311	3089	1024	415	137
65	313	3083	1019	411	135
66	317	3095	1027	414	137
67	331	3080	1018	409	135
68	337	3072	1013	405	134
69	347	3084	1021	408	136
70	349	3080	1018	406	135
71	353	3086	1022	407	136
72	359	3097	1029	410	138
73	367	3095	1027	408	137
74	373	3090	1024	405	136
75	379	3082	1019	401	135
76	383	3093	1026	405	136
77	389	3087	1032	408	138
78	397	3081	1028	405	137
79	401	3083	1029	404	137
80	409	3079	1025	401	136
81	419	3082	1027	401	136
82	421	3069	1019	397	134
83	431	3070	1019	396	134
84	433	3068	1017	394	133
85	439	3067	1016	393	133
86	443	3070	1017	393	133
87	449	3073	1019	393	133
88	457	3070	1016	391	132
89	461	3069	1016	390	132
90	463	3060	1010	387	131
91	467	3069	1016	389	133
92	479	3077	1022	392	134
93	487	3076	1020	391	134
94	491	3073	1018	389	133
95	499	3071	1016	387	132
96	503	3079	1022	390	134
97	509	3087	1027	392	135
98	521	3085	1026	391	135
99	523	3083	1024	389	134



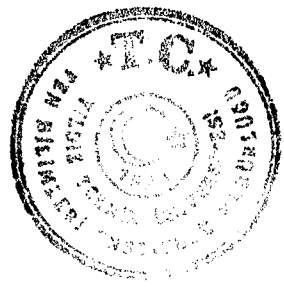
100	541	3077	1019	387	133
101	547	3069	1014	384	132
102	557	3077	1019	386	133
103	563	3084	1024	389	135
104	569	3091	1029	391	136
105	571	3083	1024	388	135
106	577	3082	1023	387	134
107	587	3089	1028	389	135
108	593	3095	1031	391	137
109	599	3098	1033	392	137
110	601	3092	1029	389	136
111	607	3091	1027	388	135
112	613	3088	1025	387	135
113	617	3087	1025	386	134
114	619	3086	1023	385	134
115	631	3078	1018	382	133
116	641	3079	1018	382	133
117	643	3077	1017	381	132
118	647	3080	1019	381	133
119	653	3086	1023	383	134
120	659	3088	1024	383	134
121	661	3081	1019	381	133
122	673	3076	1016	379	132
123	677	3080	1019	380	133
124	683	3082	1020	381	133
125	691	3077	1016	378	132
126	701	3074	1014	377	131
127	709	3073	1013	376	131
128	719	3079	1017	378	132
129	727	3076	1015	377	132
130	733	3075	1014	376	131
131	739	3073	1012	375	131
132	743	3075	1013	375	131
133	751	3070	1010	373	130
134	757	3066	1007	372	129
135	761	3066	1007	371	129
136	769	3065	1006	370	129
137	773	3071	1010	372	130
138	787	3070	1009	371	129
139	797	3075	1012	373	130
140	809	3080	1016	375	131
141	811	3076	1013	373	131
142	821	3076	1013	373	131
143	823	3075	1012	372	130
144	827	3077	1012	372	130
145	829	3075	1011	371	130



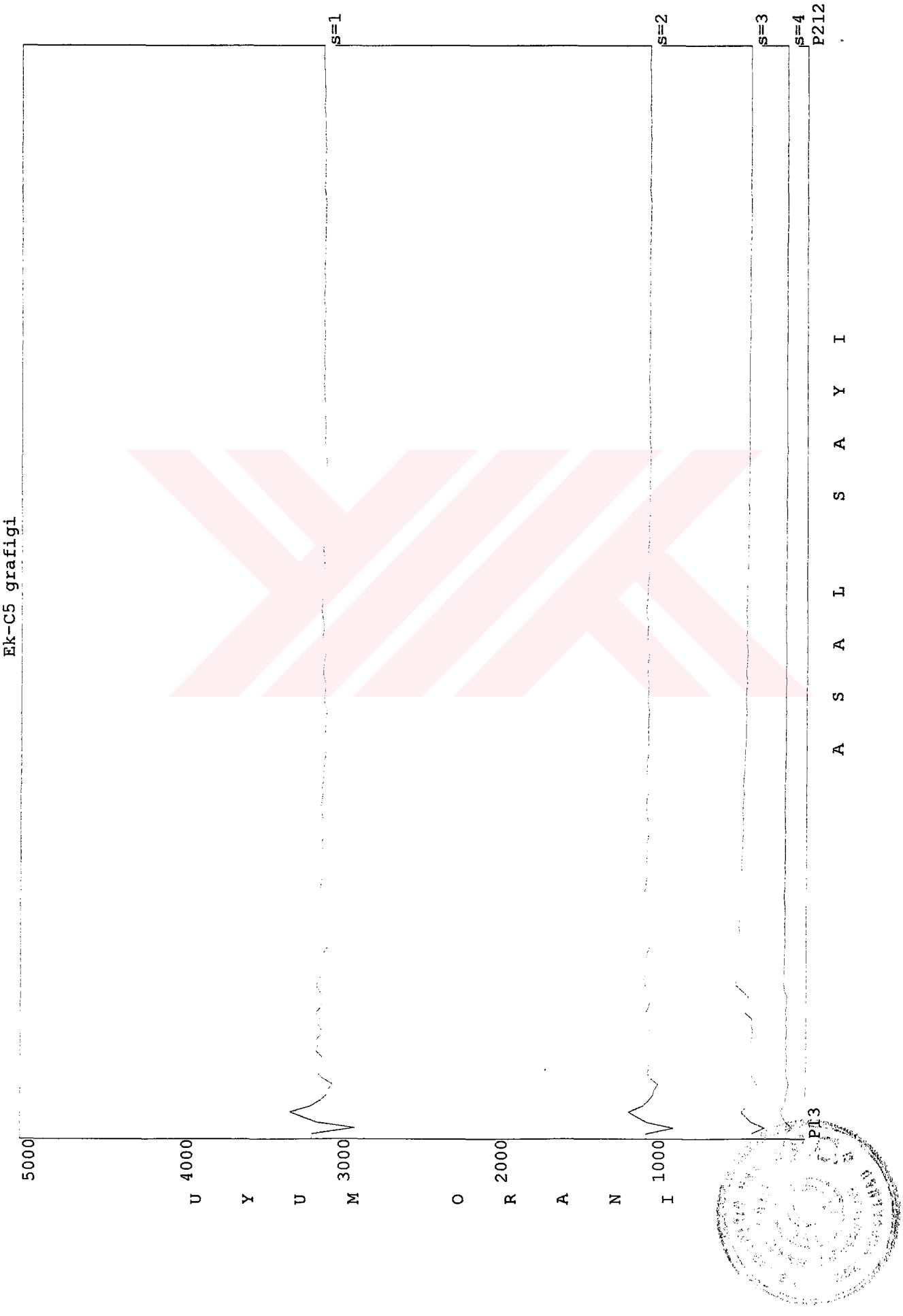
146	839	3080	1015	373	131
147	853	3079	1014	372	130
148	857	3084	1017	374	131
149	859	3080	1014	373	131
150	863	3085	1018	374	132
151	877	3084	1017	373	131
152	881	3083	1016	373	131
153	883	3079	1013	371	130
154	887	3084	1017	373	131
155	907	3083	1016	372	131
156	911	3080	1014	371	130
157	919	3078	1012	370	130
158	929	3082	1015	371	131
159	937	3080	1013	370	130
160	941	3080	1013	370	130
161	947	3082	1014	371	130
162	953	3082	1014	371	130
163	967	3078	1012	369	130
164	971	3079	1012	369	130
165	977	3083	1015	370	130
166	983	3087	1018	372	131
167	991	3082	1015	370	131
168	997	3081	1014	370	130
169	1009	3078	1012	369	130
170	1013	3080	1013	369	130
171	1019	3084	1015	370	131
172	1021	3080	1013	369	130
173	1031	3080	1013	369	130
174	1033	3079	1012	368	130
175	1039	3079	1011	367	130
176	1049	3082	1014	369	130
177	1051	3077	1011	367	130
178	1061	3077	1011	367	130
179	1063	3077	1010	367	129
180	1069	3076	1009	366	129
181	1087	3075	1008	365	129
182	1091	3076	1009	365	129
183	1093	3072	1006	364	128
184	1097	3076	1009	365	129
185	1103	3078	1010	366	129
186	1109	3082	1013	367	130
187	1117	3081	1012	367	130
188	1123	3078	1010	366	129
189	1129	3077	1009	365	129
190	1151	3077	1009	365	129
191	1153	3076	1009	364	129



192	1163	3077	1009	364	129
193	1171	3073	1007	363	128
194	1181	3074	1007	363	128
195	1187	3077	1009	364	129
196	1193	3081	1012	366	129
197	1201	3078	1010	365	129
198	1213	3077	1009	364	129
199	1217	3080	1011	365	129
200	1223	3082	1012	365	129
201	1229	3085	1014	367	130
202	1231	3082	1012	366	130
203	1237	3081	1012	365	129
204	1249	3080	1010	364	129
205	1259	3082	1012	365	129
206	1277	3083	1012	365	130
207	1279	3082	1012	365	129
208	1283	3086	1014	366	130
209	1289	3086	1014	366	130
210	1291	3088	1012	365	129
211	1297	3087	1012	364	129
212	1301	3087	1011	364	129



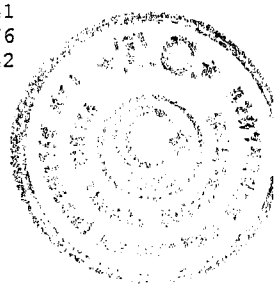
Ek-C6
Ek-C5 grafigi



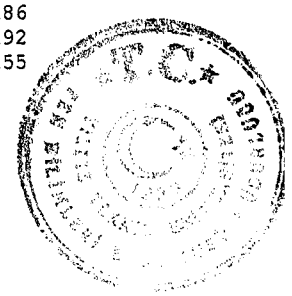
Ek-D13

$U(p,q,s)$ ve $U_0(p,q,s)$; $p=P_{13}$, $q \in \{P_{13}..P_{212}\}$, $s \in \{1..4\}$ $U_0(p,q,1)$'a göre sıralı

				s							
				1		2		3		4	
p	q	n	fiofn	U	Uo	U	Uo	U	Uo	U	Uo
41	463	18983	18480	3915	2062	763	401	148	77	25	13
41	547	22427	21840	4698	2094	975	434	225	100	55	24
41	1093	44813	43680	9409	2099	2021	450	421	93	83	18
41	967	39647	38640	8621	2174	1792	451	376	94	77	19
41	43	1763	1680	393	2229	92	521	25	141	8	45
41	859	35219	34320	7838	2225	1761	500	383	108	83	23
41	127	5207	5040	1172	2250	250	480	53	101	13	24
41	211	8651	8400	1956	2261	409	472	102	117	30	34
41	337	13817	13440	3130	2265	728	526	170	123	37	26
41	379	15539	15120	3523	2267	793	510	188	120	36	23
41	421	17261	16800	3916	2268	903	523	183	106	31	17
41	631	25871	25200	5877	2271	1279	494	289	111	61	23
41	673	27593	26880	6270	2272	1414	512	325	117	85	30
41	757	31037	30240	7053	2272	1608	518	387	124	99	31
41	883	36203	35280	8232	2273	1924	531	432	119	80	22
41	1009	41369	40320	9408	2274	2069	500	494	119	139	33
41	1051	43091	42000	9802	2274	2206	511	525	121	139	32
41	1123	46043	44880	10456	2270	2363	513	530	115	131	28
41	67	2747	2640	653	2377	153	556	34	123	10	36
41	199	8159	7920	1955	2396	434	531	90	110	13	15
41	331	13571	13200	3260	2402	786	579	174	128	30	22
41	397	16277	15840	3915	2405	963	591	232	142	70	43
41	661	27101	26400	6529	2409	1529	564	366	135	93	34
41	79	3239	3120	783	2417	174	537	44	135	7	21
41	727	29807	29040	7184	2410	1670	560	401	134	101	33
41	991	40631	39600	9800	2411	2305	567	553	136	156	38
41	157	6437	6240	1563	2428	399	619	96	149	34	52
41	313	12833	12480	3131	2439	731	569	174	135	27	21
41	937	38417	37440	9408	2448	2348	611	614	159	174	45
41	1171	48011	46800	11763	2450	2915	607	726	151	179	37
41	1249	51209	49920	12550	2450	3045	594	720	140	177	34
41	103	4223	4080	1044	2472	235	556	55	130	11	26
41	307	12587	12240	3129	2485	781	620	197	156	60	47
41	229	9389	9120	2347	2499	581	618	153	162	41	43
41	409	16769	16320	4176	2490	1032	615	251	149	63	37
41	613	25133	24480	6268	2493	1590	632	391	155	103	40
41	919	37679	36720	9407	2496	2253	597	538	142	114	30
41	1021	41861	40800	10453	2497	2652	633	619	147	131	31
41	457	18737	18240	4699	2507	1123	599	283	151	83	44
41	571	23411	22800	5874	2509	1470	627	359	153	86	36
41	139	5699	5520	1434	2516	365	640	68	119	19	33
41	277	11357	11040	2869	2526	737	648	194	170	53	46
41	691	28331	27600	7182	2535	1805	637	438	154	105	37
41	829	33989	33120	8622	2536	2171	638	603	177	164	48
41	349	14309	13920	3652	2552	911	636	221	154	65	45
41	373	15293	14880	3914	2559	1027	671	268	175	73	47
41	523	21443	20880	5482	2556	1384	645	348	162	91	42
41	223	9143	8880	2348	2568	579	633	130	142	25	27
41	1117	45797	44640	11762	2568	3079	672	805	175	227	49
41	283	11603	11280	3001	2586	794	684	185	159	34	29
41	739	30299	29520	7836	2586	2079	686	517	170	117	38
41	1231	50471	49200	13071	2589	3358	665	803	159	200	39
41	1033	42353	41280	10977	2591	2818	665	730	172	162	38
41	1129	46289	45120	12024	2597	3062	661	752	162	159	34
41	1291	52931	51600	13725	2592	3577	675	953	180	243	45
41	61	2501	2400	652	2606	157	627	40	159	8	31
41	367	15047	14640	3915	2601	993	659	291	193	94	62
41	709	29069	28320	7575	2605	1975	679	518	178	143	49
41	733	30053	29280	7838	2608	2048	681	575	191	159	52
41	1063	43583	42480	11371	2609	2920	669	734	168	180	41
41	73	2993	2880	783	2616	208	694	55	183	23	76
41	439	17999	17520	4699	2610	1171	650	301	167	77	42



41	499	20459	19920	5353	2616	1401	684	366	178	80	39
41	853	34973	34080	9147	2615	2455	701	671	191	146	41
41	877	35957	35040	9408	2616	2492	693	667	185	156	43
41	1279	52439	51120	13726	2617	3513	669	892	170	243	46
41	97	3977	3840	1043	2622	267	671	64	160	12	30
41	109	4469	4320	1174	2626	313	700	95	212	25	55
41	607	24887	24240	6530	2623	1673	672	404	162	113	45
41	619	25379	24720	6661	2624	1742	686	458	180	109	42
41	643	26363	25680	6923	2626	1871	709	488	185	135	51
41	997	40877	39840	10716	2621	2808	686	742	181	218	53
41	1069	43829	42720	11502	2624	2982	680	806	183	193	44
41	1213	49733	48480	13073	2628	3447	693	906	182	237	47
41	1237	50717	49440	13334	2629	3558	701	967	190	287	56
41	151	6191	6000	1629	2631	393	634	97	156	31	50
41	163	6683	6480	1760	2633	477	713	121	181	37	55
41	181	7421	7200	1955	2634	530	714	165	222	60	80
41	193	7913	7680	2087	2637	549	693	134	169	45	56
41	241	9881	9600	2608	2639	676	684	154	155	35	35
41	787	32267	31440	8492	2631	2294	710	635	196	210	65
41	823	33743	32880	8885	2633	2299	681	586	173	143	42
41	907	37187	36240	9801	2635	2567	690	683	183	184	49
41	1039	42599	41520	11240	2638	2906	682	726	170	184	43
41	1087	44567	43440	11764	2639	3049	684	764	171	213	47
41	271	11111	10800	2934	2640	742	667	185	166	49	44
41	433	17753	17280	4699	2646	1262	710	367	206	81	45
41	487	19967	19440	5286	2647	1354	678	360	180	101	50
41	541	22181	21600	5875	2648	1539	693	379	170	82	36
41	577	23657	23040	6267	2649	1629	688	397	167	89	37
41	601	24641	24000	6529	2649	1694	687	428	173	102	41
41	751	30791	30000	8163	2651	2079	675	512	166	128	41
41	769	31529	30720	8360	2651	2205	699	600	190	181	57
41	811	33251	32400	8817	2651	2307	693	603	181	148	44
41	1153	47273	46080	12549	2654	3326	703	878	185	242	51
41	1201	49241	48000	13071	2654	3447	700	933	189	259	52
41	1297	53177	51840	14118	2654	3756	706	967	181	242	45
41	617	25297	24640	7834	3096	2387	943	735	290	200	79
41	911	37351	36400	11759	3148	3629	971	1100	294	341	91
41	239	9799	9520	3131	3195	959	978	288	293	83	84
41	953	39073	38080	12544	3210	4071	1041	1343	343	434	111
41	1289	52849	51520	17255	3264	5667	1072	1905	360	646	122
41	659	27019	26320	9012	3335	3091	1144	1007	372	346	128
41	743	30463	29680	10189	3344	3386	1111	1181	387	409	134
41	827	33907	33040	11365	3351	3810	1123	1242	366	390	115
41	71	2911	2800	979	3363	319	1095	114	391	45	154
41	113	4633	4480	1565	3377	501	1081	157	338	59	127
41	1163	47683	46480	16078	3371	5442	1141	1889	396	617	129
41	197	8077	7840	2737	3388	924	1143	325	402	104	128
41	281	11521	11200	3914	3397	1314	1140	419	363	141	122
41	449	18409	17920	6265	3403	2092	1136	701	380	215	116
41	491	20131	19600	6853	3404	2352	1168	824	409	308	152
41	701	28741	28000	9796	3408	3334	1160	1164	404	370	128
41	419	17179	16720	5872	3418	2028	1180	768	447	302	175
41	443	18163	17680	6265	3449	2135	1175	701	385	239	131
41	1013	41533	40480	14375	3461	4992	1201	1709	411	602	144
41	683	28003	27280	9796	3498	3454	1233	1217	434	433	154
41	1277	52357	51040	18302	3495	6482	1238	2328	444	803	153
41	599	24559	23920	8618	3509	2968	1208	1023	416	351	142
41	947	38827	37840	13721	3533	4848	1248	1692	435	622	160
41	647	26527	25840	9403	3544	3295	1242	1158	436	436	164
41	89	3649	3520	1304	3573	455	1246	162	443	58	158
41	1223	50143	48880	18040	3597	6514	1299	2410	480	879	175
41	353	14473	14080	5219	3606	1863	1287	684	472	306	211
41	53	2173	2080	786	3617	281	1293	84	386	36	165
41	881	36121	35200	13065	3617	4704	1302	1694	468	626	173
41	131	5371	5200	1955	3639	722	1344	269	500	97	180
41	1103	45223	44080	16469	3641	5977	1321	2147	474	748	165
41	1259	51619	50320	18826	3647	6956	1347	2607	505	967	187
41	521	21361	20800	7833	3666	2835	1327	1011	473	362	169
41	677	27757	27040	10187	3670	3754	1352	1378	496	513	184
41	1301	53341	52000	19609	3676	7281	1364	2703	506	1000	187
41	137	5617	5440	2086	3713	774	1377	292	519	105	186
41	47	1927	1840	719	3731	265	1375	93	482	37	192
41	191	7831	7600	2934	3746	1046	1335	370	472	122	155

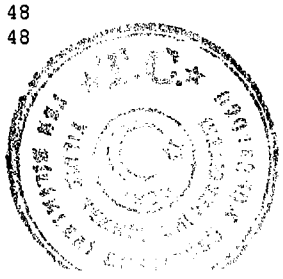


41	761	31201	30400	11757	3768	4378	1403	1644	526	621	199
41	1217	49897	48640	18824	3772	7077	1418	2608	522	907	181
41	59	2419	2320	915	3782	369	1525	152	628	64	264
41	461	18901	18400	7179	3798	2705	1431	1024	541	404	213
41	1151	47191	46000	17973	3808	6803	1441	2567	543	947	200
41	233	9553	9280	3652	3822	1386	1450	525	549	212	221
41	83	3403	3280	1306	3837	496	1457	215	631	107	314
41	311	12751	12400	4892	3836	1861	1459	718	563	299	234
41	149	6109	5920	2347	3841	862	1411	302	494	112	183
41	929	38089	37120	14633	3841	5592	1468	2118	556	826	216
41	107	4387	4240	1696	3865	641	1461	240	547	69	157
41	173	7093	6880	2738	3860	1043	1470	430	606	192	270
41	593	24313	23680	9402	3867	3566	1466	1368	562	527	216
41	431	17671	17200	6853	3878	2560	1448	957	541	344	194
41	821	33661	32800	13065	3881	5168	1535	2084	619	888	263
41	941	38581	37600	15028	3895	5814	1506	2271	588	879	227
41	41	1681	1600	656	3902	245	1457	99	588	38	226
41	167	6847	6640	2672	3902	1028	1501	410	598	166	242
41	179	7339	7120	2868	3907	1140	1553	459	625	196	267
41	269	11029	10720	4304	3902	1647	1493	633	573	236	213
41	293	12013	11680	4696	3909	1812	1508	755	628	310	258
41	1061	43501	42400	16991	3905	6606	1518	2554	587	921	211
41	317	12997	12640	5087	3913	1984	1526	786	604	316	243
41	569	23329	22720	9140	3917	3598	1542	1378	590	507	217
41	977	40057	39040	15682	3914	6129	1530	2398	598	979	244
41	1181	48421	47200	18954	3914	7372	1522	2890	596	1072	221
41	227	9307	9040	3651	3922	1421	1526	547	587	208	223
41	389	15949	15520	6264	3927	2388	1497	872	546	304	190
41	101	4141	4000	1630	3936	623	1504	269	649	107	258
41	263	10783	10480	4238	3930	1658	1537	649	601	256	237
41	809	33169	32320	13064	3938	5143	1550	2039	614	741	223
41	971	39811	38800	15681	3938	6182	1552	2466	619	1018	255
41	347	14227	13840	5610	3943	2203	1548	885	622	364	255
41	359	14719	14320	5806	3944	2206	1498	828	562	296	201
41	383	15703	15280	6198	3947	2422	1542	907	577	346	220
41	509	20869	20320	8224	3940	3198	1532	1202	575	468	224
41	557	22837	22240	9009	3944	3526	1543	1408	616	583	255
41	857	35137	34240	13850	3941	5376	1530	2088	594	834	237
41	1031	42271	41200	16663	3941	6469	1530	2464	582	903	213
41	1091	44731	43600	17645	3944	7005	1566	2763	617	1051	234
41	467	19147	18640	7570	3953	2972	1552	1183	617	476	248
41	479	19639	19120	7766	3954	3001	1528	1190	605	457	232
41	503	20623	20080	8158	3955	3205	1554	1266	613	478	231
41	563	23083	22480	9139	3959	3554	1539	1366	591	507	219
41	653	26773	26080	10578	3950	4177	1560	1590	593	643	240
41	773	31693	30880	12540	3956	4930	1555	1877	592	711	224
41	797	32677	31840	12932	3957	5096	1559	1970	602	804	246
41	1049	43009	41920	16991	3950	6659	1548	2605	605	1061	246
41	1097	44977	43840	17775	3952	6986	1553	2830	629	1208	268
41	1193	48913	47680	19347	3955	7683	1570	3066	626	1304	266
41	251	10291	10000	4076	3960	1636	1589	623	605	265	257
41	257	10537	10240	4173	3960	1614	1531	632	599	267	253
41	401	16441	16000	6525	3968	2595	1578	999	607	355	215
41	587	24067	23440	9531	3960	3766	1564	1452	603	569	236
41	719	29479	28720	11689	3965	4540	1540	1715	581	594	201
41	839	34399	33520	13652	3968	5289	1537	2029	589	762	221
41	863	35383	34480	14045	3969	5562	1571	2207	623	888	250
41	887	36367	35440	14437	3969	5747	1580	2279	626	928	255
41	1109	45469	44320	18036	3966	7125	1567	2858	628	1117	245
41	1229	50389	49120	19999	3968	7852	1558	3145	624	1233	244
41	641	26281	25600	10447	3975	4151	1579	1626	618	644	245
41	983	40303	39280	16008	3971	6313	1566	2594	643	1065	264
41	1019	41779	40720	16596	3972	6634	1587	2652	634	1089	260
41	1187	48667	47440	19345	3974	7724	1587	3124	641	1307	268
41	1283	52603	51280	20917	3976	8290	1575	3278	623	1280	243

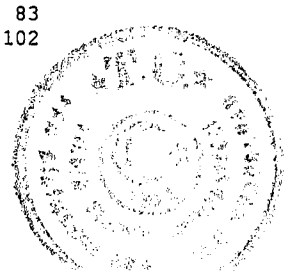
Ek-D50

$U(p,q,s)$ ve $U_o(p,q,s)$; $p=P_{50}$, $q \in \{P_{13}..P_{212}\}$, $s \in \{1..4\}$ $U_o(p,q,1)$'a göre sıralı

