

ATATÜRK ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
İŞLETME ANABİLİM DALI

Mehmet Sinan BAŞAR

144632

YER DEĞİŞTİRME ESASLI VE RASGELE ANAHTARLI YENİ
BİR ŞİFRELEME ALGORİTMASI

DOKTORA TEZİ

144632

Tez Yöneticisi
Yrd. Doç. Dr. Üstün ÖZEN

ERZURUM – 2004

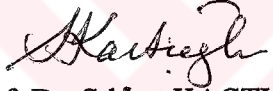
SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜNE

Bu çalışma, İşletme Anabilim Dalının Sayısal Yöntemler Bilim Dalında jürimiz tarafından Doktora tezi olarak kabul edilmiştir.



Yrd. Doç. Dr. Üstün ÖZEN

Danışman/Jüri Üyesi



Prof. Dr. Sıtkat KAÇTIOĞLU

Jüri Üyesi



Doç. Dr. M. Sinan TEMURLENK

Jüri Üyesi



Prof. Dr. H. Öner ESEN

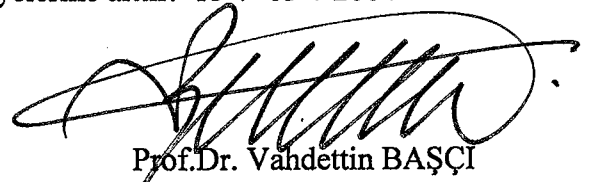
Jüri Üyesi



Prof. Dr. Hüseyin AYDIN

Jüri Üyesi

Yukarıdaki imzalar adı geçen öğretim üyelerine aittir. 15 / 03 / 2004



Prof. Dr. Vahdettin BAŞÇI

Enstitü Müdürü

İÇİNDEKİLER

	SAYFA NO
ÖZET	IV
ABSTRACT	V
TEŞEKKÜR	VI
ŞEKİLLER DİZİNİ	VII
TABLolar DİZİNİ	VIII
 GİRİŞ	 1
 BÖLÜM 1. ŞİFRELEME KAVRAMI VE ŞİFRELEME METOTLARI	 3
1.1. Şifrelemede Temel Kavramlar	3
1.1.1. Kriptoloji (Cryptology)	3
1.1.2. Kriptosistem (Cryptosystem)	3
1.1.3. Kriptografi (Cryptography)	4
1.2. Şifreleme Metotları	5
1.2.1. Şifrelemede Anahtar Kavramı	7
1.2.2. Kapalı Anahtarlı Şifreleme (Private-Key Cryptography)	8
1.2.2.1. Caesar Chiper	8
1.2.2.2. Affine Chiper	9
1.2.2.3. Random Chiper	10
1.2.2.4. Vigenere Chiper	11
1.2.2.5. Transposition Chiper	12
1.2.2.6. Enigma	12
1.2.2.7. DES (Data Encryption Standart)	14
1.2.2.8. AES (Advanced Encryption Standart)	18
1.2.3. Açık Anahtarlı Şifreleme (Public-Key Cryptography)	22
1.2.3.1. RSA (Rivest, Shamir, Adleman Cryptography)	22
1.2.3.2. RABIN	25
1.2.3.3. ELGAMAL	26

1.2.3.4. McELIECE.....	26
1.3. Kriptanaliz (Cryptanalysis)	27
1.3.1. Dilbilgisi Kuralları ve Kriptanaliz.....	27
1.3.2. Anahtar Tahmini ve Kriptanaliz.....	27
1.3.3. Matematiksel Fonksiyonlar ve Kriptanaliz	28
 BÖLÜM 2 ELEKTRONİK TİCARETTE GÜVENLİK VE ŞİFRELEME.....	29
2.1. Elektronik Ticaretin Tanımı	29
2.1.1. Elektronik Ticaretin Tanımı ve Kapsamı	29
2.1.2. Elektronik Ticaretin Araçları	32
2.1.3 Perakende Mal Alım Satımı ve E-Ticaret	32
2.1.4. Hizmet Sektörü ve E-Ticaret.....	34
2.1.5. E-Ticaretin Yararları	35
2.1.5.1. İşletmelere Sağladığı Yararlar.....	35
2.1.5.2. Müşterilere Sağladığı Yararlar	36
2.1.5.3. Toplumsal Yararlar.....	36
2.1.6. E-Ticaretin Dezavantajları	36
2.1.6.1. Teknik Dezavantajları	36
2.1.6.2. Teknik Olmayan Dezavantajları.....	37
2.2. Elektronik Ticarete Güvenlik	39
2.2.1. Bilgisayar Ağlarında Güvenlik.....	39
2.2.1.1 Güvenli Bilgisayar Sistem Değerlendirme Kriterleri (TCSEC).....	41
2.2.1.2. TCSEC Değerlendirme Sınıfları	41
2.2.1.4. Bilgi Teknolojisi Güvenliği Değerlendirme Kriterleri (ITSEC)	42
2.2.1.5. Veri İletişiminde Güvenlik.....	42
2.2.2. Elektronik Ticaret'te Ödeme Araçları.....	43
2.2.2.1. Kredi Kartları ve Akıllı Kartlar (Smart Card).....	44
2.2.2.2. Dijital (