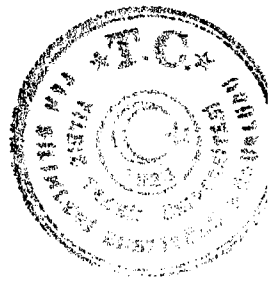
				s							
				1		2		3		4	
p	q	n	fiofn	U	Uo	U	Uo	U	Uo	U	Uo
229	911	208619	207480	41608	1994	8261	395	1653	79	335	16
229	71	16259	15960	3493	2148	733	450	160	98	35	21
229	211	48319	47880	10415	2155	2222	459	478	98	107	22
229	281	64349	63840	13878	2156	3057	475	659	102	149	23
229	421	96409	95760	20809	2158	4427	459	941	97	201	20
229	491	112439	111720	24275	2158	5242	466	1079	95	226	20
229	631	144499	143640	31207	2159	6694	463	1461	101	320	22
229	701	160529	159600	34674	2159	7440	463	1562	97	324	20
229	1051	240679	239400	52010	2160	11330	470	2435	101	518	21
229	331	75799	75240	17345	2288	3889	513	859	113	201	26
229	661	151369	150480	34675	2290	7973	526	1827	120	416	27
229	881	201749	200640	46232	2291	10570	523	2320	114	525	26
229	991	226939	225720	52010	2291	11997	528	2723	119	611	26
229	131	29999	29640	6956	2318	1531	510	314	104	62	20
229	521	119309	118560	27742	2325	6454	540	1455	121	313	26
229	1171	268159	266760	62411	2327	14634	545	3404	126	787	29
229	1301	297929	296400	69347	2327	16025	537	3651	122	840	28
229	1021	233809	232560	55477	2372	13236	566	3194	136	782	33
229	461	105569	104880	25433	2409	6096	577	1448	137	347	32
229	691	158239	157320	38144	2410	9109	575	2158	136	510	32
229	1151	263579	262200	63568	2411	15387	583	3736	141	917	34
229	311	71219	70680	17346	2435	4371	613	1121	157	311	43
229	431	98699	98040	24276	2459	5871	594	1456	147	386	39
229	463	106027	105336	26009	2453	6461	609	1556	146	378	35
229	617	141293	140448	34675	2454	8486	600	2105	148	551	38
229	821	188009	186960	46230	2458	11361	604	2889	153	743	39
229	941	215489	214320	53165	2467	13083	607	3247	150	794	36
229	1231	281899	280440	69349	2460	17018	603	4089	145	965	34
229	1291	295639	294120	72816	2463	17912	605	4405	148	1099	37
229	1061	242969	241680	60101	2473	14724	606	3642	149	898	36
229	1181	270449	269040	67036	2478	16623	614	4133	152	1045	38
229	41	9389	9120	2347	2499	581	618	153	162	41	43
229	547	125263	124488	31209	2491	7848	626	1957	156	478	38
229	971	222359	221160	55477	2494	13808	620	3447	155	868	39
229	1031	236099	234840	58946	2496	14740	624	3642	154	921	39
229	1091	249839	248520	62412	2498	15437	617	3767	150	923	36
229	1093	250297	248976	62413	2493	15467	617	3790	151	945	37
229	61	13969	13680	3499	2504	889	636	216	154	53	37
229	101	23129	22800	5803	2508	1435	620	375	162	104	44
229	151	34579	34200	8688	2512	2241	648	597	172	143	41
229	181	41449	41040	10418	2513	2556	616	608	146	147	35
229	191	43739	43320	10996	2514	2745	627	689	157	183	41
229	241	55189	54720	13882	2515	3476	629	855	154	213	38
229	251	57479	57000	14459	2515	3600	626	905	157	243	42
229	271	62059	61560	15616	2516	4017	647	1046	168	269	43
229	401	91829	91200	23121	2517	5789	630	1406	153	368	40
229	541	123889	123120	31210	2519	7839	632	2043	164	559	45
229	571	130759	129960	32943	2519	8333	637	2194	167	564	43
229	601	137629	136800	34677	2519	8664	629	2204	160	570	41
229	641	146789	145920	36987	2519	9358	637	2337	159	591	40
229	751	171979	171000	43342	2520	10948	636	2846	165	748	43
229	761	174269	173280	43920	2520	11000	631	2756	158	710	40
229	811	185719	184680	46810	2520	11716	630	2914	156	723	38
229	1201	275029	273600	69348	2521	17460	634	4290	155	1038	37
229	239	54731	54264	13883	2536	3541	646	902	164	222	40
229	953	218237	217056	55477	2542	14059	644	3505	160	884	40
229	967	221443	220248	57212	2583	14766	666	3852	173	954	43
229	1289	295181	293664	76283	2584	19604	664	5010	169	1291	43
229	659	150911	150024	39877	2642	10379	687	2788	184	727	48
229	743	170147	169176	45076	2649	11874	697	3181	186	854	50
229	859	196711	195624	52009	2643	13761	699	3650	185	962	48
229	827	189383	188328	50276	2654	13156	694	3437	181	925	48



229	1163	266327	264936	71082	2668	18818	706	4964	186	1277	47
229	43	9847	9576	2639	2680	700	710	186	188	50	50
229	113	25877	25536	6960	2689	1859	718	528	204	147	56
229	127	29083	28728	7825	2690	2089	718	517	177	127	43
229	197	45113	44688	12153	2693	3263	723	812	179	191	42
229	337	77173	76608	20812	2696	5590	724	1524	197	406	52
229	379	86791	86184	23411	2697	6345	731	1713	197	480	55
229	449	102821	102144	27743	2698	7451	724	2019	196	564	54
229	673	154117	153216	41609	2699	10988	712	2788	180	724	46
229	1123	257167	255816	69346	2696	18564	721	4958	192	1281	49
229	757	173353	172368	46810	2700	12791	737	3513	202	956	55
229	883	202207	201096	54611	2700	14704	727	3944	195	1064	52
229	1009	231061	229824	62413	2701	16873	730	4523	195	1227	53
229	443	101447	100776	27743	2734	7578	746	2088	205	574	56
229	1013	231977	230736	63567	2740	17396	749	4839	208	1313	56
229	1277	292433	290928	80907	2766	22467	768	6252	213	1744	59
229	683	156407	155496	43343	2771	11972	765	3390	216	921	58
229	599	137171	136344	38142	2780	10607	773	2952	215	827	60
229	947	216863	215688	60679	2798	16944	781	4793	221	1349	62
229	67	15343	15048	4370	2848	1241	808	353	230	90	58
229	1223	280067	278616	79752	2847	22612	807	6448	230	1915	68
229	89	20381	20064	5812	2851	1687	827	526	258	168	82
229	199	45571	45144	13022	2857	3683	808	1072	235	325	71
229	353	80837	80256	23125	2860	6570	812	1790	221	517	63
229	397	90913	90288	26011	2861	7443	818	2056	226	550	60
229	419	95951	95304	27456	2861	7781	810	2205	229	644	67
229	727	166483	165528	47676	2863	13702	823	3959	237	1102	66
229	53	12137	11856	3506	2888	1008	830	250	205	56	46
229	1259	288311	286824	83219	2886	24177	838	6915	239	1931	66
229	79	18091	17784	5235	2893	1531	846	451	249	119	65
229	157	35953	35568	10425	2899	2994	832	878	244	278	77
229	313	71677	71136	20816	2904	5976	833	1696	236	475	66
229	677	155033	154128	45076	2907	13076	843	3824	246	1112	71
229	937	214573	213408	62411	2908	18033	840	5265	245	1514	70
229	1249	286021	284544	83218	2909	24331	850	7034	245	1981	69
229	103	23587	23256	6965	2952	2089	885	601	254	184	78
229	137	31373	31008	9271	2955	2721	867	815	259	254	80
229	307	70303	69768	20817	2961	6093	866	1801	256	504	71
229	409	93661	93024	27746	2962	8148	869	2413	257	699	74
229	613	140377	139536	41609	2964	12348	879	3615	257	1079	76
229	647	148163	147288	43921	2964	13135	886	3930	265	1141	77
229	919	210451	209304	62411	2965	18415	875	5426	257	1611	76
229	47	10763	10488	3218	2989	961	892	290	269	78	72
229	139	31831	31464	9561	3003	2895	909	833	261	240	75
229	277	63433	62928	19085	3008	5812	916	1740	274	491	77
229	829	189841	188784	57211	3013	17270	909	5287	278	1650	86
229	59	13511	13224	4083	3021	1192	882	349	258	93	68
229	233	53357	52896	16198	3035	4988	934	1558	291	455	85
229	349	79921	79344	24282	3038	7395	925	2233	279	686	85
229	373	85417	84816	26014	3045	7884	923	2395	280	741	86
229	523	119767	119016	36412	3040	11066	923	3361	280	1049	87
229	929	212741	211584	64725	3042	19681	925	6017	282	1906	89
229	1103	252587	251256	76862	3042	23499	930	7135	282	2136	84
229	1117	255793	254448	78016	3049	23801	930	7286	284	2237	87
229	83	19007	18696	5813	3058	1703	895	495	260	175	92
229	149	34121	33744	10426	3055	3158	925	995	291	330	96
229	223	51067	50616	15621	3058	4786	937	1417	277	395	77
229	173	39617	39216	12157	3068	3685	930	1093	275	347	87
229	593	135797	134976	41611	3064	12687	934	3889	286	1175	86
229	107	24503	24168	7543	3078	2254	919	670	273	183	74
229	283	64807	64296	19952	3078	6094	940	1801	277	523	80
229	739	169231	168264	52011	3073	16034	947	4962	293	1533	90
229	1033	236557	235296	72816	3078	22176	937	6575	277	1944	82
229	1129	258541	257184	79751	3084	24655	953	7636	295	2413	93
229	269	61601	61104	19084	3098	5899	957	1877	304	604	98
229	367	84043	83448	26013	3095	8163	971	2618	311	837	99
229	709	162361	161424	50277	3096	15612	961	4863	299	1530	94
229	733	167857	166896	52010	3098	16031	955	4836	288	1520	90
229	977	223733	222528	69348	3099	21285	951	6536	292	1931	86
229	1063	243427	242136	75417	3098	23417	961	7254	297	2224	91
229	167	38243	37848	11870	3103	3684	963	1141	298	334	87
229	179	40991	40584	12736	3107	3846	938	1171	285	343	83
229	293	67097	66576	20817	3102	6470	964	2173	323	685	102



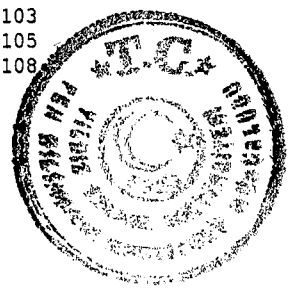
229	317	72593	72048	22551	3106	6974	960	2187	301	649	89
229	439	100531	99864	31212	3104	9549	949	2981	296	917	91
229	569	130301	129504	40455	3104	12470	957	3878	297	1230	94
229	853	195337	194256	60679	3106	18969	971	5935	303	1837	94
229	877	200833	199728	62413	3107	19240	958	6045	300	1948	96
229	1279	292891	291384	91021	3107	28165	961	8687	296	2703	92
229	227	51983	51528	16199	3116	4983	958	1508	290	477	91
229	389	89081	88464	27747	3114	8578	962	2594	291	767	86
229	499	114271	113544	35544	3110	11068	968	3428	299	1085	94
229	607	139003	138168	43344	3118	13513	972	4224	303	1283	92
229	619	141751	140904	44211	3118	13951	984	4379	308	1390	98
229	809	185261	184224	57789	3119	17956	969	5720	308	1852	99
229	997	228313	227088	71082	3113	22150	970	6875	301	2167	94
229	1069	244801	243504	76282	3116	23883	975	7557	308	2391	97
229	263	60227	59736	18797	3121	5876	975	1786	296	498	82
229	347	79463	78888	24860	3128	7725	972	2402	302	755	95
229	359	82211	81624	25727	3129	8167	993	2603	316	828	100
229	509	116561	115824	36412	3123	11352	973	3479	298	1022	87
229	557	127553	126768	39877	3126	12316	965	3838	300	1150	90
229	643	147247	146376	45944	3120	14350	974	4453	302	1414	96
229	787	180223	179208	56344	3126	17708	982	5561	308	1738	96
229	823	188467	187416	58943	3127	18608	987	5765	305	1756	93
229	857	196253	195168	61257	3121	19215	979	6069	309	1994	101
229	1049	240221	238944	75126	3127	23391	973	7197	299	2219	92
229	1097	251213	249888	78594	3128	24598	979	7716	307	2446	97
229	1213	277777	276336	86686	3120	27056	974	8507	306	2578	92
229	1237	283273	281808	88419	3121	27499	970	8524	300	2607	92
229	73	16717	16416	5238	3133	1589	950	475	284	141	84
229	97	22213	21888	6968	3136	2159	971	661	297	198	89
229	109	24961	24624	7832	3137	2445	979	825	330	287	114
229	383	87707	87096	27458	3130	8671	988	2756	314	857	97
229	467	106943	106248	33524	3134	10485	980	3310	309	1035	96
229	479	109691	108984	34390	3135	10670	972	3286	299	1064	96
229	503	115187	114456	36123	3136	11405	990	3779	328	1287	111
229	563	128927	128136	40456	3137	12736	987	4037	313	1317	102
229	587	134423	133608	42190	3138	13231	984	4150	308	1314	97
229	653	149537	148656	46811	3130	14691	982	4669	312	1445	96
229	773	177017	176016	55478	3134	17247	974	5464	308	1669	94
229	797	182513	181488	57211	3134	18006	986	5695	312	1808	99
229	907	207703	206568	65012	3130	20392	981	6259	301	1870	90
229	1039	237931	236664	74548	3133	23416	984	7385	310	2296	96
229	1087	248923	247608	78016	3134	24387	979	7708	309	2451	98
229	1193	273197	271776	85529	3130	26585	973	8254	302	2489	91
229	163	37327	36936	11726	3141	3628	971	1081	289	302	80
229	193	44197	43776	13891	3142	4327	979	1351	305	433	97
229	229	52441	51984	16488	3144	5182	988	1636	311	522	99
229	257	58853	58368	18507	3144	5843	992	1845	313	627	106
229	433	99157	98496	31213	3147	9702	978	3017	304	933	94
229	457	104653	103968	32946	3148	10385	992	3336	318	1090	104
229	487	111523	110808	35112	3148	11109	996	3451	309	1035	92
229	577	132133	131328	41612	3149	12935	978	3927	297	1224	92
229	719	164651	163704	51722	3141	16169	982	5046	306	1594	96
229	839	192131	191064	60390	3143	18824	979	5933	308	1880	97
229	863	197627	196536	62124	3143	19521	987	6143	310	1953	98
229	887	203123	202008	63858	3143	20147	991	6436	316	2071	101
229	983	225107	223896	70791	3144	22205	986	6987	310	2178	96
229	1019	233351	232104	73392	3145	23049	987	7123	305	2197	94
229	1109	253961	252624	79751	3140	24789	976	7531	296	2291	90
229	1187	271823	270408	85529	3146	26751	984	8297	305	2605	95
229	1229	281441	279984	88420	3141	27943	992	8661	307	2692	95
229	1283	293807	292296	92463	3147	28995	986	8952	304	2752	93
229	769	176101	175104	55478	3150	17494	993	5581	316	1803	102
229	1153	264037	262656	83218	3151	26191	991	8254	312	2645	100
229	1217	278693	277248	87841	3151	27682	993	8781	315	2802	100
229	1297	297013	295488	93621	3152	29376	989	9283	312	2891	97



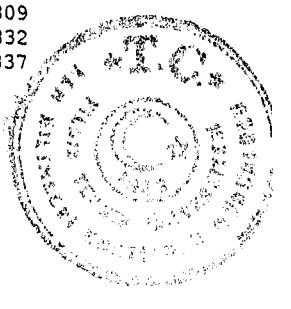
Ek-D100

$U(p,q,s)$ ve $U_o(p,q,s)$; $p=P_{100}$, $q \in \{P_{13}..P_{212}\}$, $s \in \{1..4\}$ $U_o(p,q,1)$'a göre sıralı

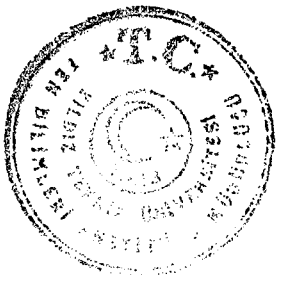
				s							
				1		2		3		4	
p	q	n	fiofn	U	Uo	U	Uo	U	Uo	U	Uo
863	211	182093	181020	41427	2275	9441	518	2223	122	506	27
863	421	363323	362040	82715	2276	18851	518	4372	120	1031	28
863	631	544553	543060	124012	2277	28129	516	6539	120	1492	27
863	1051	907013	905100	206619	2278	47092	519	10697	117	2357	25
863	331	285653	284460	68959	2414	16597	581	3975	139	985	34
863	661	570443	568920	137786	2415	33260	583	8071	141	1994	34
863	991	855233	853380	206625	2416	49794	582	12104	141	2992	34
863	1171	1010573	1008540	247934	2453	61033	603	14872	147	3667	36
863	1021	881123	879240	220397	2501	54736	621	13604	154	3354	38
863	571	492773	491340	124024	2516	31355	636	7985	162	2013	40
863	691	596333	594780	151559	2541	38657	648	9952	166	2569	43
863	463	399569	398244	103379	2587	26784	670	7005	175	1802	45
863	1231	1062353	1060260	275477	2593	71585	673	18648	175	4977	46
863	1291	1114133	1111980	289246	2596	74979	672	19449	174	5020	45
863	547	472061	470652	124029	2627	32386	686	8400	177	2198	46
863	1093	943259	941304	247940	2628	64985	688	17122	181	4572	48
863	61	52643	51720	13944	2648	3759	714	1021	193	281	53
863	151	130313	129300	34573	2653	9284	712	2510	192	652	50
863	181	156203	155160	41452	2653	10924	699	2907	186	747	47
863	241	207983	206880	55213	2654	14653	704	3896	187	1090	52
863	271	233873	232740	62093	2654	16402	701	4352	186	1104	47
863	541	466883	465480	124032	2656	33292	713	8931	191	2368	50
863	601	518663	517200	137798	2656	36518	704	9637	185	2563	49
863	751	648113	646500	172215	2657	45618	703	12068	186	3189	49
863	811	699893	698220	185983	2657	49268	703	13267	189	3601	51
863	1201	1036463	1034400	275479	2657	73152	705	19327	186	5056	48
863	967	834521	832692	227288	2723	61816	740	16789	201	4455	53
863	859	741317	739596	206640	2787	57515	775	15982	215	4400	59
863	43	37109	36204	10522	2835	2944	793	847	228	259	69
863	127	109601	108612	31147	2841	8662	790	2477	226	701	63
863	337	290831	289632	82748	2845	23525	808	6633	228	1840	63
863	379	327077	325836	93070	2845	26333	805	7612	232	2136	65
863	673	580799	579264	165340	2846	47113	811	13391	230	3813	65
863	757	653291	651672	185992	2847	52859	809	15056	230	4344	66
863	883	762029	760284	216968	2847	61896	812	17663	231	5103	66
863	1009	870767	868896	247948	2847	70644	811	20341	233	5878	67
863	1123	969149	967164	275484	2842	78110	805	22201	229	6382	65
863	67	57821	56892	17407	3010	5311	918	1642	283	543	93
863	199	171737	170676	51795	3015	15598	908	4658	271	1352	78
863	397	342611	341352	103404	3018	31249	912	9611	280	2974	86
863	727	627401	625812	189441	3019	56964	907	17111	272	5161	82
863	79	68177	67236	20848	3057	6344	930	1925	282	579	84
863	157	135491	134472	41478	3061	12707	937	4003	295	1278	94
863	313	270119	268944	82761	3063	25360	938	7836	290	2386	88
863	937	808631	806832	247957	3066	75937	939	23292	288	7210	89
863	1249	1077887	1075776	330570	3066	101272	939	31099	288	9642	89
863	103	88889	87924	27728	3119	8643	972	2662	299	812	91
863	307	264941	263772	82765	3123	26082	984	8093	305	2487	93
863	409	352967	351696	110291	3124	34449	975	10788	305	3364	95
863	613	529019	527544	165354	3125	51853	980	16281	307	5070	95
863	919	793097	791316	247958	3126	77423	976	24245	305	7642	96
863	229	197627	196536	62124	3143	19521	987	6143	310	1953	98
863	457	394391	393072	124058	3145	39011	989	12211	309	3847	97
863	911	786193	784420	247959	3153	77947	991	24408	310	7694	97
863	139	119957	118956	38047	3171	12154	1013	3893	324	1251	104
863	277	239051	237912	75886	3174	24031	1005	7545	315	2345	98
863	829	715427	713736	227308	3177	71913	1005	22724	317	7298	102
863	349	301187	299976	96532	3205	30746	1020	9870	327	3185	105
863	523	451349	449964	144709	3206	46366	1027	14859	329	4658	103
863	373	321899	320664	103415	3212	33311	1034	10698	332	3409	105
863	1117	963971	961992	309922	3215	99849	1035	32226	334	10463	108



863	223	192449	191364	62129	3228	20276	1053	6605	343	2239	116
863	283	244229	243084	79331	3248	25947	1062	8477	347	2728	111
863	739	637757	636156	206661	3240	67175	1053	21767	341	7022	110
863	1033	891479	889584	289268	3244	93825	1052	30413	341	9912	111
863	1129	974327	972336	316807	3251	102865	1055	33359	342	10757	110
863	367	316721	315492	103418	3265	33642	1062	10865	343	3536	111
863	709	611867	610296	199778	3265	65380	1068	21571	352	7133	116
863	733	632579	630984	206662	3266	67357	1064	21915	346	7161	113
863	1063	917369	915444	299596	3265	97660	1064	31701	345	10219	111
863	439	378857	377556	124065	3274	40418	1066	13063	344	4190	110
863	853	736139	734424	241081	3274	78821	1070	25939	352	8557	116
863	877	756851	755112	247965	3276	81380	1075	26545	350	8747	115
863	1279	1103777	1101636	361558	3275	118319	1071	38745	351	12695	115
863	499	430637	429276	141272	3280	46166	1072	15087	350	4953	115
863	607	523841	522372	172246	3288	56440	1077	18400	351	5997	114
863	619	534197	532716	175688	3288	57373	1074	18772	351	6167	115
863	997	860411	858552	282387	3282	92684	1077	30409	353	10014	116
863	1069	922547	920616	303039	3284	99434	1077	32544	352	10535	114
863	1213	1046819	1044744	344346	3289	113399	1083	37093	354	12070	115
863	643	554909	553404	182570	3290	60137	1083	19624	353	6472	116
863	787	679181	677532	223872	3296	73983	1089	24401	359	8101	119
863	823	710249	708564	234198	3297	77119	1085	25136	353	8281	116
863	907	782741	780972	258292	3299	85311	1089	28483	363	9456	120
863	1237	1067531	1065432	351231	3290	115381	1080	37751	353	12494	117
863	1039	896657	894756	296157	3302	97693	1089	32111	358	10583	118
863	1087	938081	936132	309925	3303	102219	1089	33789	360	11235	119
863	73	62999	62064	20867	3312	6714	1065	2162	343	682	108
863	97	83711	82752	27742	3314	9170	1095	3023	361	1014	121
863	109	94067	93096	31180	3314	10284	1093	3399	361	1130	120
863	163	140669	139644	46655	3316	15439	1097	5197	369	1723	122
863	193	166559	165504	55254	3317	18368	1102	6245	374	2128	127
863	433	373679	372384	124068	3320	41128	1100	13567	363	4362	116
863	487	420281	418932	139553	3320	46390	1103	15456	367	5195	123
863	577	497951	496512	165364	3320	54594	1096	17988	361	5942	119
863	769	663647	662016	220432	3321	72934	1098	24111	363	7791	117
863	1153	995039	993024	330578	3322	109707	1102	36441	366	12057	121
863	1297	1119311	1117152	371885	3322	122838	1097	40644	363	13391	119
863	71	61273	60340	20873	3406	7069	1153	2421	395	893	145
863	281	242503	241360	82782	3413	28322	1167	9703	400	3363	138
863	491	423733	422380	144719	3415	49287	1163	16970	400	5891	139
863	701	604963	603400	206668	3416	70248	1161	23968	396	8279	136
863	881	760303	758560	275516	3623	99776	1312	36110	474	13032	171
863	131	113053	112060	41522	3672	15031	1329	5453	482	2003	177
863	521	449623	448240	165383	3678	60637	1348	22129	492	8081	179
863	1301	1122763	1120600	413207	3680	152114	1354	56017	498	20652	183
863	191	164833	163780	62165	3771	23437	1421	8868	537	3402	206
863	761	656743	655120	247987	3776	93780	1427	35448	539	13595	207
863	461	397843	396520	151624	3811	57961	1456	22032	553	8410	211
863	1151	993313	991300	378789	3813	144382	1453	54879	552	21026	211
863	311	268393	267220	103453	3854	40014	1490	15472	576	6003	223
863	617	532471	530992	206690	3881	80177	1505	31245	586	11937	224
863	821	708523	706840	275526	3888	107282	1514	41898	591	16311	230
863	431	371953	370660	144747	3891	56261	1512	21607	580	8405	225
863	941	812083	810280	316833	3901	123255	1517	47533	585	18277	225
863	1061	915643	913720	358139	3911	139881	1527	54800	598	21388	233
863	1181	1019203	1017160	399445	3919	156715	1537	61564	604	23967	235
863	971	837973	836140	330603	3945	130300	1554	51497	614	20244	241
863	1031	889753	887860	351256	3947	139201	1564	54980	617	21575	242
863	1091	941533	939580	371908	3950	146943	1560	58327	619	23186	246
863	41	35383	34480	14045	3969	5562	1571	2207	623	888	250
863	101	87163	86200	34666	3977	13735	1575	5460	626	2191	251
863	251	216613	215500	86259	3982	34390	1587	13603	627	5437	251
863	401	346063	344800	137870	3983	54844	1584	21948	634	8863	256
863	641	553183	551680	220462	3985	87718	1585	34764	628	13871	250
863	239	206257	205156	82820	4015	33237	1611	13516	655	5541	268
863	953	822439	820624	330606	4019	133052	1617	53487	650	21510	261
863	1289	1112407	1110256	454528	4085	185549	1667	75764	681	30972	278
863	659	568717	567196	237680	4179	99320	1746	41739	733	17601	309
863	743	641209	639604	268657	4189	112556	1755	47472	740	19681	306
863	827	713701	712012	299634	4198	125496	1758	52347	733	21854	306
863	1163	1003669	1001644	423552	4220	177996	1773	74523	742	31103	309
863	113	97519	96544	41562	4261	17787	1823	7591	778	3245	332
863	197	170011	168952	72515	4265	30875	1816	13280	781	5738	337



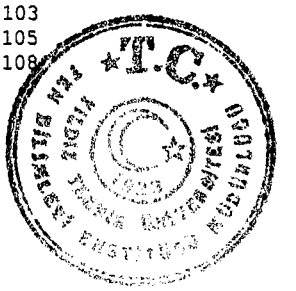
863	449	387487	386176	165413	4268	70245	1812	29776	768	12767	329
863	419	361597	360316	155093	4289	66347	1834	28459	787	12147	335
863	443	382309	381004	165418	4326	71354	1866	30683	802	13128	343
863	1013	874219	872344	378807	4333	164016	1876	71094	813	30821	352
863	1277	1102051	1099912	482076	4374	210522	1910	91823	833	39981	362
863	683	589429	587884	258340	4382	113096	1918	49478	839	21512	364
863	599	516937	515476	227367	4398	100138	1937	44300	856	19738	381
863	947	817261	815452	361601	4424	159968	1957	70523	862	31167	381
863	647	558361	556852	248019	4441	110184	1973	48835	874	21583	386
863	1223	1055449	1053364	475197	4502	214059	2028	96430	913	43491	412
863	89	76807	75856	34706	4518	15644	2036	6979	908	3053	397
863	353	304639	303424	137901	4526	62335	2046	28322	929	12841	421
863	1103	951889	949924	433891	4558	198055	2080	90537	951	41282	433
863	1259	1086517	1084396	495853	4563	226083	2080	103086	948	46862	431
863	53	45739	44824	20962	4582	9605	2099	4546	993	2122	463
863	677	584251	582712	268676	4598	123499	2113	56733	971	26087	446
863	137	118231	117232	55347	4681	25978	2197	12094	1022	5554	469
863	1217	1050271	1048192	495858	4721	234312	2230	110559	1052	52404	498
863	47	40561	39652	19257	4747	9082	2239	4214	1038	1969	485
863	59	50917	49996	24414	4794	11700	2297	5606	1101	2693	528
863	233	201079	199984	96632	4805	46663	2320	22471	1117	10869	540
863	929	801727	799936	385711	4811	185398	2312	88945	1109	42664	532
863	149	128587	127576	62236	4839	30087	2339	14519	1129	6964	541
863	83	71629	70684	34728	4848	16823	2348	8172	1140	3930	548
863	593	511759	510304	248039	4846	120171	2348	58217	1137	28078	548
863	173	149299	148264	72555	4859	35183	2356	17088	1144	8173	547
863	107	92341	91372	45045	4878	21915	2373	10656	1153	5147	557
863	269	232147	231016	113840	4903	55415	2387	27089	1166	13313	573
863	977	843151	841312	413252	4901	202439	2400	99087	1175	48537	575
863	167	144121	143092	70839	4915	34717	2408	17175	1191	8507	590
863	179	154477	153436	75999	4919	37433	2423	18393	1190	9006	582
863	293	252859	251704	124161	4910	61021	2413	30041	1188	14879	588
863	317	273571	272392	134484	4915	65900	2408	32502	1188	16069	587
863	569	491047	489616	241159	4911	118331	2409	58097	1183	28508	580
863	389	335707	334456	165453	4928	81607	2430	40263	1199	19750	588
863	227	195901	194812	96640	4933	47513	2425	23459	1197	11483	586
863	263	226969	225844	112122	4939	55170	2430	26953	1187	13212	582
863	809	698167	696496	344412	4933	169738	2431	83362	1194	41043	587
863	857	739591	737872	365064	4936	180630	2442	89001	1203	43847	592
863	509	439267	437896	217071	4941	107306	2442	52646	1198	25793	587
863	557	480691	479272	237719	4945	117391	2442	57969	1205	28608	595
863	1049	905287	903376	447676	4945	221701	2448	109473	1209	54060	597
863	1097	946711	944752	468329	4946	231284	2443	114028	1204	56423	595
863	347	299461	298252	148250	4950	73691	2460	36628	1223	18077	603
863	359	309817	308596	153411	4951	75846	2448	37469	1209	18700	603
863	383	330529	329284	163734	4953	80795	2444	40023	1210	19770	598
863	467	403021	401692	199864	4959	98629	2447	48455	1202	23678	587
863	479	413377	412036	205026	4959	101418	2453	49977	1208	24617	595
863	653	563539	562024	279018	4951	138207	2452	68376	1213	33944	602
863	773	667099	665464	330646	4956	163681	2453	81162	1216	40337	604
863	797	687811	686152	340972	4957	168758	2453	83849	1219	41453	602
863	1193	1029559	1027504	509635	4950	252117	2448	124955	1213	61942	601
863	503	434089	432724	215350	4960	106990	2464	53134	1224	26292	605
863	563	485869	484444	241161	4963	119499	2459	59007	1214	29145	599
863	587	506581	505132	251486	4964	124930	2466	62172	1227	30923	610
863	719	620497	618916	308274	4968	153043	2466	75827	1222	37465	603
863	1109	957067	955096	475213	4965	235827	2464	117170	1224	58275	608
863	1229	1060627	1058536	526848	4967	261855	2468	130049	1226	64578	608
863	257	221791	220672	110404	4977	55131	2485	27568	1242	13698	617
863	839	724057	722356	359903	4970	179029	2472	89560	1236	44806	618
863	887	765481	763732	380555	4971	188657	2464	93440	1220	46230	603
863	983	848329	846484	421860	4972	209914	2474	104382	1230	51934	612
863	1019	879397	877516	437349	4973	218028	2479	108116	1229	53267	605
863	1187	1024381	1022332	509636	4975	253448	2474	126403	1233	63070	615
863	1283	1107229	1105084	550944	4975	273481	2469	136097	1229	67800	612
863	863	744769	743044	371090	4982	185035	2484	92600	1243	46284	621



Ek-D150

$U(p,q,s)$ ve $U_0(p,q,s)$; $p=P_{150}$, $q \in \{P_{13}..P_{212}\}$, $s \in \{1..4\}$ $U_0(p,q,1)$'a göre sıralı

				s							
				1		2		3		4	
p	q	n	fiofn	U	Uo	U	Uo	U	Uo	U	Uo
863	211	182093	181020	41427	2275	9441	518	2223	122	506	27
863	421	363323	362040	82715	2276	18851	518	4372	120	1031	28
863	631	544553	543060	124012	2277	28129	516	6539	120	1492	27
863	1051	907013	905100	206619	2278	47092	519	10697	117	2357	25
863	331	285653	284460	68959	2414	16597	581	3975	139	985	34
863	661	570443	568920	137786	2415	33260	583	8071	141	1994	34
863	991	855233	853380	206625	2416	49794	582	12104	141	2992	34
863	1171	1010573	1008540	247934	2453	61033	603	14872	147	3667	36
863	1021	881123	879240	220397	2501	54736	621	13604	154	3354	38
863	571	492773	491340	124024	2516	31355	636	7985	162	2013	40
863	691	596333	594780	151559	2541	38657	648	9952	166	2569	43
863	463	399569	398244	103379	2587	26784	670	7005	175	1802	45
863	1231	1062353	1060260	275477	2593	71585	673	18648	175	4977	46
863	1291	1114133	1111980	289246	2596	74979	672	19449	174	5020	45
863	547	472061	470652	124029	2627	32386	686	8400	177	2198	46
863	1093	943259	941304	247940	2628	64985	688	17122	181	4572	48
863	61	52643	51720	13944	2648	3759	714	1021	193	281	53
863	151	130313	129300	34573	2653	9284	712	2510	192	652	50
863	181	156203	155160	41452	2653	10924	699	2907	186	747	47
863	241	207983	206880	55213	2654	14653	704	3896	187	1090	52
863	271	233873	232740	62093	2654	16402	701	4352	186	1104	47
863	541	466883	465480	124032	2656	33292	713	8931	191	2368	50
863	601	518663	517200	137798	2656	36518	704	9637	185	2563	49
863	751	648113	646500	172215	2657	45618	703	12068	186	3189	49
863	811	699893	698220	185983	2657	49268	703	13267	189	3601	51
863	1201	1036463	1034400	275479	2657	73152	705	19327	186	5056	48
863	967	834521	832692	227288	2723	61816	740	16789	201	4455	53
863	859	741317	739596	206640	2787	57515	775	15982	215	4400	59
863	43	37109	36204	10522	2835	2944	793	847	228	259	69
863	127	109601	108612	31147	2841	8662	790	2477	226	701	63
863	337	290831	289632	82748	2845	23525	808	6633	228	1840	63
863	379	327077	325836	93070	2845	26333	805	7612	232	2136	65
863	673	580799	579264	165340	2846	47113	811	13391	230	3813	65
863	757	653291	651672	185992	2847	52859	809	15056	230	4344	66
863	883	762029	760284	216968	2847	61896	812	17663	231	5103	66
863	1009	870767	868896	247948	2847	70644	811	20341	233	5878	67
863	1123	969149	967164	275484	2842	78110	805	22201	229	6382	65
863	67	57821	56892	17407	3010	5311	918	1642	283	543	93
863	199	171737	170676	51795	3015	15598	908	4658	271	1352	78
863	397	342611	341352	103404	3018	31249	912	9611	280	2974	86
863	727	627401	625812	189441	3019	56964	907	17111	272	5161	82
863	79	68177	67236	20848	3057	6344	930	1925	282	579	84
863	157	135491	134472	41478	3061	12707	937	4003	295	1278	94
863	313	270119	268944	82761	3063	25360	938	7836	290	2386	88
863	937	808631	806832	247957	3066	75937	939	23292	288	7210	89
863	1249	1077887	1075776	330570	3066	101272	939	31099	288	9642	89
863	103	88889	87924	27728	3119	8643	972	2662	299	812	91
863	307	264941	263772	82765	3123	26082	984	8093	305	2487	93
863	409	352967	351696	110291	3124	34449	975	10788	305	3364	95
863	613	529019	527544	165354	3125	51853	980	16281	307	5070	95
863	919	793097	791316	247958	3126	77423	976	24245	305	7642	96
863	229	197627	196536	62124	3143	19521	987	6143	310	1953	98
863	457	394391	393072	124058	3145	39011	989	12211	309	3847	97
863	911	786193	784420	247959	3153	77947	991	24408	310	7694	97
863	139	119957	118956	38047	3171	12154	1013	3893	324	1251	104
863	277	239051	237912	75886	3174	24031	1005	7545	315	2345	98
863	829	715427	713736	227308	3177	71913	1005	22724	317	7298	102
863	349	301187	299976	96532	3205	30746	1020	9870	327	3185	105
863	523	451349	449964	144709	3206	46366	1027	14859	329	4658	103
863	373	321899	320664	103415	3212	33311	1034	10698	332	3409	105
863	1117	963971	961992	309922	3215	99849	1035	32226	334	10463	108



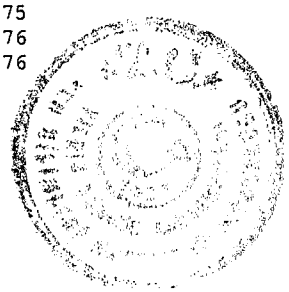
863	223	192449	191364	62129	3228	20276	1053	6605	343	2239	116
863	283	244229	243084	79331	3248	25947	1062	8477	347	2728	111
863	739	637757	636156	206661	3240	67175	1053	21767	341	7022	110
863	1033	891479	889584	289268	3244	93825	1052	30413	341	9912	111
863	1129	974327	972336	316807	3251	102865	1055	33359	342	10757	110
863	367	316721	315492	103418	3265	33642	1062	10865	343	3536	111
863	709	611867	610296	199778	3265	65380	1068	21571	352	7133	116
863	733	632579	630984	206662	3266	67357	1064	21915	346	7161	113
863	1063	917369	915444	299596	3265	97660	1064	31701	345	10219	111
863	439	378857	377556	124065	3274	40418	1066	13063	344	4190	110
863	853	736139	734424	241081	3274	78821	1070	25939	352	8557	116
863	877	756851	755112	247965	3276	81380	1075	26545	350	8747	115
863	1279	1103777	1101636	361558	3275	118319	1071	38745	351	12695	115
863	499	430637	429276	141272	3280	46166	1072	15087	350	4953	115
863	607	523841	522372	172246	3288	56440	1077	18400	351	5997	114
863	619	534197	532716	175688	3288	57373	1074	18772	351	6167	115
863	997	860411	858552	282387	3282	92684	1077	30409	353	10014	116
863	1069	922547	920616	303039	3284	99434	1077	32544	352	10535	114
863	1213	1046819	1044744	344346	3289	113399	1083	37093	354	12070	115
863	643	554909	553404	182570	3290	60137	1083	19624	353	6472	116
863	787	679181	677532	223872	3296	73983	1089	24401	359	8101	119
863	823	710249	708564	234198	3297	77119	1085	25136	353	8281	116
863	907	782741	780972	258292	3299	85311	1089	28483	363	9456	120
863	1237	1067531	1065432	351231	3290	115381	1080	37751	353	12494	117
863	1039	896657	894756	296157	3302	97693	1089	32111	358	10583	118
863	1087	938081	936132	309925	3303	102219	1089	33789	360	11235	119
863	73	62999	62064	20867	3312	6714	1065	2162	343	682	108
863	97	83711	82752	27742	3314	9170	1095	3023	361	1014	121
863	109	94067	93096	31180	3314	10284	1093	3399	361	1130	120
863	163	140669	139644	46655	3316	15439	1097	5197	369	1723	122
863	193	166559	165504	55254	3317	18368	1102	6245	374	2128	127
863	433	373679	372384	124068	3320	41128	1100	13567	363	4362	116
863	487	420281	418932	139553	3320	46390	1103	15456	367	5195	123
863	577	497951	496512	165364	3320	54594	1096	17988	361	5942	119
863	769	663647	662016	220432	3321	72934	1098	24111	363	7791	117
863	1153	995039	993024	330578	3322	109707	1102	36441	366	12057	121
863	1297	1119311	1117152	371885	3322	122838	1097	40644	363	13391	119
863	71	61273	60340	20873	3406	7069	1153	2421	395	893	145
863	281	242503	241360	82782	3413	28322	1167	9703	400	3363	138
863	491	423733	422380	144719	3415	49287	1163	16970	400	5891	139
863	701	604963	603400	206668	3416	70248	1161	23968	396	8279	136
863	881	760303	758560	275516	3623	99776	1312	36110	474	13032	171
863	131	113053	112060	41522	3672	15031	1329	5453	482	2003	177
863	521	449623	448240	165383	3678	60637	1348	22129	492	8081	179
863	1301	1122763	1120600	413207	3680	152114	1354	56017	498	20652	183
863	191	164833	163780	62165	3771	23437	1421	8868	537	3402	206
863	761	656743	655120	247987	3776	93780	1427	35448	539	13595	207
863	461	397843	396520	151624	3811	57961	1456	22032	553	8410	211
863	1151	993313	991300	378789	3813	144382	1453	54879	552	21026	211
863	311	268393	267220	103453	3854	40014	1490	15472	576	6003	223
863	617	532471	530992	206690	3881	80177	1505	31245	586	11937	224
863	821	708523	706840	275526	3888	107282	1514	41898	591	16311	230
863	431	371953	370660	144747	3891	56261	1512	21607	580	8405	225
863	941	812083	810280	316833	3901	123255	1517	47533	585	18277	225
863	1061	915643	913720	358139	3911	139881	1527	54800	598	21388	233
863	1181	1019203	1017160	399445	3919	156715	1537	61564	604	23967	235
863	971	837973	836140	330603	3945	130300	1554	51497	614	20244	241
863	1031	889753	887860	351256	3947	139201	1564	54980	617	21575	242
863	1091	941533	939580	371908	3950	146943	1560	58327	619	23186	246
863	41	35383	34480	14045	3969	5562	1571	2207	623	888	250
863	101	87163	86200	34666	3977	13735	1575	5460	626	2191	251
863	251	216613	215500	86259	3982	34390	1587	13603	627	5437	251
863	401	346063	344800	137870	3983	54844	1584	21948	634	8863	256
863	641	553183	551680	220462	3985	87718	1585	34764	628	13871	250
863	239	206257	205156	82820	4015	33237	1611	13516	655	5541	268
863	953	822439	820624	330606	4019	133052	1617	53487	650	21510	261
863	1289	1112407	1110256	454528	4085	185549	1667	75764	681	30972	278
863	659	568717	567196	237680	4179	99320	1746	41739	733	17601	309
863	743	641209	639604	268657	4189	112556	1755	47472	740	19681	306
863	827	713701	712012	299634	4198	125496	1758	52347	733	21854	306
863	1163	1003669	1001644	423552	4220	177996	1773	74523	742	31103	309
863	113	97519	96544	41562	4261	17787	1823	7591	778	3245	332
863	197	170011	168952	72515	4265	30875	1816	13280	781	5738	337

863	449	387487	386176	165413	4268	70245	1812	29776	768	12767	329
863	419	361597	360316	155093	4289	66347	1834	28459	787	12147	335
863	443	382309	381004	165418	4326	71354	1866	30683	802	13128	343
863	1013	874219	872344	378807	4333	164016	1876	71094	813	30821	352
863	1277	1102051	1099912	482076	4374	210522	1910	91823	833	39981	362
863	683	589429	587884	258340	4382	113096	1918	49478	839	21512	364
863	599	516937	515476	227367	4398	100138	1937	44300	856	19738	381
863	947	817261	815452	361601	4424	159968	1957	70523	862	31167	381
863	647	558361	556852	248019	4441	110184	1973	48835	874	21583	386
863	1223	1055449	1053364	475197	4502	214059	2028	96430	913	43491	412
863	89	76807	75856	34706	4518	15644	2036	6979	908	3053	397
863	353	304639	303424	137901	4526	62335	2046	28322	929	12841	421
863	1103	951889	949924	433891	4558	198055	2080	90537	951	41282	433
863	1259	1086517	1084396	495853	4563	226083	2080	103086	948	46862	431
863	53	45739	44824	20962	4582	9605	2099	4546	993	2122	463
863	677	584251	582712	268676	4598	123499	2113	56733	971	26087	446
863	137	118231	117232	55347	4681	25978	2197	12094	1022	5554	469
863	1217	1050271	1048192	495858	4721	234312	2230	110559	1052	52404	498
863	47	40561	39652	19257	4747	9082	2239	4214	1038	1969	485
863	59	50917	49996	24414	4794	11700	2297	5606	1101	2693	528
863	233	201079	199984	96632	4805	46663	2320	22471	1117	10869	540
863	929	801727	799936	385711	4811	185398	2312	88945	1109	42664	532
863	149	128587	127576	62236	4839	30087	2339	14519	1129	6964	541
863	83	71629	70684	34728	4848	16823	2348	8172	1140	3930	548
863	593	511759	510304	248039	4846	120171	2348	58217	1137	28078	548
863	173	149299	148264	72555	4859	35183	2356	17088	1144	8173	547
863	107	92341	91372	45045	4878	21915	2373	10656	1153	5147	557
863	269	232147	231016	113840	4903	55415	2387	27089	1166	13313	573
863	977	843151	841312	413252	4901	202439	2400	99087	1175	48537	575
863	167	144121	143092	70839	4915	34717	2408	17175	1191	8507	590
863	179	154477	153436	75999	4919	37433	2423	18393	1190	9006	582
863	293	252859	251704	124161	4910	61021	2413	30041	1188	14879	588
863	317	273571	272392	134484	4915	65900	2408	32502	1188	16069	587
863	569	491047	489616	241159	4911	118331	2409	58097	1183	28508	580
863	389	335707	334456	165453	4928	81607	2430	40263	1199	19750	588
863	227	195901	194812	96640	4933	47513	2425	23459	1197	11483	586
863	263	226969	225844	112122	4939	55170	2430	26953	1187	13212	582
863	809	698167	696496	344412	4933	169738	2431	83362	1194	41043	587
863	857	739591	737872	365064	4936	180630	2442	89001	1203	43847	592
863	509	439267	437896	217071	4941	107306	2442	52646	1198	25793	587
863	557	480691	479272	237719	4945	117391	2442	57969	1205	28608	595
863	1049	905287	903376	447676	4945	221701	2448	109473	1209	54060	597
863	1097	946711	944752	468329	4946	231284	2443	114028	1204	56423	595
863	347	299461	298252	148250	4950	73691	2460	36628	1223	18077	603
863	359	309817	308596	153411	4951	75846	2448	37469	1209	18700	603
863	383	330529	329284	163734	4953	80795	2444	40023	1210	19770	598
863	467	403021	401692	199864	4959	98629	2447	48455	1202	23678	587
863	479	413377	412036	205026	4959	101418	2453	49977	1208	24617	595
863	653	563539	562024	279018	4951	138207	2452	68376	1213	33944	602
863	773	667099	665464	330646	4956	163681	2453	81162	1216	40337	604
863	797	687811	686152	340972	4957	168758	2453	83849	1219	41453	602
863	1193	1029559	1027504	509635	4950	252117	2448	124955	1213	61942	601
863	503	434089	432724	215350	4960	106990	2464	53134	1224	26292	605
863	563	485869	484444	241161	4963	119499	2459	59007	1214	29145	599
863	587	506581	505132	251486	4964	124930	2466	62172	1227	30923	610
863	719	620497	618916	308274	4968	153043	2466	75827	1222	37465	603
863	1109	957067	955096	475213	4965	235827	2464	117170	1224	58275	608
863	1229	1060627	1058536	526848	4967	261855	2468	130049	1226	64578	608
863	257	221791	220672	110404	4977	55131	2485	27568	1242	13698	617
863	839	724057	722356	359903	4970	179029	2472	89560	1236	44806	618
863	887	765481	763732	380555	4971	188657	2464	93440	1220	46230	603
863	983	848329	846484	421860	4972	209914	2474	104382	1230	51934	612
863	1019	879397	877516	437349	4973	218028	2479	108116	1229	53267	605
863	1187	1024381	1022332	509636	4975	253448	2474	126403	1233	63070	615
863	1283	1107229	1105084	550944	4975	273481	2469	136097	1229	67800	612
863	863	744769	743044	371090	4982	185035	2484	92600	1243	46284	621

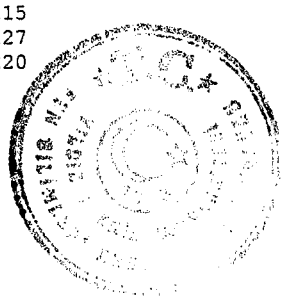
Ek-D200

$U(p,q,s)$ ve $U_o(p,q,s)$; $p=P_{200}$, $q \in \{P_{13}..P_{212}\}$, $s \in \{1..4\}$ $U_o(p,q,1)$'a göre sıralı

				s							
				1		2		3		4	
p	q	n	fiofn	U	Uo	U	Uo	U	Uo	U	Uo
1223	211	258053	256620	53181	2060	10948	424	2351	91	513	19
1223	421	514883	513240	106175	2062	22006	427	4612	89	935	18
1223	631	771713	769860	159177	2062	32852	425	6857	88	1418	18
1223	1051	1285373	1283100	265193	2063	54604	424	11407	88	2448	19
1223	331	404813	403260	88519	2186	19215	474	4165	102	883	21
1223	661	808403	806520	176857	2187	38639	477	8492	105	1857	22
1223	991	1211993	1209780	265201	2188	58004	478	12596	103	2723	22
1223	1021	1248683	1246440	282879	2265	63603	509	14480	115	3345	26
1223	571	698333	696540	159195	2279	36410	521	8262	118	1843	26
1223	691	845093	843180	194532	2301	44954	531	10392	122	2434	28
1223	463	566249	564564	132696	2343	31284	552	7316	129	1709	30
1223	1231	1505513	1503060	353568	2348	82868	550	19436	129	4504	29
1223	1291	1578893	1576380	371238	2351	86809	549	20151	127	4727	29
1223	61	74603	73320	17908	2400	4367	585	1049	140	267	35
1223	151	184673	183300	44388	2403	10712	580	2523	136	578	31
1223	181	221363	219960	53215	2403	12827	579	3119	140	751	33
1223	241	294743	293280	70877	2404	17009	577	4161	141	1063	36
1223	271	331433	329940	79709	2404	19245	580	4628	139	1095	33
1223	541	661643	659880	159205	2406	38341	579	9167	138	2238	33
1223	601	735023	733200	176872	2406	42608	579	10349	140	2491	33
1223	751	918473	916500	221045	2406	53546	582	12931	140	3119	33
1223	811	991853	989820	238714	2406	57592	580	14008	141	3415	34
1223	1171	1432133	1429740	344736	2407	82832	578	19855	138	4841	33
1223	1201	1468823	1466400	353572	2407	84899	578	20340	138	4869	33
1223	967	1182641	1180452	291729	2466	71699	606	17886	151	4453	37
1223	43	52589	51324	13515	2569	3464	658	950	180	276	52
1223	127	155321	153972	39991	2574	10297	662	2677	172	651	41
1223	337	412151	410592	106220	2577	27134	658	6967	169	1822	44
1223	379	463517	461916	119468	2577	30774	663	7875	169	1979	42
1223	547	668981	667212	172469	2578	44402	663	11362	169	2830	42
1223	673	823079	821184	212223	2578	54795	665	13901	168	3412	41
1223	757	925811	923832	238726	2578	61515	664	15929	172	4138	44
1223	883	10799091	077804	278482	2578	71591	662	18363	170	4726	43
1223	1009	12340071	231776	318241	2578	82156	665	21276	172	5558	45
1223	1093	13367391	334424	344747	2579	88599	662	22693	169	5732	42
1223	1123	13734291	371084	353577	2574	91196	664	23488	171	6115	44
1223	67	81941	80652	22355	2728	6039	736	1631	199	442	53
1223	199	243377	241956	66494	2732	18204	747	4969	204	1373	56
1223	397	485531	483912	132733	2733	36015	741	9847	202	2749	56
1223	727	889121	887172	243155	2734	66543	748	18446	207	5010	56
1223	859	1050557	1048476	287327	2734	78636	748	21685	206	5949	56
1223	103	125969	124644	35604	2826	10051	797	2810	223	774	61
1223	307	375461	373932	106244	2829	30197	804	8658	230	2476	65
1223	409	500207	498576	141575	2830	40022	800	11422	228	3330	66
1223	613	749699	747864	212241	2831	59817	797	16915	225	4755	63
1223	919	1123937	1121796	318257	2831	89992	800	25441	226	7104	63
1223	229	280067	278616	79752	2847	22612	807	6448	230	1915	68
1223	457	558911	557232	159241	2849	45406	812	12891	230	3553	63
1223	139	169997	168636	48850	2873	14121	830	4146	243	1243	73
1223	277	338771	337272	97416	2875	27824	821	8019	236	2336	68
1223	829	1013867	1011816	291756	2877	83881	827	24343	240	7135	70
1223	349	426827	425256	123915	2903	36105	845	10602	248	3104	72
1223	373	456179	454584	132747	2909	38489	843	11050	242	3162	69
1223	523	639629	637884	185745	2903	53735	840	15579	243	4542	71
1223	1117	1366091	1363752	397781	2911	115525	845	33684	246	9700	71
1223	223	272729	271284	79758	2924	23348	856	6786	248	1967	72
1223	739	903797	901836	265257	2934	77966	862	22943	253	6820	75
1223	1033	1263359	1261104	371276	2938	109454	866	32336	255	9520	75
1223	367	448841	447252	132751	2957	39067	870	11512	256	3368	75
1223	709	867107	865176	256423	2957	75616	872	22387	258	6655	76
1223	733	896459	894504	265257	2958	78354	874	23147	258	6836	76

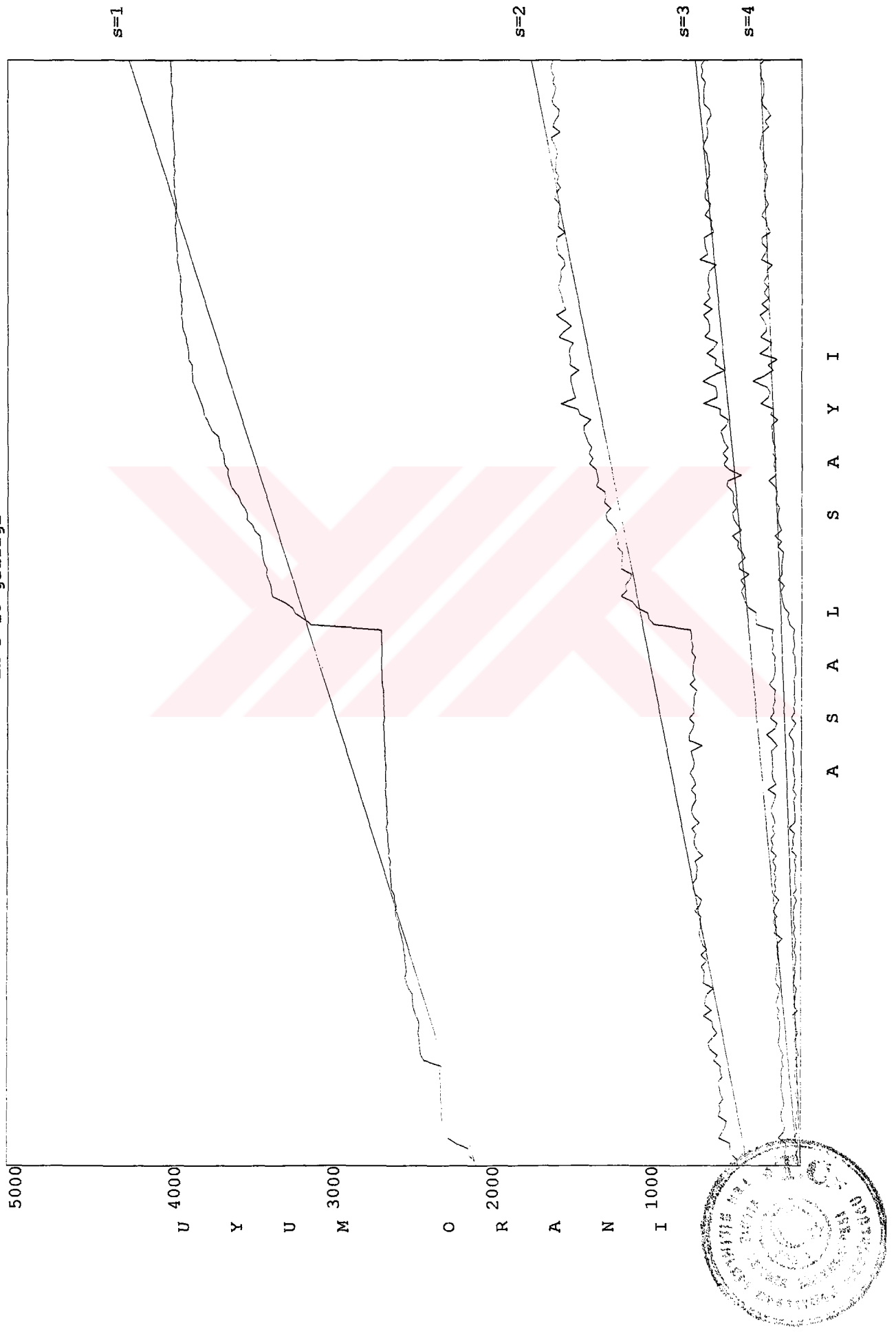


1223	1063	1300049	1297764	384529	2957	114019	877	33989	261	10172	78
1223	439	536897	535236	159251	2966	47149	878	14000	260	4183	77
1223	853	1043219	1041144	309431	2966	91864	880	27070	259	7970	76
1223	877	1072571	1070472	318267	2967	94233	878	27826	259	8197	76
1223	1279	1564217	1561716	464049	2966	137745	880	40659	259	12099	77
1223	499	610277	608556	181335	2971	53666	879	15812	259	4625	75
1223	607	742361	740532	221088	2978	65635	884	19665	264	5892	79
1223	619	757037	755196	225505	2978	67326	889	19944	263	5951	78
1223	643	786389	784524	234340	2979	69635	885	20546	261	6110	77
1223	997	1219331	1217112	362442	2972	107700	883	32132	263	9654	79
1223	1069	1307387	1305096	388948	2975	115682	884	34552	264	10375	79
1223	1213	1483499	1481064	441962	2979	131184	884	39066	263	11583	78
1223	1237	1512851	1510392	450798	2979	134495	889	40038	264	11869	78
1223	787	962501	960492	287348	2985	85572	889	25530	265	7568	78
1223	823	1006529	1004484	300599	2986	89479	888	26832	266	7920	78
1223	907	1109261	1107132	331520	2988	99249	894	29754	268	8815	79
1223	1039	1270697	1268436	380115	2991	113430	892	33728	265	10119	79
1223	1087	1329401	1327092	397784	2992	118623	892	35437	266	10557	79
1223	73	89279	87984	26796	3001	8062	903	2440	273	717	80
1223	79	96617	95316	29003	3001	8672	897	2583	267	823	85
1223	97	118631	117312	35622	3002	10704	902	3274	275	962	81
1223	109	133307	131976	40036	3003	11952	896	3636	272	1120	84
1223	157	192011	190632	57691	3004	17360	904	5362	279	1634	85
1223	163	199349	197964	59898	3004	17971	901	5353	268	1608	80
1223	193	236039	234624	70936	3005	21015	890	6229	263	1875	79
1223	283	346109	344604	104051	3006	31144	899	9266	267	2718	78
1223	313	382799	381264	115092	3006	34638	904	10449	272	3096	80
1223	433	529559	527904	159253	3007	47845	903	14471	273	4407	83
1223	487	595601	593892	179129	3007	53773	902	16144	271	4839	81
1223	577	705671	703872	212255	3007	63748	903	19078	270	5637	79
1223	769	940487	938496	282931	3008	84880	902	25639	272	7729	82
1223	937	1145951	1143792	344774	3008	103720	905	31350	273	9458	82
1223	1129	1380767	1378416	415457	3008	124602	902	37437	271	11291	81
1223	1153	1410119	1407744	424294	3008	127650	905	38277	271	11426	81
1223	1249	1527527	1525056	459636	3009	138300	905	41567	272	12485	81
1223	1297	1586231	1583712	477306	3009	143539	904	43212	272	12953	81
1223	71	86833	85540	26805	3086	8330	959	2598	299	768	88
1223	281	343663	342160	106269	3092	32986	959	10345	301	3277	95
1223	491	600493	598780	185761	3093	57339	954	17675	294	5544	92
1223	701	857323	855400	265271	3094	81667	952	25080	292	7520	87
1223	911	1114153	1112020	344781	3094	106528	956	32819	294	10291	92
1223	881	1077463	1075360	353630	3282	115885	1075	37623	349	12103	112
1223	191	233593	232180	79807	3416	27390	1172	9442	404	3264	139
1223	761	930703	928720	318299	3419	108709	1168	37127	398	12866	138
1223	461	563803	562120	194625	3452	67261	1192	23185	411	8107	143
1223	1151	1407673	1405300	486170	3453	167843	1192	58133	412	20095	142
1223	311	380353	378820	132802	3491	46459	1221	16199	425	5573	146
1223	617	754591	752752	265299	3515	93326	1236	32994	437	11698	155
1223	431	527113	525460	185797	3524	65343	1239	22850	433	7925	150
1223	821	1004083	1002040	353648	3522	124416	1239	43902	437	15596	155
1223	1061	1297603	1295320	459671	3542	162738	1254	57465	442	20044	154
1223	1181	1444363	1441960	512682	3549	182229	1261	64664	447	23285	161
1223	971	1187533	1185340	424334	3573	151460	1275	54171	456	19275	162
1223	1031	1260913	1258660	450836	3575	160995	1276	57483	455	20516	162
1223	1091	1334293	1331980	477342	3577	171376	1284	61572	461	22120	165
1223	41	50143	48880	18040	3597	6514	1299	2410	480	879	175
1223	101	123523	122200	44511	3603	15923	1289	5725	463	2099	169
1223	131	160213	158860	57752	3604	20512	1280	7348	458	2627	163
1223	251	306973	305500	110731	3607	39829	1297	14477	471	5187	168
1223	401	490423	488800	176973	3608	63820	1301	23190	472	8443	172
1223	521	637183	635440	229972	3609	82938	1301	30037	471	10982	172
1223	641	783943	782080	282976	3609	101809	1298	36475	465	12880	164
1223	941	1150843	1148680	415499	3610	149798	1301	53794	467	19147	166
1223	1301	1591123	1588600	574534	3610	207614	1304	75081	471	26905	169
1223	239	292297	290836	106321	3637	38491	1316	14093	482	5131	175
1223	953	1165519	1163344	424333	3640	154327	1324	56232	482	20453	175
1223	1289	1576447	1573936	583374	3700	215686	1368	80159	508	29881	189
1223	743	908689	906724	344833	3794	130774	1439	49590	545	18767	206
1223	827	1011421	1009372	384588	3802	145794	1441	55313	546	20897	206
1223	1163	1422349	1419964	543624	3822	207183	1456	79003	555	29955	210
1223	113	138199	136864	53365	3861	20415	1477	7778	562	2983	215
1223	197	240931	239512	93095	3863	36177	1501	14001	581	5475	227
1223	449	549127	547456	212328	3866	81720	1488	31473	573	12113	220

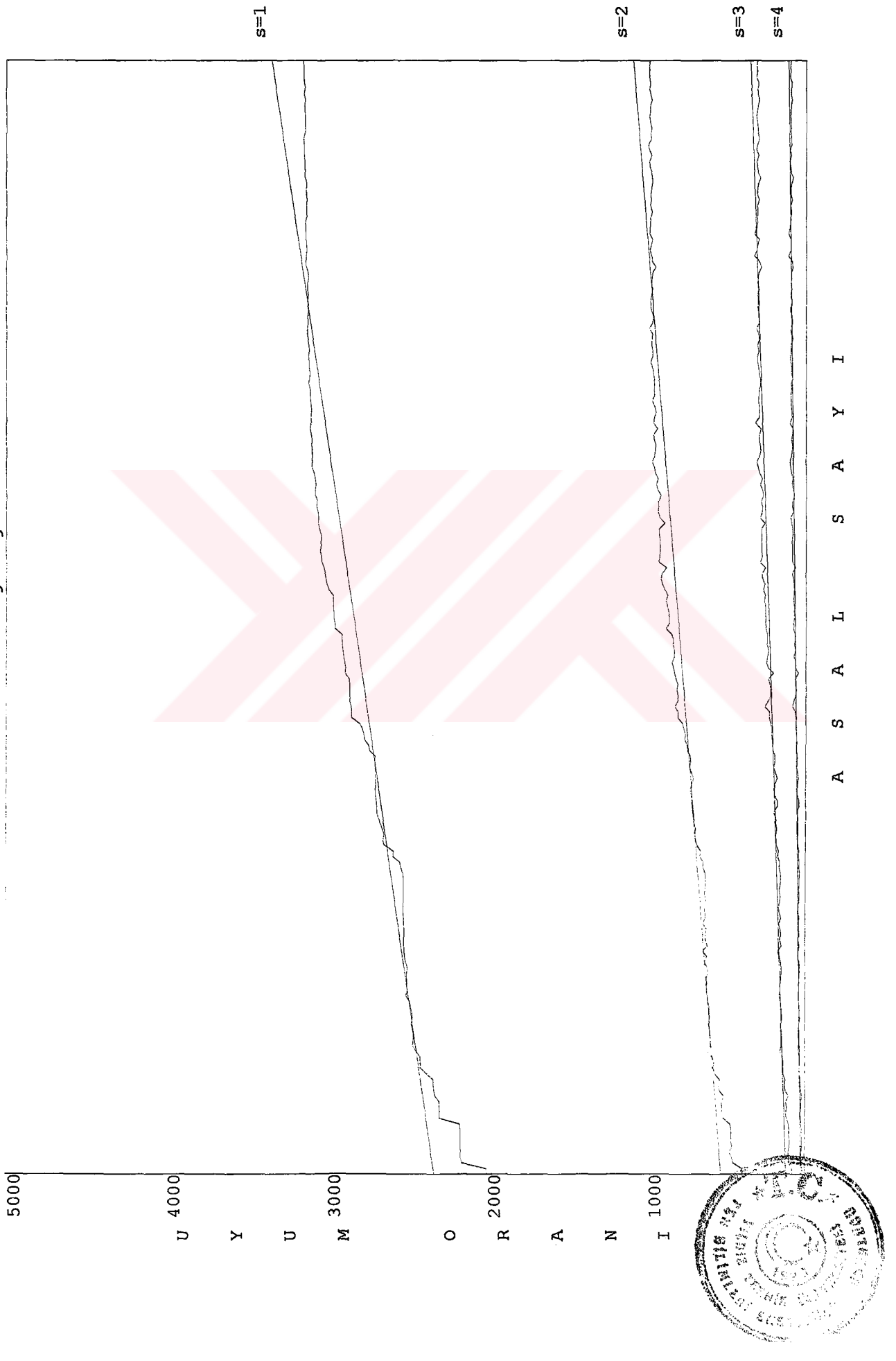


1223	659	805957	804076	311710	3867	120599	1496	46802	580	18205	225
1223	419	512437	510796	199081	3884	77497	1512	30316	591	11628	226
1223	1013	1238899	1236664	486200	3924	190862	1540	74981	605	29590	238
1223	683	835309	833404	331596	3969	131749	1577	52226	625	20620	246
1223	1277	1561771	1559272	618735	3961	245244	1570	97014	621	38523	246
1223	947	1158181	1156012	464119	4007	186273	1608	74617	644	29852	257
1223	647	791281	789412	318345	4023	128429	1623	51478	650	20713	261
1223	89	108847	107536	44564	4094	18285	1679	7557	694	3142	288
1223	353	431719	430144	177016	4100	72404	1677	29452	682	12025	278
1223	1103	1348969	1346644	556898	4128	230072	1705	95311	706	39545	293
1223	1259	1539757	1537276	636419	4133	262690	1706	108655	705	45066	292
1223	137	167551	166192	71061	4241	30063	1794	12753	761	5419	323
1223	443	541789	540124	230026	4245	97497	1799	41237	761	17456	322
1223	1217	1488391	1485952	636425	4275	271720	1825	115791	777	49242	330
1223	47	57481	56212	24733	4302	10692	1860	4594	799	1962	341
1223	599	732577	730756	316161	4315	136080	1857	58327	796	24991	341
1223	59	72157	70876	31354	4345	13574	1881	5870	813	2551	353
1223	233	284959	283504	124051	4353	53960	1893	23347	819	10156	356
1223	929	1136167	1134016	495065	4357	215567	1897	93764	825	40863	359
1223	149	182227	180856	79902	4384	34932	1916	15195	833	6554	359
1223	593	725239	723424	318375	4389	139807	1927	61458	847	26801	369
1223	83	101509	100204	44594	4393	19710	1941	8650	852	3727	367
1223	173	211579	210184	93148	4402	40842	1930	17780	840	7739	365
1223	107	130861	129532	57836	4419	25518	1950	11290	862	4997	381
1223	977	1194871	1192672	530411	4439	235322	1969	104067	870	45900	384
1223	269	328987	327496	146136	4441	64761	1968	28591	869	12542	381
1223	293	358339	356824	159385	4447	71170	1986	31570	881	14088	393
1223	569	695887	694096	309545	4448	137650	1978	61336	881	27307	392
1223	167	204241	202852	90947	4452	40365	1976	17895	876	8078	395
1223	179	218917	217516	97569	4456	43861	2003	19849	906	8939	408
1223	317	387691	386152	172633	4452	76669	1977	34018	877	15085	389
1223	227	277621	276172	124061	4468	55459	1997	24669	888	11038	397
1223	389	475747	474136	212380	4464	95138	1999	42785	899	19480	409
1223	809	989407	987376	442064	4467	197355	1994	88299	892	39408	398
1223	263	321649	320164	143931	4474	64240	1997	28770	894	12948	402
1223	509	622507	620776	278629	4475	124779	2004	56020	899	25136	403
1223	557	681211	679432	305132	4479	136610	2005	60783	892	26976	396
1223	857	1048111	1046032	468568	4470	209376	1997	93961	896	42198	402
1223	1049	1282927	1280656	574591	4478	257677	2008	115594	901	51816	403
1223	347	424381	422812	190299	4484	85436	2013	38516	907	17511	412
1223	359	439057	437476	196923	4485	88321	2011	39453	898	17592	400
1223	383	468409	466804	210172	4486	94426	2015	42183	900	18877	403
1223	653	798619	796744	358136	4484	160529	2010	71847	899	32083	401
1223	773	945379	943384	424395	4489	190491	2014	85339	902	38335	405
1223	797	974731	972712	437647	4489	196287	2013	87707	899	39456	404
1223	1097	1341631	1339312	601097	4480	269473	2008	120942	901	54523	406
1223	1193	1459039	1456624	654109	4483	292700	2006	131053	898	58710	402
1223	53	64819	63544	29165	4499	13199	2036	5900	910	2544	392
1223	467	571141	569452	256546	4491	115611	2024	52280	915	23632	413
1223	479	585817	584116	263172	4492	117991	2014	52844	902	23651	403
1223	503	615169	613444	276423	4493	124249	2019	55939	909	25028	406
1223	563	688549	686764	309548	4495	138983	2018	62283	904	27697	402
1223	587	717901	716092	322800	4496	144905	2018	65116	907	29155	406
1223	719	879337	877396	395682	4499	178272	2027	80125	911	35813	407
1223	1109	1356307	1353976	609932	4497	273753	2018	122994	906	55152	406
1223	1229	1503067	1500616	676199	4498	304622	2026	137382	914	62081	413
1223	257	314311	312832	141727	4509	63661	2025	28679	912	13001	413
1223	839	1026097	1024036	461945	4501	207929	2026	93413	910	41893	408
1223	863	1055449	1053364	475197	4502	214059	2028	96430	913	43491	412
1223	887	1084801	1082692	488449	4502	219577	2024	98577	908	44244	407
1223	983	1202209	1200004	541460	4503	243733	2027	109509	910	49262	409
1223	1019	1246237	1243996	561339	4504	252461	2025	113185	908	50779	407
1223	1187	1451701	1449292	654110	4505	294942	2031	132828	914	59977	413
1223	1283	1569109	1566604	707124	4506	318809	2031	143613	915	64466	410
1223	677	827971	826072	373599	4512	168397	2033	75675	913	34039	411
1223	1223	1495729	1493284	675096	4513	304093	2033	137039	916	61724	412

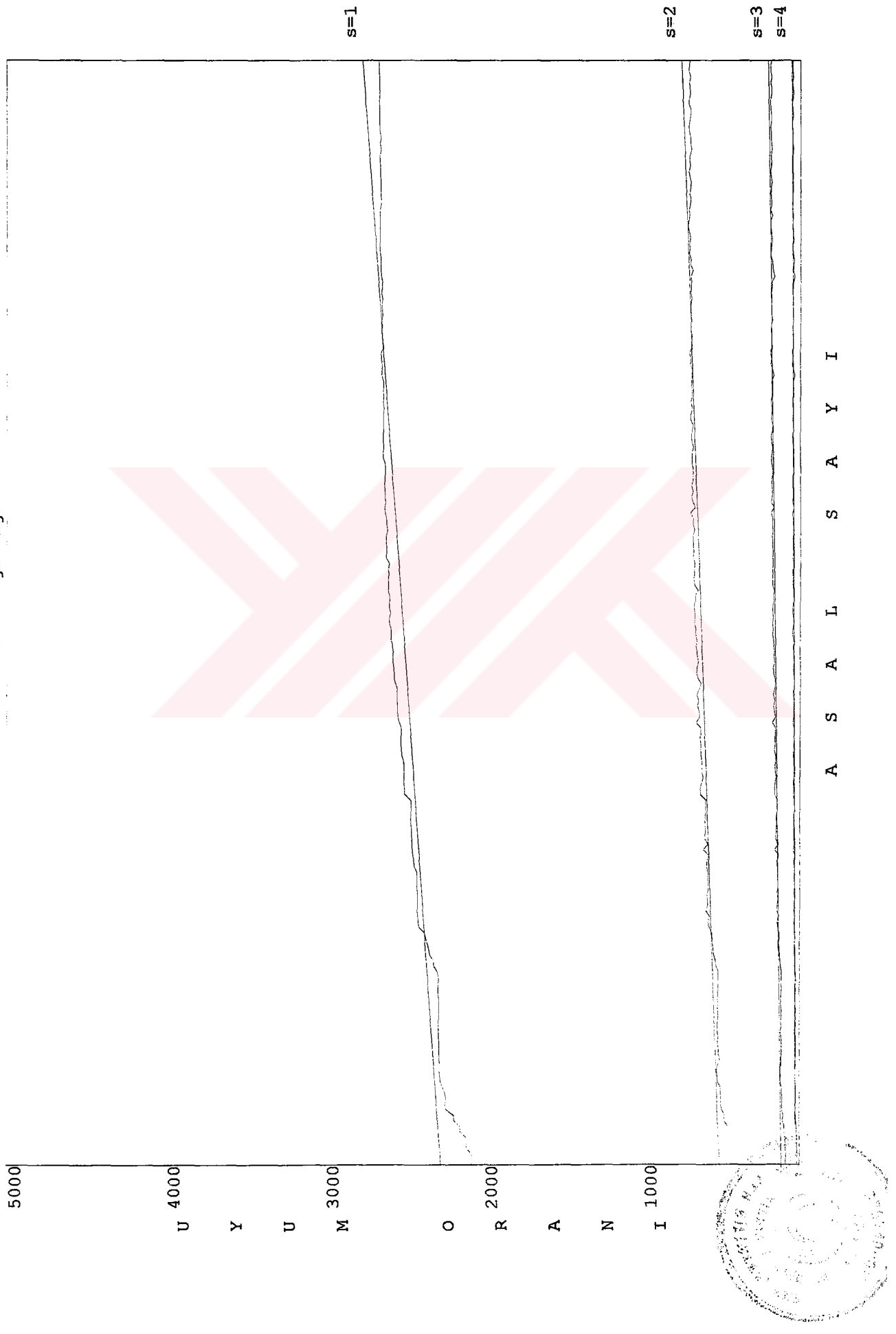
Ek-E-13
Ek-D-13 grafigi



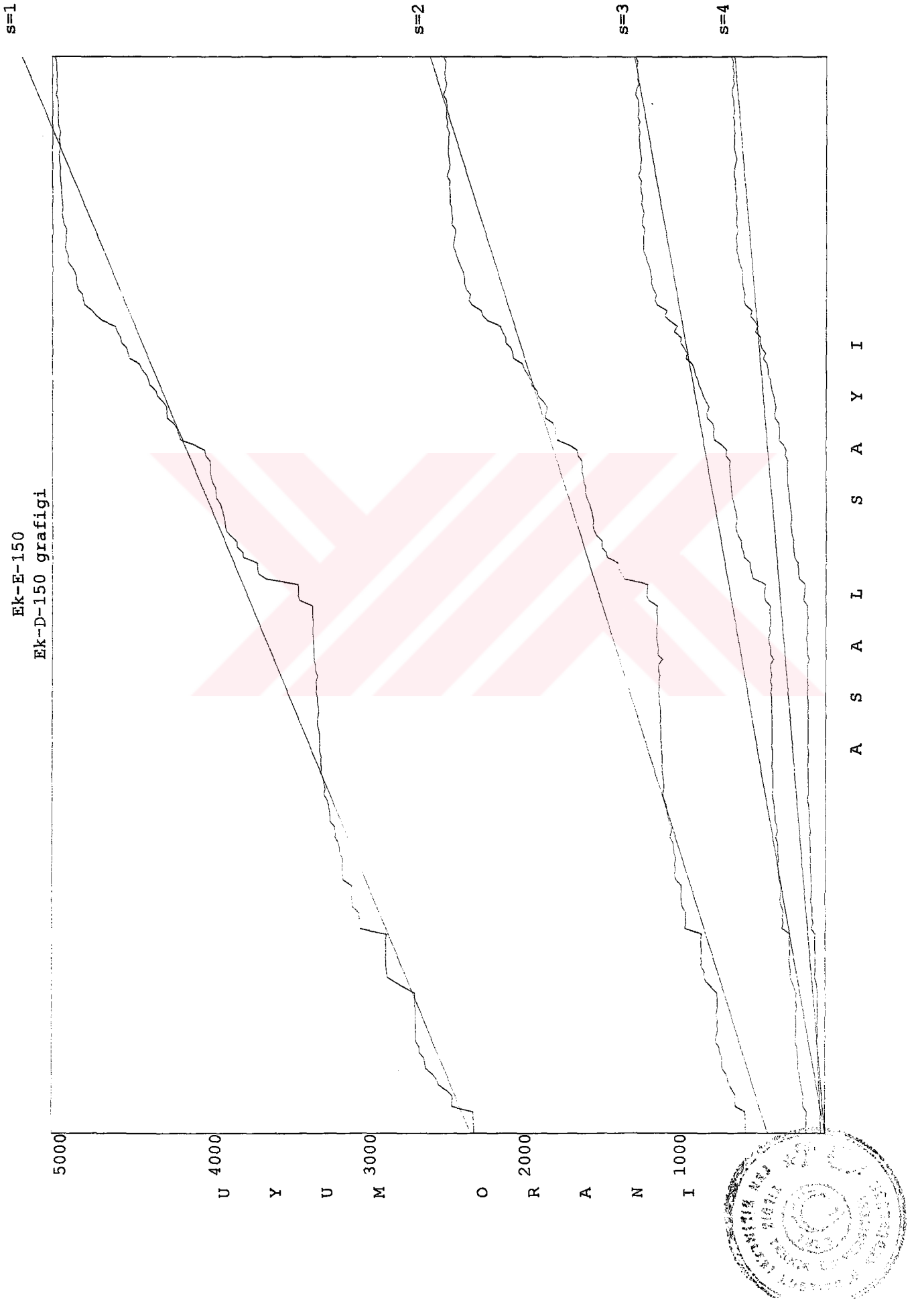
Ek-E-50
Ek-D-50 grafigi

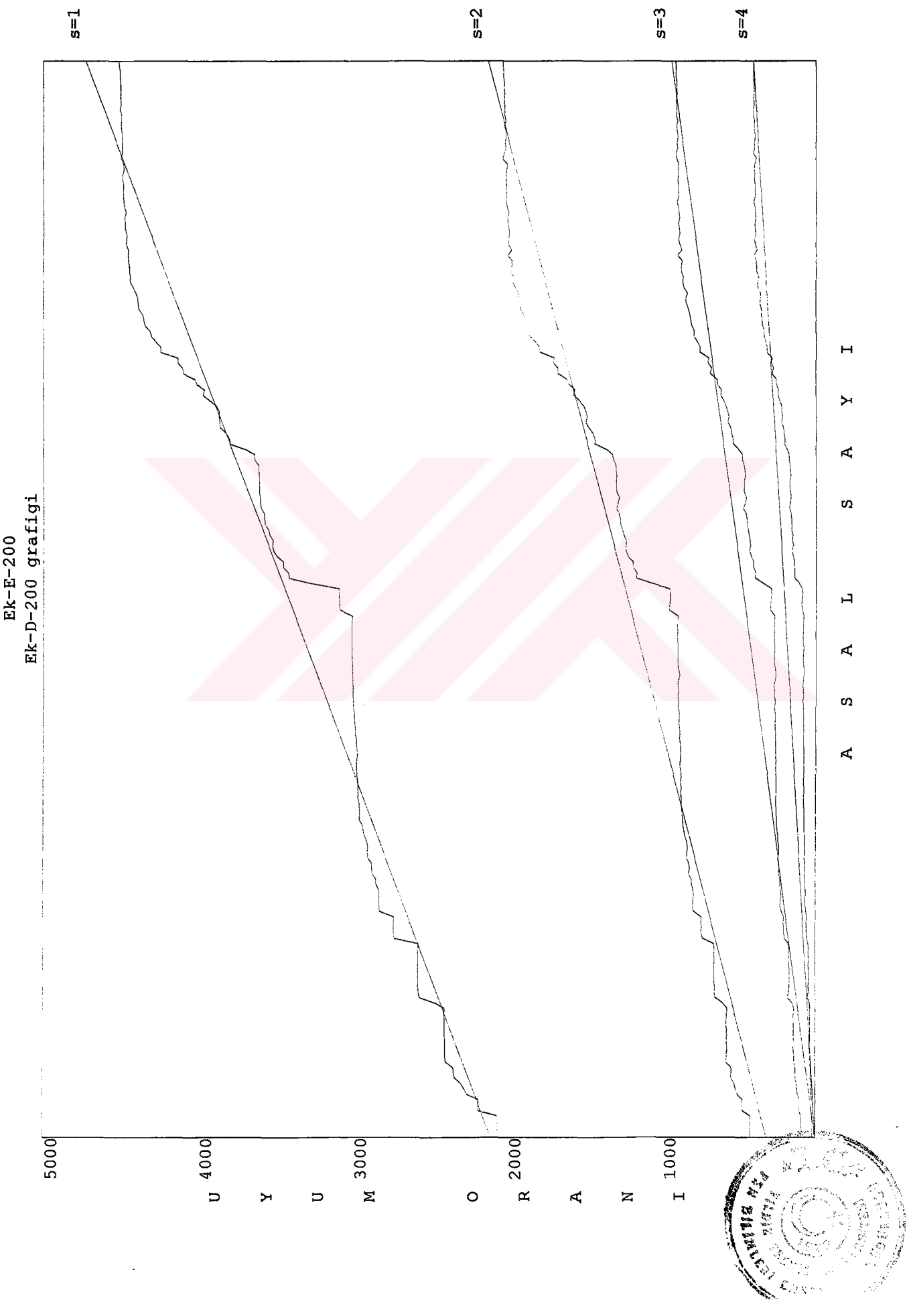


Ek-E-100
Ek-D-100 grafigi



Ek-E-150
Ek-D-150 grafigi



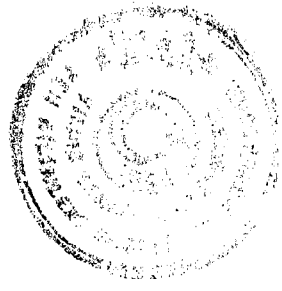

Ek-E-200
Ek-D-200 grafigi
s=1
s=2
s=3
s=4
5000
4000
3000
2000
1000
U Y U M O R A N I
A S A L S A Y I

Ek-F-1
Sistem sayıları ile Seviye Anahtarları

Sembol	Değer
M	43841651828672405848059309709515750136971
a	59928302355241427583868506337732586811191
p	62228809749892649614109586926888399956309606359249805529046 1
q	46695238499321305088763925547134075213191172396379432249800156761564 91
n	29057891128001282466182501703839299752671535452630581345971293032125 60045554669489128154423979417708353075383058084126437095532351
$\phi(n)$	29057891128001282466182501703839299752671535452630581345971246336887 09491136063113809103569476027120351836182018795553923364085400
d_1	161716115508631835982635085434711223837385611907245380204172332975 3
e_1	13252356495563795285394549975383744787312576969256186422332195692226 87995626230190588495292956241371426373181570941238314764111017
d_2	73170135644984406156461732149175338062535034074106863768663566368407 47671034070568046548442600792108474173697465972610815039282175
e_2	37316743966042782328066146074356074463502773941960674284538493005579 06575003238221430361847275242793222683379163627447335775473 53
d_3	61824372286690061065213563339988698176993507028439020771371743558479 26568148533321442971669153742403176140868727243167824084194695
e_3	15656478436682986353338052426039868881442191540831774587229660611894 42796599236847416181794590887003434013392182549817045627431629
d_4	12985383866032842227305697628590877954454523092569420805643616725519 49990273987756416707949276011409842901115233627402870514005033
e_4	18085984289598764270423621095607785952423050085453337586991506016522 09425421231708134539884184468174191937864430673713186588175297
d_5	76311726512906032958047552547635439011181009068129160687577069043517 72919418959394532910347583578930837477096618856138770689410 89
e_5	90211897739648343016725914946252515879377348959969093348196965004751 85393814023651402625017707337504356720471708973036583664150 09
d_6	79223351950182286927214789760276227921662397523602628892256597800430 58162247386659047521058119071663862773976023807488188831982 93
e_6	55057433367966046092827139762356504294172576737426899679216475799492 43217393057883571424696293122993386220004529134124757897069 57
d_7	20643370308554553302407338922127424969953708941613291695682964081074 86958537723178458159975371408080159880929312581251301564273 57
e_7	15962620840502324061524142639868879234191841121152152797801330452823 73616791974916341268171337603546437060333237368036987690183293
d_8	90676281310915405127594933083786381879004040271945250814949403021083 02450541587101365978049854702927351872924916392432489575592 97
e_8	56166495713425699337900288936943816019398067606216076432334036293431 48713424055896786288154971882209063028299877619462826245308 33
d_9	30009970068088658535317641694768460394107120916997601019299156057073 58773832422234538459185751868957418277573114158961753156845 87
e_9	95278520198770229990367758068689747543871348205407892445028174568295 21335492882166476735809998020894879542765321326952837100759 23
d_{10}	78710738824529172575280923910315470981608598517009225670362166852344 74230261312385075710820960806015171803346077044345617924697 11
e_{10}	19853494840062534460776765775950709830427228587578957397773808221794 08787278422447089865303649676308416072859329610372597003935 91

Ek-F-1
A Grubu Şifreleme İşlemleri

g	651351673460003571830032721125092823717828175849441735756008682841686392 92704514371260219498507463 81
g^a	125765276378066773452505344688651096502302454030780225410921225992233660 82820238208466774572261650300395712385403126755974996943 62
g^{-a}	368234008734215766469700527806503047855220711953223067491030345084400896 40010707032253419648406708238785451674807682484342312948 5
$(M * g^{-a})$	107537346204758568377381355908908869491222830680606644746658601870323034 97775327973845267221505561151847098736827068332511118179 68
$(M * g^{-a})^{e1}$	108455429219643827276279446820883485611322624556016565496407948483782098 53337319893439695078816167598812067028140321095165432287 89
$(M * g^{-a})^{e2}$	243678840950409662356993397791206504290488454179687165627318429854447449 53988149723302609548758866314058994356274196808631612448 5
$(M * g^{-a})^{e3}$	260653740968230524340906664519380578928472953997203880339319281764172643 54479261435664734789998551104030979005976154485188751691 28
$(M * g^{-a})^{e4}$	187212312226490838319252806332701728826432513551264105733757118206882311 22240601494212771430740415704220466047493091200440799688 0
$(M * g^{-a})^{e5}$	326775778739200327246288905981907126531645886664778285494379372921721553 84902660187633620922270271798654890273357979088630800057 1
$(M * g^{-a})^{e6}$	225753737217314592425407445908088242859065113750199185831266538857998079 49946717899553855924282460751281027740361520667946205950 08
$(M * g^{-a})^{e7}$	205383952520107335305221317475389540802617033322019356451020087146634621 79425331661867021199395855480289045722332126854661000562 88
$(M * g^{-a})^{e8}$	276316729260863674947874729494525926649084733921856570772753355208417956 68268923892779064834006870272153285328463513745462306984 71
$(M * g^{-a})^{e9}$	236190923656718081474067962462346360392061889799336111134010482363083359 72795510877442028421666956584240805355801369638652256937 37
$(M * g^{-a})^{e10}$	191499027245970502382854321319463536940639715886883543921685972553577781 87991518466774242031655388322725287415829067593979525365 07

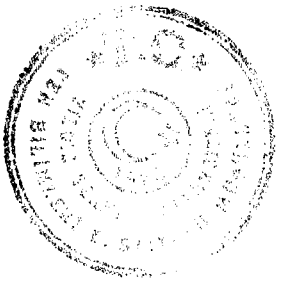


Ek-F-1
A Grubu Şifre Çözme İşlemleri

$((M * g^{-a})^{e1})^{d1}$	1075373462047585683773813559089088694912228306806066447466586018703230349777532797384526722150556115184709873682706833251111817968
$((M * g^{-a})^{e2})^{d2}$	1075373462047585683773813559089088694912228306806066447466586018703230349777532797384526722150556115184709873682706833251111817968
$((M * g^{-a})^{e3})^{d3}$	1075373462047585683773813559089088694912228306806066447466586018703230349777532797384526722150556115184709873682706833251111817968
$((M * g^{-a})^{e4})^{d4}$	1075373462047585683773813559089088694912228306806066447466586018703230349777532797384526722150556115184709873682706833251111817968
$((M * g^{-a})^{e5})^{d5}$	1075373462047585683773813559089088694912228306806066447466586018703230349777532797384526722150556115184709873682706833251111817968
$((M * g^{-a})^{e6})^{d6}$	1075373462047585683773813559089088694912228306806066447466586018703230349777532797384526722150556115184709873682706833251111817968
$((M * g^{-a})^{e7})^{d7}$	1075373462047585683773813559089088694912228306806066447466586018703230349777532797384526722150556115184709873682706833251111817968
$((M * g^{-a})^{e8})^{d8}$	1075373462047585683773813559089088694912228306806066447466586018703230349777532797384526722150556115184709873682706833251111817968
$((M * g^{-a})^{e9})^{d9}$	1075373462047585683773813559089088694912228306806066447466586018703230349777532797384526722150556115184709873682706833251111817968
$((M * g^{-a})^{e10})^{d10}$	1075373462047585683773813559089088694912228306806066447466586018703230349777532797384526722150556115184709873682706833251111817968
$((M * g^{-a}) g^{a}$	438416518286724058480593097095157501369 7

Ek-F-1
B Grubu Şifreleme İşlemleri

g	207472224677348520782169522210760858748099647472111729275299258991219668475054965831008441673255007 7
g^a	245260209101123813010450163721126335545929224916066269289475576891833874313203937380082066961388262071694110925735458890012920514 3
g^{-a}	791260062562259707567447717121590577857792138972553879563719662183397298506312468246139931401532473560820001672653028136881682050
$(M * g^{-a})$	189752187360951916665985720710488451280334998935070580708375290487088881704924776267850876522816226007179426190907731185249028561 8
$(M * g^{-a})^{e1}$	385862442277676495386756014882851656187561717285692180721074827262278392418458320191860954068579051613225944101151864548654812 02
$(M * g^{-a})^{e2}$	167931793157197769691027504338430209519061168857275179194347398992467063887770619794886570350866545165307205680907110284514459358 4
$(M * g^{-a})^{e3}$	141724704463299781589093501386083462368783688634926766490815142109887274979043799713745831266249270153522332370997053301352395355 9
$(M * g^{-a})^{e4}$	251450731601556944170162758720227386851990787520085507655966885848288638366485540386010918295893477988736895949213821558021318191 5
$(M * g^{-a})^{e5}$	209029998020029672495101858104282090154098209352473662788115433764622190910150330181824509584174805618863092663939311817484347023 4
$(M * g^{-a})^{e6}$	647031791392197842004960433125182358197114408895853105990130935319711419918241467932658919157745039063180624111128579130934263094
$(M * g^{-a})^{e7}$	233034496345902059868946692738431530683352664001208015632062900632169357634597352940319494266909539310311530906173690624192107262 0
$(M * g^{-a})^{e8}$	144058176099583746199240726688289989951144196749208354220549856705136822660923317982125547264050717271127171252955542857179289621 4
$(M * g^{-a})^{e9}$	256242658617369822552020353427108025299533108334792724586240408543006113756224772672026830693406250341205709066542647675348998778 6
$(M * g^{-a})^{e10}$	274744367770670770582633913014941247018181375548595702318753115600569230410026253359635960743477359779227607786656834503508398748 3



Ek-F-1
B Grubu Şifre Çözme İşlemleri

$((M * g^{-a})^{e1})^{d1}$	189752187360951916665985720710488451280334998935070580708375290487088881704924776267850876522816226007179426190907731185249028561 8
$((M * g^{-a})^{e2})^{d2}$	189752187360951916665985720710488451280334998935070580708375290487088881704924776267850876522816226007179426190907731185249028561 8
$((M * g^{-a})^{e3})^{d3}$	189752187360951916665985720710488451280334998935070580708375290487088881704924776267850876522816226007179426190907731185249028561 8
$((M * g^{-a})^{e4})^{d4}$	189752187360951916665985720710488451280334998935070580708375290487088881704924776267850876522816226007179426190907731185249028561 8
$((M * g^{-a})^{e5})^{d5}$	189752187360951916665985720710488451280334998935070580708375290487088881704924776267850876522816226007179426190907731185249028561 8
$((M * g^{-a})^{e6})^{d6}$	189752187360951916665985720710488451280334998935070580708375290487088881704924776267850876522816226007179426190907731185249028561 8
$((M * g^{-a})^{e7})^{d7}$	189752187360951916665985720710488451280334998935070580708375290487088881704924776267850876522816226007179426190907731185249028561 8
$((M * g^{-a})^{e8})^{d8}$	189752187360951916665985720710488451280334998935070580708375290487088881704924776267850876522816226007179426190907731185249028561 8
$((M * g^{-a})^{e9})^{d9}$	189752187360951916665985720710488451280334998935070580708375290487088881704924776267850876522816226007179426190907731185249028561 8
$((M * g^{-a})^{e10})^{d10}$	189752187360951916665985720710488451280334998935070580708375290487088881704924776267850876522816226007179426190907731185249028561 8
$((M * g^{-a}) g^{a}$	43841651828672405848059309709515750136 97

Ek-F-1
C Grubu Şifreleme İşlemleri

g	23674957702171429952648279486668092330664094976998701120031493523803751 24855230068487109373226251983
g^a	70603143148965101432773216446981261762990247798449893438673783225934129 39980916692259615776139171033045473656896922350991311726O5
g^{-a}	11198450671785157451678690258870379033730863317356423981740650367964968 83263252232171405985593677334661487459750176965324478529957
$(M * g^{-a})$	11937110785365834993670929317873436014738570867968854248056990836568979 12479592012025407362466739570697336774819862421563065307690
$(M * g^{-a})^{e1}$	19349168156232837594901573691886357083704006106309478860532689593077238 13722772854274584025599561752426276143653181622067229599085
$(M * g^{-a})^{e2}$	13410201764165588687702738082997866763140057875589603772592300268886741 49293332093321880603995840414744850023569427258259162304316
$(M * g^{-a})^{e3}$	25341824384563342851903274147578539098594367874157695854774415220847021 74303772454725504520313282166526549535524737339677449628683
$(M * g^{-a})^{e4}$	19612282196488002170844782847227276010957616881189623781487521314166065 25221334298123909873062330827494996342316706230752216939597
$(M * g^{-a})^{e5}$	11414558735745362466495025819927681177588534837988220599705817199130644 74648912102522396568752779954697808472702363112842864848l1
$(M * g^{-a})^{e6}$	18159812440753475085936890694475151214031932060926150866170630908283417 08032089987670035039759451909027316020252967940433934118954
$(M * g^{-a})^{e7}$	20158195732840896379585199189421737418195292919328716973631335099181167 17006999640473827559739967259612671687497011224201187148917
$(M * g^{-a})^{e8}$	11960595237330621157939521411421691297638346057647972185891691193125572 07702706321330202148761366881244021061449610821946297037868
$(M * g^{-a})^{e9}$	21226693265695745368898241473540693329988251347303004660154763356088762 44334152408111466571619840857856729387753377664814155029673
$(M * g^{-a})^{e10}$	26073641866189361555619970903960416245088070710223949689554581639245950 68310164933066887955498193146919721643852611855252504819834

Ek-F-1
C Grubu Şifre Çözme İşlemleri

$((M *g^{-a})^{e1})^{d1}$	1193711078536583499367092931787343601473857086796885424805699083656897912479592012025407362466739570697336774819862421563065307690
$((M *g^{-a})^{e2})^{d2}$	1193711078536583499367092931787343601473857086796885424805699083656897912479592012025407362466739570697336774819862421563065307690
$((M *g^{-a})^{e3})^{d3}$	1193711078536583499367092931787343601473857086796885424805699083656897912479592012025407362466739570697336774819862421563065307690
$((M *g^{-a})^{e4})^{d4}$	1193711078536583499367092931787343601473857086796885424805699083656897912479592012025407362466739570697336774819862421563065307690
$((M *g^{-a})^{e5})^{d5}$	1193711078536583499367092931787343601473857086796885424805699083656897912479592012025407362466739570697336774819862421563065307690
$((M *g^{-a})^{e6})^{d6}$	1193711078536583499367092931787343601473857086796885424805699083656897912479592012025407362466739570697336774819862421563065307690
$((M *g^{-a})^{e7})^{d7}$	1193711078536583499367092931787343601473857086796885424805699083656897912479592012025407362466739570697336774819862421563065307690
$((M *g^{-a})^{e8})^{d8}$	1193711078536583499367092931787343601473857086796885424805699083656897912479592012025407362466739570697336774819862421563065307690
$((M *g^{-a})^{e9})^{d9}$	1193711078536583499367092931787343601473857086796885424805699083656897912479592012025407362466739570697336774819862421563065307690
$((M *g^{-a})^{e10})^{d10}$	1193711078536583499367092931787343601473857086796885424805699083656897912479592012025407362466739570697336774819862421563065307690
$((M *g^{-a})g^{a}$	43841651828672405848059309709515750136 97

Ek-F-1
D Grubu Şifreleme İşlemleri

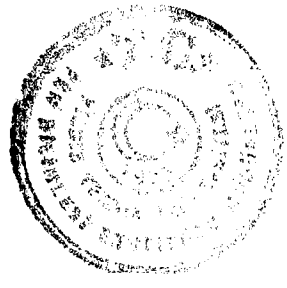
g	181415956681997030798268171682210701603892017050439145746256348519812691673516726021561952342971403 1
g^a	818715283553783501059509737962254077338038942255464542685055751408310310038824013576525189763514275601790897510466837013696369839
g^{-a}	224631824091900358079286142536625210127762757385227943503772411004221495564384125020851020241457928228820085440926782927655507262 5
$(M * g^{-a})$	198797754345135430987130741153325613891239631466988324336018142624272542989071313638794698799616119539189678467162293802946068427 1
$(M * g^{-a})^{e1}$	244567097333647563332296687570129716035184473199438843931957179690387890374313756933994094799887145212906816056378441163607704658 7
$(M * g^{-a})^{e2}$	282606286625230802944980298599411041604325654611529684630356848156387785120373491194760843654747982635476281663510508353660184158 4
$(M * g^{-a})^{e3}$	237189701673186411090158822885903632079676206339483361493084337919662391490317602235679044159921393963332325803492793620011009911 1
$(M * g^{-a})^{e4}$	148057255409977027136358833271131657926421860447187016895441338783433046681470414876373977705285159154611891456506430009859369506 3
$(M * g^{-a})^{e5}$	208895534743867562828698791017754833564617696698229297985480452551143224699050711028425048558319054980515890804757100117845720656 3
$(M * g^{-a})^{e6}$	211704899408722801824444580758036560284082536511854210208808732986741692552474357808316490695440772012170211490006343814195610209 0
$(M * g^{-a})^{e7}$	501100019269447174361090124123052180697292232023017440513887819873082847796682417730718533994165526756601405624362352115787757791
$(M * g^{-a})^{e8}$	309051766520378580168015813383269878392634615541210805443916279004343745192951274850781868054561891596774788572949883568422103337
$(M * g^{-a})^{e9}$	192914529804674352062164708646394306220290988665620264055681081078315238248152355883381204946903647198035190047041720072049250664 1
$(M * g^{-a})^{e10}$	137256636401544186666602609461407118770182051028500941639438130898757904923935263966613979128562189741426628361202275857006975303 2

Ek-F-1
D Grubu Şifre Çözme İşlemleri

$((M * g^{-a})^{e1})^{d1}$	19879775434513543098713074115332561389123963146698832433601814262427254 29890713136387946987996161195391896784671622938029460684271
$((M * g^{-a})^{e2})^{d2}$	19879775434513543098713074115332561389123963146698832433601814262427254 29890713136387946987996161195391896784671622938029460684271
$((M * g^{-a})^{e3})^{d3}$	19879775434513543098713074115332561389123963146698832433601814262427254 29890713136387946987996161195391896784671622938029460684271
$((M * g^{-a})^{e4})^{d4}$	19879775434513543098713074115332561389123963146698832433601814262427254 29890713136387946987996161195391896784671622938029460684271
$((M * g^{-a})^{e5})^{d5}$	19879775434513543098713074115332561389123963146698832433601814262427254 29890713136387946987996161195391896784671622938029460684271
$((M * g^{-a})^{e6})^{d6}$	19879775434513543098713074115332561389123963146698832433601814262427254 29890713136387946987996161195391896784671622938029460684271
$((M * g^{-a})^{e7})^{d7}$	19879775434513543098713074115332561389123963146698832433601814262427254 29890713136387946987996161195391896784671622938029460684271
$((M * g^{-a})^{e8})^{d8}$	19879775434513543098713074115332561389123963146698832433601814262427254 29890713136387946987996161195391896784671622938029460684271
$((M * g^{-a})^{e9})^{d9}$	19879775434513543098713074115332561389123963146698832433601814262427254 29890713136387946987996161195391896784671622938029460684271
$((M * g^{-a})^{e10})^{d10}$	19879775434513543098713074115332561389123963146698832433601814262427254 29890713136387946987996161195391896784671622938029460684271
$((M * g^{-a}) g^{a}$	43841651828672405848059309709515750136 97

Ek-F-2
Sistem sayıları ile Seviye Anahtarları

Sembol	Değer
p	622288097498926496141095869268883999563096063592498055290461
q	466952384993213050887639255471340752131911723963794322498001567615649l
n	290578911280012824661825017038392997526715354526305813459712930321256004555466948912815442397941770835307538305808412643709553235l
$\phi(n)$	290578911280012824661825017038392997526715354526305813459712463368870949113606311380910356947602712035183618201879555392336408540 0
d_1	64686446203452734393054034173884489534954244762898152081668936974l
e_1	213243442105422827964255529383617605564706132197738214982179419214979302481408577854814549594114201037228955908983690320899903766l
d_2	14951982293299318732321522983878048632939234638025568978508101004974853 7
e_2	11429518989262150513834059251333541885192005226263481663587736064540133632595477462871055934673696354640840096911136886773176546733
d_3	25795061563712299187098399348172647228404124738074736569757588977302112211150568468598162163226921780949941181070077542801591333389
e_3	13158279547239125146406624237775570733411794845474688835015053164228140976828965222044635684784001558215397156889629260687387169090
d_4	50085069424772990906786007685788346508105079989848864944967116986734240520994593876763774742575445913340859720993413989785714040 3
e_4	26608471459250284948984618852927712180711195383014495630762327650508041758208256315352655791919678000181785284703187266435543446l7
d_5	25611602224524776784629871707382190972427841848451812932189446431888538315476880556391056585969813591577728026024450967683896076l7
e_5	85505902155818182250896191171735427492719480885506938803071148391003278858076392087129770582214869135393026191335256390840069634 3
d_6	25689037267876253025426968933276048547836154121524869992923431865121366379955255105956420178525873674856601934927716721070413205l7
e_6	27037677404488678239808623696107475221486401354520546606288664451871362000276486869487308316167634843628183776828510112260247076l3
d_7	25553740145338996716195302389868672195782966567404624952397786071290487733747768270859394018780702742263357119935173360122066518l1
e_7	81974404519101905124106282597848406078617445036765499937589001598468769125986644453911881752576203066907048618516826333110081449l
d_8	11566775890732708464627360888525700315336477518975048616936197650285151030917976999251885975236842290887143734505299537279908270l9
e_8	84889635759032037810156643892001393346662523539921325641136187671073574872234829737869599489177438397666238008309465594471538864l
d_9	22517471089381356753422963861972750834170083875616708285832384992836923500392339598881539814670119793720849999341325431948939010l1
e_9	16889405136873193010668613977133234541804951786858643347888902549013963784801025647130705547214432344414545810889921816065570336l1
d_{10}	95391590500979729063288432684888046786885122753735434649540205896926514500229681020911525902710854880388532168219384820340442592 9
e_{10}	67967726255719689792085128533948753648717649049157780542368246726497171291691202823673795833265980023394998781521277072723556016 9
d_{11}	10603655764873925911376838895137978883340284286144715533803089803106193109475652972809098637094518171395268537113715514105914863l3
e_{11}	13046796340841675400867114860461907751280583154850012308592038724276118058925214268812797942332886422833019223586993967836730824l7



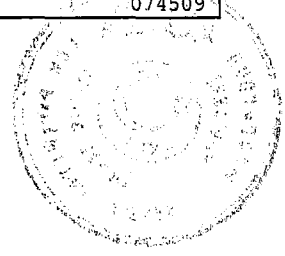
Ek-F-3
Sistem sayıları ile Seviye Anahtarları

Sembol	Değer
p	185323955009471744507093833849366798683834244443114056794632807824057962331639 77
q	282755483533707287054752184321121345766861480697448703443857012155326440743976601304240257 1
n	524013645090821979473180293242354572577178846519482878737641104334621362706388822663800529464312102029916678856080019578845825620094242530679723148447686610196908938486 7
$\phi(n)$	524013645090821979473180293242354572577178846519482878737641104334621362706388794388252174240343846459980801673007104399029769036881453713837939875678864393015981381832 0
d_1	457826886537180985369990597552922849342604056517217004216176482949781513619622507729 3
e_1	952906526299441581022312686443678399429374320453951872463414570098193186501431580801263236733508058705117287827626562076397854811144126906784467860361758116538780753 17
d_2	594973097158120365307519923329780839603215060541892816441358505052973047430246767466668381
e_2	145394733070280483842631015444572306933728020737386148031798588144753467257554524605971707920612089631138703124993598074902649902413065040179563833180869390844796411882 1
d_3	517842656858135903522259789569395649454837188143640258752569575616302745676788162899902219645868827327304521355883431052414075110391827890490173427627565679991077972252 9
e_3	142850862244913486181071456914851168261155431078124541698797016050668545677974488217992635727179762031890489819663170926482649420253542990418652205026988093148502917124 9
d_4	468151264966435480390269457773602506565899891611658227753142094338431313839695708687027633567806354537216074427257522455403376105834383052570881895439908173288644961320 9
e_4	291025076300458530773279651628521990594507945773163081421483476208272068444168976007011730467391455778033072774323802710830564491261675354360559930031137686133509749456 9
d_5	360449922674800774096324490488483333228739511787826995125234645277231766386529167759401062910416712652157717964407062473714569173615312813505995490803236766595707242860 3
e_5	218403859652257624995990310756716210652690929190480556982007166434440221085442715016582468487406515289887830413114050679008327251404702094789132017062732876943208316222 7
d_6	260502359565071715309605391761063561532798372720628907322460661114619284691983318393854348803887904738319487413563621845621509299706046802446626691767787456572983584410 9
e_6	125852628391895073928774976038241734980556644000306426770431932017240331880461150983111471909345366393434363471597806594120460253125999904949068885146684555855423437795 09
d_7	506846170881010081595835020894349110204065931352818532340291149582814646113122416652597416184266876776983364619427792061626091902394250000327604253283358234026548185131 9
e_7	143572511649603789070036775371181842133251345446140536508142135128591271693495616951001125731550702762149535716478443687783470987795954105649383359295120451001717016075 9
d_8	220546984785518037475412386382565955502292754541689851270374462426191615837153858501612520835955548888258420979919920335218028150085536783007793639429542292569798100221 1
e_8	367056732827839159195628673434611749493369529308574084197342380433160758891159909431751370608821799124007409275188121615175340478584168882111268802921684045311369827737 1
d_9	812238195821823021842999123359429004330990164709803557272781094146910112005090671406333829212707627760528351595125612619296698803126304453527311070924073031373028345731
e_9	436976342395892308687858168626175381350342657651051931153366465761165386107495756996517594341436889822990929799839522804656457154036899543167105595428546327355094888721 1
d_{10}	902000564463901254048856376400854641436727283209687952691161344162754788898859024645938673014359174710674515613820208797189862100556917506845830257843499290944282695669
e_{10}	433932476198818790407322582035170208605169890337870960012200467975174 94

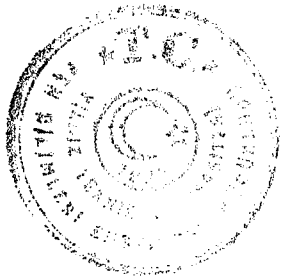
	075912654122349063041778541393260213281940096233617931974966596392462400667111807168735559312713 09

Ek-F-4
Sistem sayıları ile Seviye Anahtarları

Sembol	Değer
p	20747222467734852078216952221076085874809964747211172927529925899121966 847505496583100844167325500 77
q	49949091806585030192119760356408111278062369027342098434296869059406461 21085912172293044610060051708652944665271663688 51
n	10363049197725317508669387683496701839236198913033989136856985863094448 68089174229195716248366153402959491569020359019704074688304997565650402 53565289851373218837356747929481574452420959789063509745266015257210961 0451527
$\phi(n)$	10363049197725317508669387683496701839236198913033989136856985863094448 68089174229195716248366153402460000650954508717780802362494142967661957 15015736992080173868649869356541440031439038123294434173213654802116571 1532600
d_1	64383380457150019108049430636514587981992776123653960756109147769453967 41942919519896774972258058684244896078 9
e_1	10791439663276929341688056330575584359249977446556106381926655694171510 72774675772925380665526646130933249468945476316797228932406897172091521 37162219347743943103894170169796751432016632241168863427728774579423150 074509
d_2	64383380457150019108049430636514587981992776123653960756109147769453967 41942919519896774972258058684244896078 9
e_2	10791439663276929341688056330575584359249977446556106381926655694171510 72774675772925380665526646130933249468945476316797228932406897172091521 37162219347743943103894170169796751432016632241168863427728774579423150 074509
d_3	64383380457150019108049430636514587981992776123653960756109147769453967 41942919519896774972258058684244896078 9
e_3	10791439663276929341688056330575584359249977446556106381926655694171510 72774675772925380665526646130933249468945476316797228932406897172091521 37162219347743943103894170169796751432016632241168863427728774579423150 074509
d_4	64383380457150019108049430636514587981992776123653960756109147769453967 41942919519896774972258058684244896078 9
e_4	10791439663276929341688056330575584359249977446556106381926655694171510 72774675772925380665526646130933249468945476316797228932406897172091521 37162219347743943103894170169796751432016632241168863427728774579423150 074509
d_5	64383380457150019108049430636514587981992776123653960756109147769453967 41942919519896774972258058684244896078 9
e_5	10791439663276929341688056330575584359249977446556106381926655694171510 72774675772925380665526646130933249468945476316797228932406897172091521 37162219347743943103894170169796751432016632241168863427728774579423150 074509
d_6	64383380457150019108049430636514587981992776123653960756109147769453967 41942919519896774972258058684244896078 9
e_6	10791439663276929341688056330575584359249977446556106381926655694171510 72774675772925380665526646130933249468945476316797228932406897172091521 37162219347743943103894170169796751432016632241168863427728774579423150 074509
d_7	64383380457150019108049430636514587981992776123653960756109147769453967 41942919519896774972258058684244896078 9
e_7	10791439663276929341688056330575584359249977446556106381926655694171510 72774675772925380665526646130933249468945476316797228932406897172091521 37162219347743943103894170169796751432016632241168863427728774579423150 074509
d_8	64383380457150019108049430636514587981992776123653960756109147769453967 41942919519896774972258058684244896078 9
e_8	10791439663276929341688056330575584359249977446556106381926655694171510 72774675772925380665526646130933249468945476316797228932406897172091521 37162219347743943103894170169796751432016632241168863427728774579423150 074509
d_9	64383380457150019108049430636514587981992776123653960756109147769453967 41942919519896774972258058684244896078 9
e_9	10791439663276929341688056330575584359249977446556106381926655694171510 72774675772925380665526646130933249468945476316797228932406897172091521 37162219347743943103894170169796751432016632241168863427728774579423150 074509

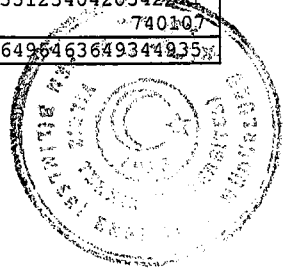


d_{10}	643833804571500191080494306365145879819927761236539607561091477694539674194291951989677497225805868424489607 89
e_{10}	107914396632769293416880563305755843592499774465561063819266556941715107277467577292538066552664613093324946894547631679722893240689717209152137162219347743943103894170169796751432016632241168863427728774579423150074509
d_{11}	643833804571500191080494306365145879819927761236539607561091477694539674194291951989677497225805868424489607 89
e_{11}	107914396632769293416880563305755843592499774465561063819266556941715107277467577292538066552664613093324946894547631679722893240689717209152137162219347743943103894170169796751432016632241168863427728774579423150074509

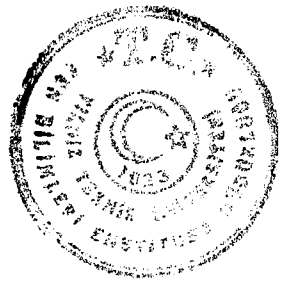


Ek-F-5
Sistem sayıları ile Seviye Anahtarları

Sembol	Değer
p	20747222467734852078216952221076085874809964747211172927529925899121966 847505496583100844167325500 77
q	49949091806585030192119760356408111278062369027342098434296869059406461 210859121722930446100600517086529446652716636885 1
n	10363049197725317508669387683496701839236198913033989136856985863094448 68089174229195716248366153402959491569020359019704074688304997565650402 53565289851373218837356747929481574452420959789063509745266015257210961 0451527
$\phi(n)$	10363049197725317508669387683496701839236198913033989136856985863094448 68089174229195716248366153402460000650954508717780802362494142967661957 15015736992080173868649869356541440031439038123294434173213654802116571 1532600
d_1	64383380457150019108049430636514587981992776123653960756109147769453967 41942919519896774972258058684244896720 7
e_1	94360457894483896529645854512386659091573128534970214734722081318797883 04351859777504080214546548886200968341309048717932818730692318678305640 12816572918066581656298281693146471828998312555296285892970296746509749 624543
d_2	55440670797542976964606028181912113728565321248694151701430172278848725 95524538090195925094162744941860173913957776296649322193920999234263413 64884037352876474751157786012467779642611623978749671687016334733428119 853513
e_2	28649290753278112503831193464718416003079054633171147097673990224000451 12685313918074831626310070781189393158820549800566145491418186973093688 13426798741751228315831242014300066293729254954912964222534123117390669 264977
d_3	79114816850849143938759564019427236518725824457215777702379550210176546 85347892060166339668841735969384749837245404265611399420643395247034536 50230775494114016449510791407249238981732094946544385970601926763537636 884177
e_3	41265534830545142923966006293818941261551708840263396595551230472649158 76903863507607952211406426726057680413481826030982285948052366020708318 15449200203654409062805290683084585789111779630060683889948673028990642 00113
d_4	87636820013236571598467012546070654368668750618542072724221974122590233 95933182714946077822186793131574234022689982679384202866494956937800483 87588411640719056319593818575935478991246064902084665052820793100328877 485611
e_4	96400010670889890139150315098050515249423544676884723489375579665312495 91071569288033000238031815164354898068424423535397620791604008245782948 28718208731058463157373143485257630632151597561231478375272982539112378 164491
d_5	19500214917849091395728951834411911841884875999849817884750908113265748 56163017908599979813143073053964085077179813668617730503596650702041976 69473884405211747392978507863302051585556537190458110415319443805770589 154117
e_5	60077427353093259457111983966063667402415348559631264539355257336740607 52825695960192222826342827301960988062672441530234145725655873864851027 33616673869264310706578099935562747862884864229644604311438885546677 94 823453
d_6	18126507633869286598236562912200028748936750536121632595751651589349056 58580376115395953226075513251333461512722576162955499411418491264073882 82114114894319748785010642064428710423841788470873171763831835656082310 090103
e_6	10090768456892984378938935822029383498248962682799538248528341389666382 44506200598586751905404601214006721336397694060924781196711705120202869 28017941085264279847498258263638507801138632843751825432870996051961009 8479367
d_7	94437501761165490255142263825288284552726101338088077227053558117091492 91504301995144013685969033691003184730855637572373471507802764192242714 19403348681342177476065169253906140134989525759848087946754230846870437 883643
e_7	52575401018420150458534196433939603981044120968798706243565828171384569 77725834911819995902311810541918829282005516146631283057595266795301913 26389251105883318821043946878279890135615947481418892265512340420542271 740107
d_8	67239935519310684211297179161725414420460264977197859396495463649344935

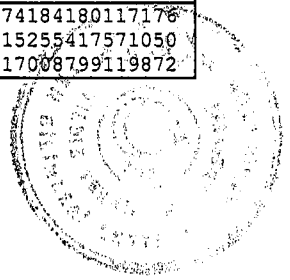


	28968297269109542400781250934023523437899784094655180355478581077561910 96976713305299802006137803603258999211027030246377542291224737611141448 550593
e_8	82818835072953956275050818221388209217749250872353146662628472931012809 54841565134231081014800536114986562529119002326792142282433017809208924 15131864220131169591447249876185623086146445374357568097949693344035820 497857
d_9	37223616395592516412615360134387567721088177836658533476362692425503757 52861424060500283528427160408136932162676557758774374877303477415370174 31514207125585901143313469261097428677154600058098488786839666300031593 624081
e_9	77172056999908892424311607614509229888997839483902230896558786846732373 06910265404605905758632217406575882492611846335913105757956370724636638 64620216404125041609814556950118248168836187583127905841270821037923532 801521
d_{10}	47106196600628565526144563568557846449406390643878089838716082907283508 13689223847881240584770016071368200593603180299657598270099010507186474 99708397393707389535580665383375822419520370632827104820212666906403028 718209
e_{10}	95986021481119529720759074307936237822969897415146157131367008420508329 59140801877846099244630671905959096279774864898751679263649532412317610 95181280928243512752563310265995895363807155584668108867817927893184616 307689
d_{11}	60090739576418467088971194035070898284097669977874162039285492386076052 44031323368922956182160978237205538082188871939106067950855592165516541 23354805472601486357600996479826445666645264797168588661495447692432806 05961
e_{11}	69137418492021036930654197984278635703536762173669817743012578649797378 28909795898239280329552069674542080584379786023874930303701873948697905 33016890853664172551622245875966692113054178932222075388300938911527130 09841



Ek-F-6
Sistem sayıları ile Seviye Anahtarları

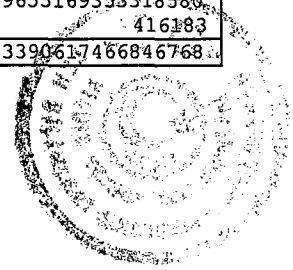
Sembol	Değer
p	20747222467734852078216952221076085874809964747211172927529925899121966 847505496583100844167325500 77
q	49949091806585030192119760356408111278062369027342098434296869059406461 210859121722930446100600517086529446652716636885 1
n	10363049197725317508669387683496701839236198913033989136856985863094448 68089174229195716248366153402959491569020359019704074688304997565650402 53565289851373218837356747929481574452420959789063509745266015257210961 0451527
$\phi(n)$	10363049197725317508669387683496701839236198913033989136856985863094448 68089174229195716248366153402460000650954508717780802362494142967661957 15015736992080173686498693565414400314390381232944341732136548021165 71 1532600
d_1	64383380457150019108049430636514587981992776123653960756109147769453967 41942919519896774972258058684244896078 9
e_1	10791439663276929341688056330575584359249977446556106381926655694171510 72774675772925380665526646130933249468945476316797228932406897172091521 37162219347743943103894170169796751432016632241168863427728774579423150 074509
d_2	82601519059704382801557686800807649586013116342782676493216033368856340 79262001573801907223450929259540276176964 13
e_2	49030990043103916939608009516581088499737956870796492273827027459639293 12276205475988734630205638084697997170731513223384723332078008609101925 52157670529062149654874616975414389841617035629318865991828257402446647 649677
d_3	23823592454214467360668988978040404301143914645500305885797805349482914 35642232124922230266033133571548877176526339489989537170148209470264814 18513623491613135750063101382197380097301922440996495789230499280219275 708353
e_3	69809370874455803698514646955334123719329501411737592161326790378051653 64049119121903603485978356136563972450534226745907326306801958198354889 78189830600686358500535080515214412677446418313860237172858754049905931 307817
d_4	28034235318902920524773640213512461716392495304429859731976259716115436 10178348099665749593333776118213451778212753235143342593807429642542454 21929961226688427756509249411260540087568048770429918263988845835095414 885127
e_4	56668578532848860435830010543866821645142361009682362843207782049173840 15638761284130587166072417307974789343627316530923074415274760913523744 60729384321401300192918067890447187629862998051547512998052157975792948 418063
d_5	45312223178559551227313632905143444325003760068801127708858242932648140 09457621817772352606152758247341519534121221043152075997409143619665127 40860745757722576744018494444068123898216884603346141000130903936867730 375031
e_5	52861537484863041197342971606871111552518295726281436833652077222683151 66218805733000006851846988308503070982095246238150031527294197484933442 89508894005468712797604660957971671312431930256311972900373925252259794 12871
d_6	64390231654709521785702761345095732649148804269237445529166348846151804 97214560946016960110545094449979247819028766780033783730875277593535743 59100868163497443224380371344785549010828084946994292098419404422514260 045139
e_6	32773143256141384030754670339200778876463037373494687106182999212083496 84486610873192894052866870566550002852902544790806651814176073860665180 88842249112517803411701258669157186099425989712818714174087209595596271 032459
d_7	11145342489955219608093897148440474071573805485712144153307658138753098 11908884939664810103693648311495416765154420446400768415809625309268588 04222420072800747240501679013842260885369838025945855369820290759216001 018449
e_7	99403459198099827619592153772775911211213253450195197704837487046562157 05436033237651852151528594747973985598187415043450308300828879987304081 81111616831915619391280345863189416573536448469287767565877374981642791 655249
d_8	90229472498392226926144291750341738013471663529347584083074184180117176 23970386259739353346708501419364295187688625190714583770815255417571050 61543951014685075046382304275804666760609059807768202528017008799119872



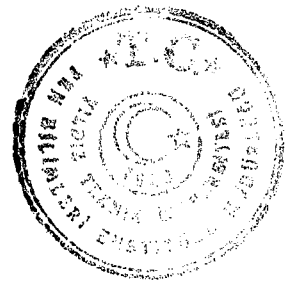
	001039
e_8	46555535130541512975393966939605028984314410237105476260660394826637413 71360624881489784659100373268268476688702302110420819736968415539879793 88314262302275280191671617290921566277940264706485448792062031244772165 036559
d_9	36172078752910755945454934896674985627180910507728454115708492865099761 32125807717214865500566411480645129366838703411742290717862298475025747 67942516812490955687315180708010191283711486871357802901776213769505958 544693
e_9	19714303812651496662594050716167871131814333111588307824980047103328410 71900552386423456711599597119779792205126215196248382123418996746902853 67495952530087609126296420719920181724315349136093070127690561076314091 453357
d_{10}	83154508306423529025243587297709872386203435836805926781767678962399153 33356003174111646422983639828584001948722642335329258681647506874089820 02773161012166563315891645801498173090876037941222077110578856223020058 126957
e_{10}	16138908240727089411085598868791524846659243775341373839325632626037031 33079911937364674552717063238704563971463857883244802455426974257240633 24353242623991457862185510579952633687074073473846292954674156872844305 335893
d_{11}	28811511729701906755005896278896650505336308090854749922568557660718551 86708685145974744954526335362934761595401202060694221129946500697015659 78637689910927875355642829192028298369101061940045583189604610504282513 743553
e_{11}	49665016442505550160836064541832137518756869424757586335088081140962115 47092601090211060802211906245048973212368642476596244685334207212693308 41774777870617310463530300124811803444762614680844748067768689856081498 793217

Ek-F-7
Sistem sayıları ile Seviye Anahtarları

Sembol	Değer
p	20747222467734852078216952221076085874809964747211172927529925899121966 847505496583100844167325500 77
q	49949091806585030192119760356408111278062369027342098434296869059406461 21085912172293044610060051708652944665271663688 51
n	10363049197725317508669387683496701839236198913033989136856985863094448 68089174229195716248366153402959491569020359019704074688304997565650402 53565289851373218837356747929481574452420959789063509745266015257210961 0451527
$\phi(n)$	10363049197725317508669387683496701839236198913033989136856985863094448 68089174229195716248366153402460000650954508717780802362494142967661957 15015736992080173868649869356541440031439038123294434173213654802116571 1532600
d_1	64383380457150019108049430636514587981992776123653960756109147769453967 41942919519896774972258058684244898244 3
e_1	42857254451185370257632882310929118618561277106482357723145394635402848 42623101683272619604923686266951752180967363976036897433358862648930956 64136382207375228850533273482366992577069636663372905062309677888080500 309707
d_2	55440670797542976964606028181912113728565321248694151701430172278848725 95524538090195925094162744943063841733976622247520925934729981641812807 89470072083535873866683606249655756073136580555696684190820256251770895 942613
e_2	99484890983322826901310588260677488561026767458013041437497706778457444 35741663899836829389533228360327106247399607953229835670474109425208226 50455685173195714330098821930239587150903358600459785206122360404009197 877877
d_3	15121299241081425054258674841493115280236049071672713263520888806169548 18696838440188278851963633322471835579123143068866655115893984797387741 41692714613392057525145409577805459028441415354011987473856982798260270 854457
e_3	59321236587009468665244150669166969427804179479505488994343135043296454 41041661248762684641080553615422493386381577894172719668611824902659482 64231273914299595214628689951963114799965477447012737344158694804766312 074193
d_4	10895587143765281756771269064259517623443211678360349561930578495504593 60883060488768658893904741149488348364332803332777000694778075499649513 33124121210602206203365175842764562491653118672370225916541446321695402 362941
e_4	53438646689631129966965366303202791418926254120482636105395884142521932 04457177792098593732800785966194498098893754029216186578250131520152876 18036383727862242557374665412768418403330528117658970779994250423023476 835861
d_5	53285630527413529485620892054925781638949041602966731370160743285984336 97883530446786887701000485810425828242424988945843640708492677135283580 50714614910330698943078796927803204730416301609304952604537504158910034 471729
e_5	48791328331877115714476281295221694746266539149227986671926678190810908 53434468395036331574898645743100647248286580156309131026801897435632362 29967145852828262316081194580705188592073180166784303617209486193882983 16369
d_6	93636424574810435228161769132462169734551907282213955862662749943329616 25279036767114507825835340404076779735767877958398421887409647831470 26 48361714168591164811256777186075515124043407714522213947718610690939768 594753
e_6	97686896373063412572648530583464114354597112677590974042270398650778990 11687411963056264002912409798309379255516446546284727365613605234335900 76864992167763718984050165358094683059500584402516818344994964624199960 169817
d_7	87761389993685681727726423357791871750691830327760079116071562949432213 43545275254831102789643932901831496079454839852535249047343026671213088 13779404795892033343315927842816090743619169737583011347426448612351591 131447
e_7	75069920977308787510824740141144388797652495745471836252136387725837097 77146817072647227429640799457291692285232811011362377289933597261577278 87356775651421723652650069227810802204641915512304342599655169353318580 416183
d_8	43579920366009427405353572860308248828619232667925142413390617466846768

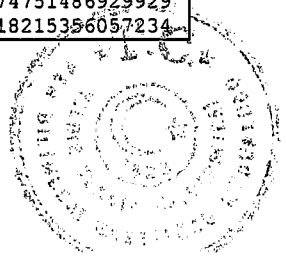


	455956234677833102334881937318751558055446349937606758203312154672477174444760427432845230373069817913277354910196235200820270061644542229070101760 1
e_8	351489586688040587355471191404552441380249610775951692019942255562399038807209528603882738033640326824185735840163871082612244373104811430317410536143586118763331702908194576381613127499221108250877948542503699327659001
d_9	942649597791653635121673310424063341556289471589173483051923716110916462262130100358883321732994938964522572791182825431598958421449157713041339035012166701655786766848671661363743128588611014525280013582125384789551949
e_9	236810443482630716236116778733696651257692390833047822953725088155124041599515132997445565728143653701982797274824570172700920658983627980925524687467632713933672549554077260045268587638366309479148092882890968088549549
d_{10}	253171150543017464889512605450657103313652987696412717780951443119898920110873890158702215695849458319090540705665889717863933345696639918535420204243854815639740484879045126925987242792075038985763399788361789102057897
e_{10}	294066157637450870724980745925660393257451136781399326756450253544881888536465275291024555048035382827448709701015809402211604023441320573032015446306221201190515803909509446016207984526408830349123621046362126762962833
d_{11}	841770644457972065443636549828222578430301896347976944241842339957241123460788740825735122496967858250454949409555688942324998851340390699481092430076596598907120987253182621260588977597547619490931019340542984918454163
e_{11}	775356934057810680849502945627926216604033514663340983137793395360459142078902318705519722359157443904449770513243127601586012915658717659820208601642779821744117097485662193429014456115975957222410048239041466932556027
d_{12}	358967042755016807225802734508612144780245786138227845676613743289376213745137161965799697914931388714405262814406247175771765187902555555235188732698937821780712633007228290359251479677752000230833377828501225642065447
e_{12}	267895328875279215218877635363110782611819901600690542068850623281393071679995271979142061453429135522340186628718562266311786595840780144059616752295106112122331172199928564502704384873328435117800353487327585146997383

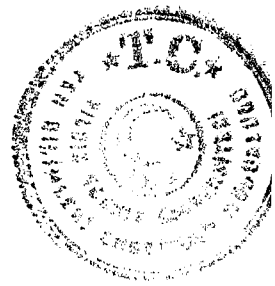


Ek-F-8
Sistem sayıları ile Seviye Anahtarları

Sembol	Değer
p	20747222467734852078216952221076085748099647472111729275299258991219668475054965831008441673255007 7
q	49949091806585030192119760356408111278062369027342098434296869059406461210859121722930446100600517086529446652716636885 1
n	10363049197725317508669387683496701839236198913033989136856985863094448680891742291957162483661534029594915690203590197040746883049975656504025356528985137321883735674792948157445242095978906350974526601525721096104515 27
$\phi(n)$	10363049197725317508669387683496701839236198913033989136856985863094448680891742291957162483661534024600006509545087177808023624941429676619571501573699208017386864986935654144003143903812329443417321365480211657115326 00
d_1	64383380457150019108049430636514587981992776123653960756109147769453967419429195198967749722580586842448969023
e_1	44760490252113602410797538993452359733747313786237734214991149615021339078653172738520275325083654934310579895687653465055499060244626768238927617932212547912489870410195672849583013760160570894079718392053432502329148 7
d_2	18862806999653903426869348917301987307475882006321601906637657791559313433893601439167916247765500300754771717684 21
e_2	32363290817664178715261667176511215654624078210591705385110877407313513291892806252186455374783589655200703596510772347689555523286433212841219736006969671000582575225927623578984652950173149191947897914934046952688698 1
d_3	48488341128758746078703356316554094910316085047194829989042904269263403193295865327081694939709341551247844162160482632527777747641498927430816810413277531024503230426283120728554219321369531238623324266583092430543019 7
e_3	90022983221912177252835746266241769415350205593903994805519052201827743150632938442532584564703792754740316228631407297166961458367734840663617358794347078044450149822412527335536453099942201785689940172026831816859473 3
d_4	43391519947708462979173899336989296544808102384932098422500269608362534055008539519851679500283443195984432157522459802952372079100228679849436813438668834435154424191068944661526759586889095681178635928903810232695443 1
e_4	81930658879649981704840728741896906261528133106288180538567295429405149730015835184565314938830760819647541852221032809059912840958601649620154588364447070756868305232081633166353947193480200819850309874405723149395867 1
d_5	97487787612015662252836538596960216538412565570125550059648621964604578401643111596698726212365773071890567782134899288876068576867618512343386738093791573320428149235194634693888107174085920319400188882648770563314148 3
e_5	73411934104553413130284819269518964312576776447356005714960174378303937620342683382568677199852467824632379402501823065891755435689668305613751865223124166155476580616006914948246246379517090730708587854485360414583334 7
d_6	21899480584159702210416806975024580430189656682986827991987273679092020897193820014387111019039487780028100791856375478781991667690538913455658159898724283423198043507768462917696952578560842626495889806010018734727075 1
e_6	33610909760690196668042299952878908863313315330763919979531293295205377371770060871771137651630580222340474470312143854019726815522146675576071538927195181361676738099781014788370719099540631063325699999519997903343375 1
d_7	50841440922257998617491483761633236312889788739724651896622285503604999289072186576038222846805588495136900723437590711073658727581318891338302954900506709897215908354452951599432358081921093183264230995473651295231518 9
e_7	32142311973519940824282191804260358471043987093617810494420562222841028265111474693670113954982489951454336267323139007368417717179253542367293789646203582319834997628075543174430506901430051381141980848844490991211510 9
d_8	93914098521958879672860541590543833540404761309443136900594866095927278741255839196252091843442352303167378648467696118858629393747514869299293685715902741284393781765224360425243807791996958106924521821535605723 4

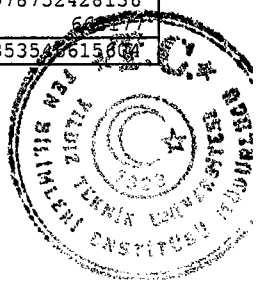


	298107
e_8	630495794915712311270437372081641951451037996449172559655213205343010641408021815877049806653618132909580687281275241899817356861711266860794622707527389800915750292950522132688349676177959928220953048574856256571813243
d_9	528958526539413344620680296446811700264985657115325653524575913043122956057314507818023795431105576390115754253748370027602752253132407876544293879340918971134632586389770897927956553761297673594542531240245322062812499
e_9	441704134531065442871641898502722898863077428480955474551120725556313434962811092250415671993087408569665906617024176158446943626450838507034461935438318848548711295394464615159476798891386386026878042039313665550770099
d_{10}	870642392691110432225673386900465759989005394982884465529819740187890268343123286743161068627438193885973326321266591913003704247389025681936799230396060646196436563533481157565398857658851573112804239892315620414306551
e_{10}	380670288417703709546199360474604661720936545517630028019971819636745996794059918875052561955074782702161873968810136093603873288641552827027870076188111339934466663014322720021254835209442870408176113839157577880188551
d_{11}	556547143421983789037790074050820592653881742163463099683188506535911913414897707896320521381084868092410861847347129210522613669369349680770832073845164312499165480946086281131717113261705021853520872523969197990 05317
e_{11}	131450278800214857532172438305302777499353404678998196531919841690578497302303461932244505076894661113106881256524264286769671726307594009141168376367725121563170124109425505151644024732008601871113487656675264113351053
d_{12}	535948110151282625265526062604554854451504341046885899026170364216150218150685326197962796933972978452812103782886445999179569539665376983271967021043507613080435544977865660488955936090648621708006668413888886859477711
e_{12}	465424122261847731434491197803846913827499044551985495076855892601468998111255313608245510130580733454948325465588083068220164238979691192146404547786203675593200578888626025877941967692877618130165898762766222220271791
d_{13}	201198143974365004320705274984136626333160578951799802412777571801901879949800681804375308940034787019909551393377168186618815041674667432843588795090160494873186386609909166535826935934835752816324054702349728455512 41
e_{13}	832052509287189459203510638320834102603654544566120372484945403233441383238912536778095275957319410157234000117141813051240309399217267127948333546850250230206589761064067851441619221931672877160988660184129423314565161
d_{14}	173279655303623882481688635458485991160944942076305992002903175866329806879296602623386237344033788750233313277027918144917501749587433700772827638427279489578941594125249632815856422305301193818358032464417122612508019
e_{14}	944428384879476938535147684940734722295070976701600839950652393467002411443273016056145065747111180237830145224586157949878204590516968155172796168066014573486690365803625011310950789132336100350808577340155403341571979



Ek-F-9
Sistem sayıları ile Seviye Anahtarları

Sembol	Değer
p	20747222467734852078216952221076085874809964747211172927529925899121966 847505496583100844167325500 77
q	49949091806585030192119760356408111278062369027342098434296869059406461 21085912172293044610060051708652944665271663688 51
n	10363049197725317508669387683496701839236198913033989136856985863094448 68089174229195716248366153402959491569020359019704074688304997565650402 53565289851373218837356747929481574452420959789063509745266015257210961 0451527
$\phi(n)$	10363049197725317508669387683496701839236198913033989136856985863094448 68089174229195716248366153402460000650954508717780802362494142967661957 15015736992080173868649869356541440031439038123294434173213654802116571 1532600
d_1	64383380457150019108049430636514587981992776123653960756109147769453967 4194291951989677497225805868424489902 73
e_1	44453148519370807403206249346681625636652886145387981943101663275755479 28473378271742269614053374311114395924856298354567836726659052084087273 58081732963911340425561047657595835635092801270964000680239637451860729 186937
d_2	55440670797542976964606028181912113728565321248694151701430172278848725 95524538090195925094162744944031266226324054423083716667060859307442769 83790305901842607729393871179906610666457593488091580452564222025923629 449803
e_2	72145822189806605442838071757482054454236667321676657822361018135799821 43303672264865661362551919967724652779990891388295359374036673541861954 54328884000069079722481125832938353174143711840933882757733079318295076 585667
d_3	83778688457661393739692137440940272360483757294582187429148182084615572 78256888762312323714596468986252733995237048749957258754332326718565709 63039613842564243959586728600033289317979118906704622829660768024826514 613277
e_3	85033435032376578098436204029636127334897308250003693451748084835064821 74462875516975123367636706901680596092833703790096057899046711149915953 72676799221294100830278503170312161925066678148418316659484791688660232 558213
d_4	76701768302530818873266421539332401264176272308954044234309487818381524 82708907475038768669312077177699554083503122776288637353297520379098833 84739224443718611288347915345902528837237127393436459417442201859089644 007723
e_4	58076993262581531741067632365439721186394683780141645641421161651509635 73181816208550190420894022064778387094779616130806819030253579699688320 08979277799735029512800808838911575357318681913998435519738719960445194 584987
d_5	76684101784944192129187548566047453702467812966384110264392742382785123 57924237068169391151595966773395648704449439710409451251591593395914195 44357878445296928279565419683525722211649767637065955486997970000002191 344469
e_5	43218118002821700155619788430125861629904426290210532519175644085205446 04499246636953889983181657095641947889827530711528205438656513690288427 69287329207517018296292585699049251555110740199300857112578916521752661 124229
d_6	36476305204042685249627436852514196781481639111742749196522132321590175 02887568141336080185712411680169890852287663899380228286998874824646690 93676357374318600179684718877425274661939006321769401105181540981292673 486387
e_6	90722853844980815983910371241609945719841462865966358926106819354868185 44454199378383499611902778350688836119867170795427893010260736256794508 06911974865101682088665393715237552169833150481686206365451583717271355 720923
d_7	35107143221377196265736136552904339239377435824718687119449198442699332 22726903540561800168923854056263556239124210946236014136847395886728385 22811161767337766132907264396651799116381065143461189480283472522514455 846913
e_7	28955467624024908238526936334988468459678660879491621928926999105646029 01319326868059029515040403286450860699064930306742645023807133755987986 86526971091875987265070638880346052697969871160606272140088978752428136 66[illegible]
d_8	79964709609594586178219446158053066411052903503501906937597353546615[illegible]

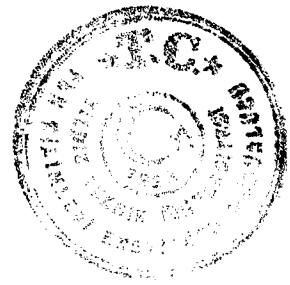


	204739551975402316415061560847829541342711510303583253618174875028198161366656919320356471838692109880659660691441932615464499506202626505780306766 1
e_8	381382123206632165391193160926504959070128197006873187461913017558965790230989220177839826015216611699077882504275356468280316720125070700787124608723276961912884629895380610925347771858190245021970851574223159746330941
d_9	678943872506827758586854822491129648166042807003719561299755301218700329463637920336457881874219972622701975923626098868112852955370622654716260371341115249907781579206648040492547801343973423048208263085144680239070421
e_9	718343592042717757232800783616817585586817484847112299264131856801452861395145004245667911532605244977829571317972175189901278053320931114012895980006300220417715018136335872328186863361026535591179811664705280660283781
d_{10}	938309887471900857656852058962995907470105369689849205098141477571720374393162075003167235815433764166033631620765863514703182382880691484247451031261178427496851113127710948631018541862111093611620361809996320246456093
e_{10}	337431683471683015359948277011141658174728455012869165833839602668562638156295093841849310446362148306140172684570822101260311745286198134803393621448819337880280535186909710239668674293962585825412388379252248537047957
d_{11}	103397573548320225271750220986504255323068759737601427997615822264405821012299182833969760966049862617137105670250397651057422139821600625801000525293384079451480340961975031622496040060971018791792833983301749310726887
e_{11}	919631103282525884304551882624920128436267870556886318501426424021027277220662350392273942924764199414790656620142156346268533584907872082406646747356486552916836674026333610563208159599740501175678509309404149299787223
d_{12}	449799353985984725976127015910182357875110033370875335251574740157340978558538732777308966265431566841123328500186021795076496337607603721868358002345517711885825640957608385684068537848269828947143788125209585717570249
e_{12}	495870899557108799586094622594368445259991973804525490575732557889553004696097500696153597189795768537560850654653291994708354974342544638837434886130758290068656167533594166259643526960509684459861434467260683240991049
d_{13}	302875497422072328122173258620967879568527019725195671083658424205182524690020798415582715935756656325815728997560857409095814439207392745533782642210854126237959368706042836817385695040473560029773530749850284651463273
e_{13}	100598869017538645349307956645732774548757971676804003582994388742205153874359701536391728900825046892984350363815229434213304672302346122389139176950964429836698732244678295880209328454622203597040218461615864813 6410737
d_{14}	603830162498212857325443681255705203173199110651383658101901788505644229005172998272079320568151363421327607614061219681130931123626458613801881301215989469188662386410787477038501909245367701655169455492038701543 3871
e_{14}	113825679211818067418992398979267924817251754617786240500243408514449444307746789486849224802276321181562019346295689466317810648521747573813477434840141731668114154481518917530354707243391147591826156246059036960125031
d_{15}	603506946415365936560963392671376773595240208002902083434720423362669544701887978451811756741389497726665275168851902500708754486974660993763514505747779725616487413154818081816585548882094838087615441496960716227166177
e_{15}	318224222456659216305418658590143224743712490324140871133821816680449808806043241190564348911878072649286067773045740135587688820066550971494304657923294888176485063710825633216793817074791281916605123938331340185 61913

Ek-F-10
Sistem sayıları ile Seviye Anahtarları

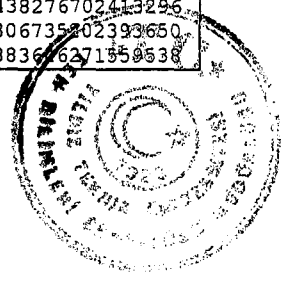
Sembol	Değer
p	4994909180658503019211976035640811127806236902734209843429686905940646121085912172293044610060051708652944665271663688517991415083182120225986209137374173851157962904073290919488354522121518442644531155217703627128153004567880738702606371720064149874
q	5452212151844264453115521770362712815300456788073870260637172006414987479914150831821202259862091373741738511579629040732909194883
n	2723330453214476861058807216890612454671703175572623500080112948218106868902465129047599975847851159476915811434707668778223776100827098333693035798157110631621389427086109595189617023713765704358700931422632243260864861288913067531529481981019789433
$\phi(n)$	2723330453214476861058807216890612454671703175572623500080112948218106868902465129047599975847851159476915811434707668772771563948483342962511663725873200212756851526231615644279024032955809533850485487492838766169469026541169385086605974720944225700
d_1	1043710774729182694003605009026135589878237925742436359877135850539062658142193219525570441747404589718566596776545627737751791
e_1	5553556073410097309405668577073976115425055206633636121009910701665023252229309842602957352545375247718761806098364537682145811408356394573943627141100186195648567067874805779596978442320896852161578270130856742151001771380962536340766377160266558319
d_2	2018359978328937283011410602796550507930139451849105757896774434339445502200782749302621821563900160835135598020050423329955732430
e_2	1352001437002260644492923775601434417215184187362720977528316817987128518940520599874496737735029184339514978777831428064951747562914841038663447778132613355256957111582959007330770479219183985173784029499971944206748186938138606885948463448173774489
d_3	1911006466936903085536635660264536676768947076293064750437259258421569027163309955100477752357195858485229962194299779030721569251077127529742965576940643735836477660489339466972142231681220487078630697889854421712435496232553562870444537680681326419
e_3	1123332973971646197357231179956938781526784218053406244187726360708583956377438956666375624039320400330560254423702016498248770240146278484812824259863723743744165064618937842880245233669957831979379652790349493155890805310341495957159020057939836879
d_4	2579646649375185938184695355877461362514080144662751230088042993243187846149533481502518524375061784253980591743132734447884806479523797170713023707371488768997941437021834309277146481488824961401738954201929237726467869996040165191235018588083898591
e_4	2412301707839877409986185024118171061876176051603510971537368581982289128608889610577067906680294433210150412201740974732699390918261563637886125260833399626671729416282070375433320497386415036901072529072236914649596784333245848834506066650226285939
d_5	1640423679005255170782870871910308867527984473466863647695647521083592878786631913321865906416697410650265091548901047767881750214420953805736762303882713370705117984127033014931439562648248729723019319212782862634768596453144792784691499223315882197
e_5	2300021675530744427164777413851991556875063025411022350143381476021355112513666206664737678899064833052090908437880455653826217022145674539613350147625150044117430195880898458820794709088330697475966317077310798795764365853083587730105518758708201233
d_6	1610203938520478235011752296789265850104030014483594317926610994994437068681858647822310678511632983792244242032738745376828021450110729731609590236264882585362222178012665400148194279431118131917272397699866142925969877390856429627965586094273949
e_6	7392550695348590959638260533609013032841311026934617586654705419446692168787231006147668767942798454099620061112713022348508862004398394199169124017289118963329481724216290823493866228344927366303955161061105083112821548163069973498170622635337465994
d_7	2439190097392874308844095735722639150547139481386042415511341476618446199012061010595543601332852046379165653551404482783318610270352444752008121085319997682278558680835407368959250515544064243155925383091317882915839695961474174449545088721242984467
e_7	2361890773587583234715159615881080314150427587755627495475602434135194349952896570209776118660664267949485502488777267380286680916707600590530059152575202608698985593018739998196448980834200122918707111785018926432604961685412675163559727915520686303
d_8	1675928978630025275949785351076249379140011972604128439589204937072865027642082474225365155171099713803695590750087395491640253619666607030136833457816444320150621466557076037186999251058364181153434493694732428 11

	523012412209467454825097356701690543 7
e_8	173022675258280056075680249526459290628528869755445350943678269708404275745364918459784158074388363112947039067490758201292600636603322771173525962151120868961872520775583583859428820902084749482317888478494962535259621511208689618725207755835838594288209020847494823178884784949625324548100547967960990597014223633804737
d_9	265046169750391258200072820024084335607927605197786894003560169248978685263441134256713316193544042101358215177421316703474505585949404597016489561031909656099529750580309318781101234303489214094517729190779127365843588565114353817795340354167399882937
e_9	192048259021850281684608171766333749417622275723480807900294883550566934015501604412492521646299690088269949508241043800399571190891488542030601750955941701626195210970716016304599571081693592703674814471409102787702379866756864342133575601531212656937
d_{10}	109057146803837817075459837462537232688470662618994334904551049653424545592932026828317795614782674835035156204317715064481262771744671009109917749603210621650174072132231695057739124828622789912542710975375424307889881629893454019354917848512884870137
e_{10}	222626587473308572019250259155832454221264681782709532530104892918765415194471896020496077529229052601813980382836155602623834212436580447056441661461739908657129337584882322335526562581493810629350527919610505671043355285249790124447343768426512660137

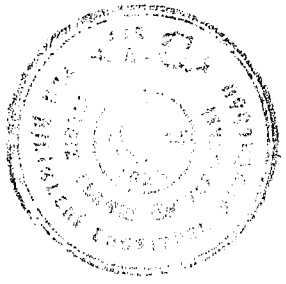


Ek-F-11
Sistem sayıları ile Seviye Anahtarları

Sembol	Değer
p	4994909180658503019211976035640811127806236902734209843429686905940646121085912172293044610060051708652944665271663688511
q	5452212151844264453115521770362712815300456788073870260637172006414987479914150831821202259862091373741738511579629040732909194883
n	2723330453214476861058807216890612454671703175572623500080112948218106868902465129047599975847851159476915811434707668778223776100827098333693035798157110631621389427086109595189617023713765704358700931422632243260864861288913067531529481981019789433
$\phi(n)$	2723330453214476861058807216890612454671703175572623500080112948218106868902465129047599975847851159476915811434707668772771563948483342962511663725873200212756851526231615644279024032955809533850485487492838766169469026541169385086605974720944225700
d_1	2087421549458365388007210018052271179756475851484872719754271701078125316284386439051140883494809179437133193553091255474347591624712533807240909452125310739367900664161586116797774075987135195800545408621318834995998155461917040087307622673615519645037807029739047239399847731310077668293294706087100056904761178670953414478610424042653505487744778613100766829329470608710005690476117867095341447861042404265350548722760121403300847809650198688880394007599523785303058643327171666547919124932577248690447571534032473630393989975222807329936497121095471807682804270009696166498991778400599552378530305864332717166654791912493257724869044757153176245644791792716165086143432128782189444734100323823242586974286692182575028154263262629217493328160707807028672608733180574173420291313123963168664448041556024636850619864607723565771560000258422194879174506038577333942477967366680378778448578481763124708619482230468354536897833086764126201453001237115608730825816395606984292814355982304242563840120696672617673068589231739317323621926961352703687645507396774627897661560053267250469970453101193833038064166379708422630048077010389854536921281721313208078964178726812186437024240554933282237864983800650228864397206404815434150417267804104517096355321323332438285325151688664267147192979345211862730854263029482892551658256776921354713839336197959577004289517871103151422055834314945552281485279747712287808602654895072035797517227430445021769286331565417198261893904864225514877616683668834399674243680929120167256811914939678358437229477792301487431009649536345679070202865862718752682358138624682141600593133159951665284728158446098050937403941703563322248049326319016696296266119826322687595343969720137438146756045871413983539071933927104862061448648924666004071473337574183310448981753874348925810004761824969658864486222506613122703841278950039640276141067435794314722851126124038989240286667296686662417308257547077331799223144078504218607690562816994101613863511025851226915981175823024593515747759259354960788943602547418347147793597647299646703750830816749020182486243078132586573304015130225313384774773797735965623716098710876986776721775942583669177701772807588497316970527518194251857188787959794245152246508660541602474750072459076489604219974270186787923285573790676622872023194267460375624208178774566200928197724402252957485615533714007566004333376857542424396784016996701766281136172068287869675059930501562434226315719213297251409947743194720820830742078158586178704297468307664729998319196308656940797508689990933628171309558440682779111833884682692200023577054552916907962894668640034404715338301172699109867723751754565855791416813286305487415140580718519323812401415203519379756401627630138033422278210299242091210178169208243027119843400623419882856319647071628344692237729770632838328147754509821593259643256500296463894313896356040438133962892155581321525562880515492415859631205015084907342089909544463491477383728707105286543675646271679496258926289246248772813687029609715416594797940463910067617936590040568269334163034025774980997913441240239989431046305248509975081165310838771059918172908486841640781762030523460346586100345870652050363099601971046261746331633353982859285926988944275345066965799795472104316780027805416888770919593770480658034441401630532781171289136248733344654738769629979431046305248509975081165310838771059918172908486841640781762030523460346586100345870652050363099601971046261746331633353982859285926988944275345066965799795472104316780027805416888770919593770480658034441401630532781171289136248733344654738769629979431046305248509975081165310838771059918172908486841640781762030523460346586100345870652050363099601971046261746331633353982859285926988944275345066965799795472104316780027805416888770919593770480658034441401630532781171289136248733344654738769629979431046305248509975081165310838771059918172908486841640781762030523460346586100345870652050363099601971046261746331633353982859285926988944275345066965799795472104316780027805416888770919593770480658034441401630532781171289136248733344654738769629979	1201984987455909597811868090318559229477451854388463554943827670241329692976604788835213499088732956530113076582626434046348303306735802393650587597293648119192630392191831406294268394179810522343338836627155953

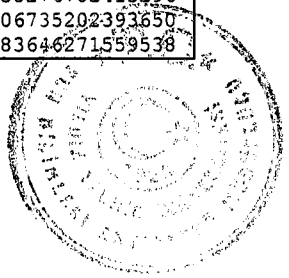


	797797581660293099653090911952517311 3
e_8	391730972903875969018625798749171324355713488344503359667856653771117830074765676769489931370309590703003398989952003066581833920177898210440870880966092410852298421461067518514513178242652800804781198646761185121225664148146826449922020152002074977
d_9	162344695014570543704857417669970027210193108938359146038182992500661739443952267879468001113552659585979085619301293287347215502974159254791365715510420773930594840459091465389577928967130921274376548794953322018285510020101572160283537582422670064 9
e_9	802712358602022041492504490095813353167777975410518080678546315339427215419466093307410146689880440385759413670836175373731638997188757479338342686592873095488477261335643772044386451670717341913705799656762854230126282204863103197383366760273263249
d_{10}	372424968419278044163735127201073431474248545082499323488538803685037866503448036908203638844861384571809367522579391556346393514531003326689599807974890226613449990830615211267241822684118241045117280819032929148825734290898002501055348531912539691
e_{10}	263324715317849497515644087989595299470656634309334660660168039633645540356497122925658786273253675675600622429698863161644260624202539223585732799582882583275735109661613145166079173238989313601145629741131389626182336487272539828420611273347515231 1
d_{11}	251420876600260893717810090926117411641395286474117859902268719620082824510103993403403313034096500474178349936527840443978797026892091129741817064494770181551937224690610198841730406115110577238634800292799605714523349803089382252587718921407043799 1
e_{11}	228749315067450461072734190780273635407266152770779138294702752568527678130023209633837690010714971810726328010439329270301906595004192881176557310829481856908024937776145357261539098218066263804262651116256807187259368708660912023212115164546125921 1

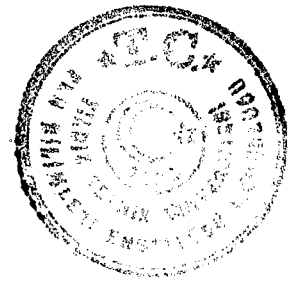


Ek-F-12
Sistem sayıları ile Seviye Anahtarları

Sembol	Değer
p	4994909180658503019211976035640811127806236902734209843429686905940646121085912172293044610060051708652944665271663688511
q	5452212151844264453115521770362712815300456788073870260637172006414987479914150831821202259862091373741738511579629040732909194883
n	2723330453214476861058807216890612454671703175572623500080112948218106868902465129047599975847851159476915811434707668778223776100827098333693035798157110631621389427086109595189617023713765704358700931422632243260864861288913067531529481981019789433
$\phi(n)$	2723330453214476861058807216890612454671703175572623500080112948218106868902465129047599975847851159476915811434707668772771563948483342962511663725873200212756851526231615644279024032955809533850485487492838766169469026541169385086605974720944225700
d_1	2087421549458365388007210018052271179756475851484872719754271701078125316284386439051140883494809179437133193553091255474345759
e_1	2471253380724090945212531073936790066416158611679777407598713519580054540862131883499599815546191704008730762267361551964503780702973904723939984773131007766829329470608710005690476117867095341447861042404265350548722276012140330084780965019868888039
d_2	3247363039398997522280732993649712109547180768280427000969616649899177840059955237853030586433271716665479191249325772486904475715 3
e_2	1762456447917927161650861434321287821894447341003238232425869742866921825750281542632626292174933281607078070286726087331805741734202913131239631686644480415560246368506198646077235657715600002584221948791745060385773339424779673666803787784485784817
d_3	1230819482230468354536897833086764126201453001237115608730825816395606984292814355982304242563840120696672617673068589231739317323621926961352703687645507396774627897661560053267250469970453101193833038064166379708422630048077010389854536921281721313
e_3	2080789641787268121864370242405549332822378649838006502288643972064048154341504172678041045170963553213233324382853251516886642671471929793452118627308542630294828925516582567769213547138393361979595770042895178711031514220558343149455522814852797477
d_4	6728086026548950720357975172274304450217692863315654171982618939048642255148776166836688343996742436809291201672568119149396783584372294777923014874310096495363456790702028658627187526823581386246821416005931331599516652847281584460980509374039417 03
e_4	5633222480493263190166962962661198263226875953439697201374381467560458714139835390719339271048620614486489246660040714733375741833104489817538743489258100047618249696588644862225066131227038412789500396402761410674357943147228511261240389892402866676 67
d_5	2966866624173082575470773317992231440785042186076905628169941016138635110258512269159811758230245935157477592593549607889436025474183471477935976472996467037508308167490201824862430781325865733040151302253133847747737977359656237160987108769867767216 21
e_5	7759425836691777017728075884973169705275181942518571887879597942451522465086605416024747500724590764896042199742701867879232855737906766228720231942674603756242081787745662009281977244022529574856155337140075660043333768575424243967840169967017662816 81
d_6	7759425836691777017728075884973169705275181942518571887879597942451522465086605416024747500724590764896042199742701867879232855737906766228720231942674603756242081787745662009281977244022529574856155337140075660043333768575424243967840169967017662816 81
e_6	2080174176896884594270175074584285824256433524644313509888309118564228791941681286305487415140580718519323812401415203519379756401627630138033422278210299242091210178169208243027119843400623419882856319647071628344692237729770632838328147754509821593
d_7	2596432565002964638943138963560404381339628921555813215255628805154924158596312050150849073420899095444634914773837287071052865436756462716794962589262892462487728136870296097154165947979404639100676179365900405682693341630340257749809979134412402399
e_7	8943104630524850997508116531083877105991817290848684164078176203052346034658610034587065205036309960197104626174633163335398285928592698894427534506696579979547210431678002780541688870919593770480658034441401630532781171289136248733344654738769629 9
d_8	1201984987455909597811868090318559229477451854388463554943827670241329692976604788835213499088732956530113076582626434046348303306735202393650587597293648119192630392191831406294268394179810522343338836462715595 38

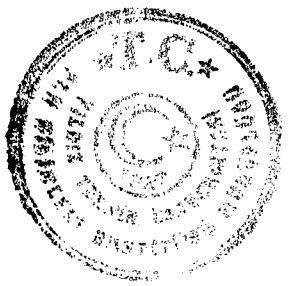


	797797581660293099653090911952517311 3
e_8	391730972903875969018625798749171324355713488344503359667856653771117830074765676769489931370309590703003398989952003066581833920177898210440870880966092410852298421461067518514513178242652800804781198646761851212256641481468264499220201520020749770
d_9	162344695014570543704857417669970027210193108938359146038182992500661739443952267879468001113552659585979085619301293287347215502974159254791365715510420773930594840459091465389577928967130921274376548794953322018285510020101572160283537582422670064 9
e_9	802712358602022041492504490095813353167777975410518080678546315339427215419466093307410146689880440385759413670836175373731638997188757479338342686592873095488477261335643772044386451670717341913705799656762854230126282204863103197383366760273263249
d_{10}	372424968419278044163735127201073431474248545082499323488538803685037866503448036908203638844861384571809367522579391556346393514531003326689599807974890226613449990830615211267241822684118241045117280819032929148825734290898002501055348531912539691
e_{10}	263324715317849497515644087989595299470656634309334660660168039633645540356497122925658786273253675675600622429698863161644260624202539223585732799582882583275735109661613145166079173238989313601145629741131389626182336487272539828420611273347515231 1
d_{11}	251420876600260893717810090926117411641395286474117859902268719620082824510103993403403313034096500474178349936527840443978797026892091129741817064494770181551937224690610198841730406115110577238634800292799605714523349803089382252587718921407043799 1
e_{11}	228749315067450461072734190780273635407266152770779138294702752568527678130023209633837690010714971810726328010439329270301906595004192881176557310829481856908024937776145357261539098218066263804262651116256807187259368708660912023212115164546125921 1



Ek-G
40 basamaklı n ile uygulama

Sembol	Değer
M	40206835204840513073
p	29497513910652490583
p	58995027821304981167
q	29497513910652490691
q	58995027821304981383
n	348041330763654876564811111728100613961
$\phi(n)$	348041330763654876553012106148549065141 2
d_1	117990055642609962551
e_1	121930487005373292872624941318523229436 7
d_2	235980111285219971757
e_2	773210091362229345159571702547734562 13
g_A	12764787846358441471
g_A^a	257955406254464603675318080856221800689 9
g_A^{-a}	640334615279740907447812468810353966804
$M * g_A^{-a}$	148896614084594564445740081579475339312 9
$(M * g_A^{-a})^{e1}$	136805020720192244414722878145079798913 4
$((M * g_A^{-a})^{e1})^{d1}$	148896614084594564445740081579475339312 9
$M * g_A^{-a} * g_A^a$	40206835204840513073
$(M * g_A^{-a})^{e2}$	115494349570908901813900055450843784583 8
$((M * g_A^{-a})^{e2})^{d2}$	148896614084594564445740081579475339312 9
$M * g_A^{-a} * g_A^a$	40206835204840513073
g_B	717554403153425368 73
g_B^a	222521721811334105969765968249766926682 7
g_B^{-a}	435692230280492623551870560036897969 51
$M * g_B^{-a}$	921739288450469261728073479111601688543
$(M * g_B^{-a})^{e1}$	137361662358658461390009340798063405649 9
$((M * g_B^{-a})^{e1})^{d1}$	921739288450469261728073479111601688543
$M * g_B^{-a} * g_B^a$	40206835204840513073
$(M * g_B^{-a})^{e2}$	237986657002221796917210945015669123675 2
$((M * g_B^{-a})^{e2})^{d2}$	921739288450469261728073479111601688543
$M * g_B^{-a} * g_B^a$	40206835204840513073



Ek-G
60 basamaklı n ile uygulama

Sembol	Değer
M	513821217024129243948411056803
p	590872612825179551336102197349
p	118174522565035910267220439469 9
q	564819669946735512444543557459
q	112963933989347102488908711491 9
n	133494589662593261977487397277570947086115561043280664741438 1
$\phi(n)$	133494589662593261977487397277339808629561178030524535590476 4
d_1	231079717554434674774154129501 5
e_1	111419169880183583342504703065787554518965898830507240063318 3
d_2	69624747704261828912966741927 01
e_2	664131177142405029439768681136991338036113907846598499332065
g_A	41606470020165830619632013793 1
g_A^a	100160984466889309705464782643226676918862366321427220055077 9
g_A^{-a}	888032742794715114383623311577438773652359401046522758851 87
$M *g_A^{-a}$	411681516668245614646615638865771056197956551682737453758965
$(M *g_A^{-a})^{e1}$	639039990553877153063788230308017929739512854196788157293725
$((M *g_A^{-a})^{e1})^{d1}$	411681516668245614646615638865771056197956551682737453758965
$M *g_A^{-a} * g_A^a$	513821217024129243948411056803
$(M *g_A^{-a})^{e2}$	952978971102774771393114027972422565656708899013439652762230
$((M *g_A^{-a})^{e2})^{d2}$	411681516668245614646615638865771056197956551682737453758965
$M *g_A^{-a} * g_A^a$	513821217024129243948411056803
g_B	280829369862134719390036617067
g_B^a	111433691938883301896098971964285776032362974845842337427 4297
g_B^{-a}	448749861195104149631310621059867005409108914668977738536080
$M *g_B^{-a}$	267456357122398859454484636672140116679600875392498632011345
$(M *g_B^{-a})^{e1}$	761289635771825851371055246563653500584747614914772175519975
$((M *g_B^{-a})^{e1})^{d1}$	267456357122398859454484636672140116679600875392498632011345
$M *g_B^{-a} * g_B^a$	513821217024129243948411056803
$(M *g_B^{-a})^{e2}$	117875348233738485570515251913178388987187061435165013037 35
$((M *g_B^{-a})^{e2})^{d2}$	267456357122398859454484636672140116679600875392498632011345
$M *g_B^{-a} * g_B^a$	513821217024129243948411056803

Ek-G
80 basamaklı n ile uygulama

Sembol	Değer
M	607538052934545886014457739870476161 4649
p	242596762305237077275763315697698247 4883
p	485193524610474154551526631395396494 9767
q	145173047051377849223662959899216603 8001
q	290346094102755698447325919798433207 6003
n	140874044754600441765457168701157228244543807912660981749645956434762 48721141301
$\phi(n)$	140874044754600441765457168701157228244466253950789658764346071179643 10424115532
d_1	750663825569343501891593518349206424 5747
e_1	117492547089493759077934531940870403880609757027249696638646395531944 26474943655
d_2	902234447770343622781548143956912302 2805
e_2	125071582728041134455962286150525901013525193062982040629085436408166 22415099201
g_A	361541588158511790855024350530978552623 1
g_A^a	204996984020213612674149050060108426671630936833986017858952601178983 4708515538
g_A^{-a}	933661757828202497571692434048440403074015262086448787354317167489372 8452870359
$M * g_A^{-a}$	804169045903924178180471874015411218304884743598209650035676167029482 6411845212
$(M * g_A^{-a})^{e1}$	811838746527601592648429064980291028753649974003390708777385374600813 3856097361
$((M * g_A^{-a})^{e1})^{d1}$	804169045903924178180471874015411218304884743598209650035676167029482 6411845212
$M * g_A^{-a} * g_A^{a}$	607538052934545886014457739870476161 4649
$(M * g_A^{-a})^{e2}$	112226348066224563572465827877644947912969777526562473549074904092771 90362237224
$((M * g_A^{-a})^{e2})^{d2}$	804169045903924178180471874015411218304884743598209650035676167029482 6411845212
$M * g_A^{-a} * g_A^{a}$	607538052934545886014457739870476161 4649
g_B	599283023552414275838685063377325868 1119
g_B^a	751663368180454737685853253963156501305856348415482398541421339868327 7270044313
g_B^{-a}	157240708015056310633184341379261874566127503052164487062704120816767 2825250285
$M * g_B^{-a}$	770263638359394204459996035988272370070227470750433801938266956923741 5994839594
$(M * g_B^{-a})^{e1}$	106952559999333932586656949747517779735914485362014451704370132604852 6404206773
$((M * g_B^{-a})^{e1})^{d1}$	770263638359394204459996035988272370070227470750433801938266956923741 5994839594
$M * g_B^{-a} * g_B^{a}$	607538052934545886014457739870476161 4649
$(M * g_B^{-a})^{e2}$	724827830954879572394179127963859081354750441124651728834530218471977 9860648452
$((M * g_B^{-a})^{e2})^{d2}$	770263638359394204459996035988272370070227470750433801938266956923741 5994839594
$M * g_B^{-a} * g_B^{a}$	607538052934545886014457739870476161 4649

Ek-G
100 basamaklı n ile uygulama

Sembol	Değer
M	2992740239799128648962783773417918638518829638222 7
p	2295368686771969123000270782186855260112447233006 9
p	4590737373543938246000541564373710520224894466013 9
q	3076254225030127069205146053958616692729173276755 9
q	6152508450060254138410292107917233385458346553511 9
n	2824455048273649742990732799740923357594737963820658137593682606059926 8 8821848165326408701922392154 1
$\phi(n)$	2824455048273649742990732799740923357594737963820550705135446564136082 7 7988175874382503018681372628 4
d_1	1062912046836171622659881934085592894060002225471 11
e_1	3627090704012215855051431058021615820566313694059809878785491407194073 4 8366421545316208131169247103
d_2	3365028149138794679626481871324234053111397187601 57
e_2	2522735738373082838769229152664284123556633975218242344113770470368089 3 1606640838433527753782934074 5
g_A	4648472980354018310183016787562378879453344121677 9
g_A^a	2276976945245333194083885323413335691394248044480775514539038566779064 8 8318072536286826584173093691 2
g_A^{-a}	1709624344969482189324609610908046203553907826356117356161653815983914 3 2029140488953222770289409126 6
$M * g_A^{-a}$	9411968456298836793301512197950401033287625157825794621938797030893724 9 8829210085266277969822560 8 5
$(M * g_A^{-a})^{e1}$	1655368429197224275478416738574266662149520812085312105568313488921813 7 3166454207877180837102592232 7
$((M * g_A^{-a})^{e1})^{d1}$	9411968456298836793301512197950401033287625157825794621938797030893724 9 8829210085266277969822560 8 5
$M * g_A^{-a} * g_A^a$	2992740239799128648962783773417918638518829638222 7
$(M * g_A^{-a})^{e2}$	1770390879091367677513771189283471182055197459144737484530739703131182 3 6145494136667481215283835655 9
$((M * g_A^{-a})^{e2})^{d2}$	9411968456298836793301512197950401033287625157825794621938797030893724 9 8829210085266277969822560 8 5
$M * g_A^{-a} * g_A^a$	2992740239799128648962783773417918638518829638222 7
g_B	9564780647927552813573378126620390479441956306440 7
g_B^a	2159623176804323653960000362830032180243486774929539604873914002925332 0 5038412530405913293256362819 1
g_B^{-a}	2644196887000710885398535452018475099749424030461762290149093073766106 4 5863062086497345008092495826 7
$M * g_B^{-a}$	2831641714352836465191195850372990487709901682074591481075659349607738 8 1190118405510002542744111210
$(M * g_B^{-a})^{e1}$	5462488242657222411358894569362605329957962782388017352728047153876780 0 4445483125080188953720099455
$((M * g_B^{-a})^{e1})^{d1}$	2831641714352836465191195850372990487709901682074591481075659349607738 8 1190118405510002542744111210
$M * g_B^{-a} * g_B^a$	2992740239799128648962783773417918638518829638222 7
$(M * g_B^{-a})^{e2}$	2190633611687130647239095870850033474312164741570868358403643398717698 5 3079171804273305107071630227 7
$((M * g_B^{-a})^{e2})^{d2}$	2831641714352836465191195850372990487709901682074591481075659349607738 8 1190118405510002542744111210
$M * g_B^{-a} * g_B^a$	2992740239799128648962783773417918638518829638222 7

Ek-G
120 basamaklı n ile uygulama

Sembol	Değer
M	313539589974026666385010319707341761012894704055733952484113
p'	668486051696691190102895306426999370394054817506916629005341
p	133697210339338238020579061285399874078810963501383325801068 3
q'	668486051696691190102895306426999370394054817506916629008239
q	133697210339338238020579061285399874078810963501383325801647 9
n	178749440525212514544851259394651225903634064291329784971820684167562275265916124323216762662395965293314030295397204515 7
$\phi(n)$	178749440525212514544851259394651225903634064291329784971820416773141596589440083165094191862647807671387027528745601799 6
d_1	267394420678676476041158122570799748157621927002766651602716 3
e_1	159545931593313756248948357298889737031842690151945738285104293681816840503389237617288249507700847596964572220075295533 1
d_2	534788841357352952082316245141599496315243854005533306564794 1
e_2	652515854743821061438124818924627043070465035709201889667210937221665887639808560949387466020357109471628502221065555449
g_A	4702877858580764415667235078667510929270158248348819067635 07
g_A^a	121149239418353834512256995635506266353823584331991018105420389634564259150120132267968490809727645928365158032113666700 4
g_A^{-a}	116587274671427405206372056598720159051258818851197102118436286438111196553995163164148478513541526741517154530331522532 7
$M * g_A^{-a}$	121175252854998406955489340999892006342683921458199320091572038407849562217916322640524621665512444680268645245185937258 7
$(M * g_A^{-a})^{e1}$	155890092569704219715614029876705261057347455293207706143197978245489759543543856907540723974814605550316481612481701080 3
$((M * g_A^{-a})^{e1})^{d1}$	121175252854998406955489340999892006342683921458199320091572038407849562217916322640524621665512444680268645245185937258 7
$M * g_A^{-a} * g_A^a$	313539589974026666385010319707341761012894704055733952484113
$(M * g_A^{-a})^{e2}$	840015536828272266357083512158969256845417284197705963210842964588159478218780304426963231598798296113075431470958451385
$((M * g_A^{-a})^{e2})^{d2}$	121175252854998406955489340999892006342683921458199320091572038407849562217916322640524621665512444680268645245185937258 7
$M * g_A^{-a} * g_A^a$	313539589974026666385010319707341761012894704055733952484113
g_B	378348910233465647859184421334615532543749747185321634086219
g_B^a	778351002832542866252082431512935943603385867711156176385396034738448781111089257974288475525159124204912843242711740519
g_B^{-a}	685903465097846626508837993976509755110939358626353518829109008504706494316984237487587069283166398678188650378762654 46
$M * g_B^{-a}$	896228431316219576006991172049307797537044670289499088664338258611140945833243806157063206004755621679147175963557450006
$(M * g_B^{-a})^{e1}$	558965803873354579219185536714909790755106496867918913335375131671406319464687120724597065625733752784355432275537015052
$((M * g_B^{-a})^{e1})^{d1}$	896228431316219576006991172049307797537044670289499088664338258611140945833243806157063206004755621679147175963557450006
$M * g_B^{-a} * g_B^a$	313539589974026666385010319707341761012894704055733952484113
$(M * g_B^{-a})^{e2}$	400321861323930594307392696468285457550414766461832833825309685032853500799244211008558518556687480577350863599029117426
$((M * g_B^{-a})^{e2})^{d2}$	896228431316219576006991172049307797537044670289499088664338258611140945833243806157063206004755621679147175963557450006
$M * g_B^{-a} * g_B^a$	313539589974026666385010319707341761012894704055733952484113

Ek-H-1
P_1 .. P_{212} listesi

i	P_i
1	2
2	3
3	5
4	7
5	11
6	13
7	17
8	19
9	23
10	29
11	31
12	37
13	41
14	43
15	47
16	53
17	59
18	61
19	67
20	71
21	73
22	79
23	83
24	89
25	97
26	101
27	103
28	107
29	109
30	113
31	127
32	131
33	137
34	139
35	149
36	151
37	157
38	163
39	167
40	173
41	179
42	181
43	191
44	193
45	197
46	199
47	211
48	223
49	227
50	229
51	233
52	239
53	241
54	251
55	257
56	263
57	269
58	271
59	277
60	281

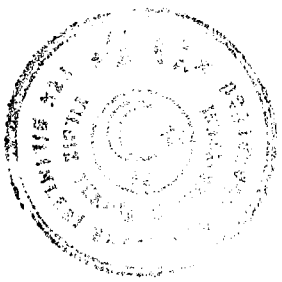
i	P_i
61	283
62	293
63	307
64	311
65	313
66	317
67	331
68	337
69	347
70	349
71	353
72	359
73	367
74	373
75	379
76	383
77	389
78	397
79	401
80	409
81	419
82	421
83	431
84	433
85	439
86	443
87	449
88	457
89	461
90	463
91	467
92	479
93	487
94	491
95	499
96	503
97	509
98	521
99	523
100	541
101	547
102	557
103	563
104	569
105	571
106	577
107	587
108	593
109	599
110	601
111	607
112	613
113	617
114	619
115	631
116	641
117	643
118	647
119	653
120	659

i	P_i
121	661
122	673
123	677
124	683
125	691
126	701
127	709
128	719
129	727
130	733
131	739
132	743
133	751
134	757
135	761
136	769
137	773
138	787
139	797
140	809
141	811
142	821
143	823
144	827
145	829
146	839
147	853
148	857
149	859
150	863
151	877
152	881
153	883
154	887
155	907
156	911
157	919
158	929
159	937
160	941
161	947
162	953
163	967
164	971
165	977
166	983
167	991
168	997
169	1009
170	1013
171	1019
172	1021
173	1031
174	1033
175	1039
176	1049
177	1051
178	1061
179	1063
180	1069

i	P_i
181	1087
182	1091
183	1093
184	1097
185	1103
186	1109
187	1117
188	1123
189	1129
190	1151
191	1153
192	1163
193	1171
194	1181
195	1187
196	1193
197	1201
198	1213
199	1217
200	1223
201	1229
202	1231
203	1237
204	1249
205	1259
206	1277
207	1279
208	1283
209	1289
210	1291
211	1297
212	1301

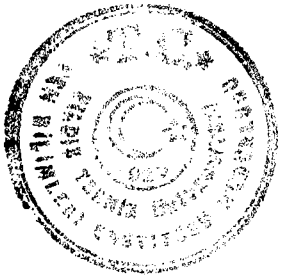
Ek-H-2
P_1 .. $P_{1,000,000}$ listesi

i	P_i	i	P_i
1	2	1,000	7,919
2	3	2,000	17,389
3	5	3,000	27,449
4	7	4,000	37,813
5	11	5,000	48,611
6	13	6,000	59,359
7	17	7,000	70,657
8	19	8,000	81,799
9	23	9,000	93,179
10	29	10,000	104,729
20	71	20,000	224,737
30	113	30,000	350,377
40	173	40,000	479,909
50	229	50,000	611,953
60	281	60,000	746,773
70	349	70,000	882,377
80	409	80,000	1,020,379
90	463	90,000	1,159,523
100	541	100,000	1,299,709
200	1,223	200,000	2,750,159
300	1,987	300,000	4,256,233
400	2,741	400,000	5,800,079
500	3,571	500,000	7,368,787
600	4,409	600,000	8,960,453
700	5,279	700,000	10,570,841
800	6,133	800,000	12,195,257
900	6,997	900,000	13,834,103
		1,000,000	15,485,863



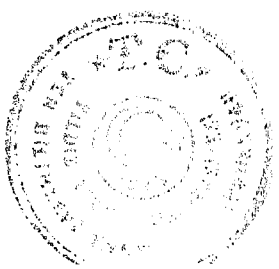
Ek-I
Üretilen p, q listesi

sno	*i*	P_i	$1+2*P_i$	*sno*	*i*	P_i	$1+2*P_i$
1	2	3	7	1,000	8,065	82,499	164,999
2	3	5	11	2,000	17,464	193,601	387,203
3	5	11	23	3,000	27,455	318,203	636,407
4	9	23	47	4,000	38,067	454,799	909,599
5	10	29	59	5,000	49,038	599,213	1,198,427
6	13	41	83	6,000	59,546	740,189	1,480,379
7	16	53	107	7,000	70,390	887,693	1,775,387
8	23	83	167	8,000	81,371	1,039,463	2,078,927
9	24	89	179	9,000	92,363	1,191,941	2,383,883
10	30	113	227	10,000	103,516	1,349,423	2,698,847
20	72	359	719	20,000	219,947	3,047,123	6,094,247
30	124	683	1,367	30,000	340,423	4,876,643	9,753,287
40	176	1,049	2,099	40,000	463,445	6,793,379	13,586,759
50	240	1,511	3,023	50,000	589,726	8,795,483	17,590,967
60	304	2,003	4,007	60,000	714,295	10,802,243	21,604,487
70	357	2,399	4,799	70,000	843,392	12,903,341	25,806,863
80	424	2,939	5,879	80,000	971,509	15,013,403	30,026,807
90	488	3,491	6,983				
				82,211	999,556	15,478,349	30,956,699
100	541	3,911	7,823	82,228	999,837	15,483,101	30,966,203
200	1,304	10,691	21,383	82,229	999,841	15,483,161	30,966,323
300	2,078	18,131	36,263	82,230	999,859	15,483,581	30,967,163
400	2,850	25,913	51,827	82,231	999,880	15,483,971	30,967,943
500	3,729	34,949	69,899	82,232	999,952	15,485,273	30,970,547
600	4,548	43,649	87,299	82,233	999,959	15,485,339	30,970,679
700	5,396	52,883	105,767	82,234	999,962	15,485,363	30,970,727
800	6,269	62,423	124,847	82,235	999,968	15,485,441	30,970,883
900	7,209	72,911	145,823	82,236	999,976	15,485,549	30,971,099

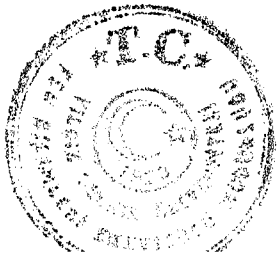


Ek-J
SÖZLÜK

Access	erişim
Access Level	erişim seviyesi
Associativity	birleşme özelliği
Commutativity	değişme özelliği
Distributivity	dağılma özelliği
Canonical Factoring	kanonik açılım
Complexity	karmaşıklık, zaman maliyeti
Computing Roots	kök alma
Computing Square Roots	karekök alma
Constant	sabit
Crypto	şifre
CryptoAnalysys	şifre kırma
Cryptography	şifre sistemi
Text, Message	açık mesaj
Cypher, CypherText, Cryptotext	şifrelenmiş mesaj
Encode, Encryption	şifreleme
Decode, Decryption	şifre çözme
Discrete Logarithm	ayrık logaritma
Empirical	sayısal
Euclid Algorithm	
Extended Euclid Algorithm(Eea)	
Factor, Divisor, Proper Divisor	bölen
Factoring, Factorization	çarpanlara ayırma
Prime Factor	asal çarpan
Feasible	verimli
Infeasible	verimsiz
Gcd	OBEB, ortak bölenlerin en büyüğü
Group	grup
Hierarchical	hiyerarşik
Key	anahtar
Legend	kısaltma
Linear Regression	doğru uydurma
Number Theory	sayı teorisi
One-way Function	tek yönlü fonksiyon
Trapdoor	açık kapılı
Trapdoor One-way Function	açık kapılı tek yönlü fonksiyon
Private	gizli
Public	açık
Polinomial	polinom
Linear	doğrusal
Non-polinomial, NP	polinom olmayan
Exponential	üstel
Prime	asal
Composite	asal olmayan
Random	rassal



Residue	kalan
Residue Set	kalanlar kümesi
Reduced Residue	indirgenmiş kalan
Reduced Residue Set	indirgenmiş kalanlar kümesi
Quadratic	karekök
Quadratic Residue	karekökü mevcut
Role-Based	grupsal, görev tabanlı
Sender	gönderici
Receiver	alıcı
Intruder, CryptoAnalyst	şifre kırıcı
Stable	durağan
Successive	ardışık
Tractable, Easy	kolay
Intractable, Hard	zor
Undecidible	çözümsüz
Turing Machine	Turing makinası



ÖZGEÇMİŞ

Doğum Tarihi	11 Mart 1962	
Doğum Yeri	İstanbul	
İlkokul	1968-1973	Büyük Esma Sultan İlkokulu, Beşiktaş-İstanbul
Ortaokul	1973-1976	Anafartalar Ortaokulu, Beşiktaş-İstanbul
Lise	1976-1980	Deniz Lisesi, Heybeliada-İstanbul
Lisans	1980-1984	Deniz Harp Okulu, Heybeliada-İstanbul
Yüksek Lisans	1988-1990	Naval Post Graduate School, Monterey-California Bilgisayar Bilimi'nde İleri İhtisas
Doktora	1991-1998	Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Bilimleri ve Mühendisliği Anabilim Dalı
İş	1984-1986	T.C.G. Saros Gemisi Seyir-Harekat Subayı
	1986-1988	T.C.G. Kuşadası Gemisi II. Komutanı
	1991-1993	Deniz Harp Okulu Yazılım Müh. Öğretim Görevlisi
	1993-1996	Deniz Harp Okulu Yazılım Müdürü Öğretim Görevlisi
	1996-Devam	Harp Oyunu Merkezi Yazılım Müdürü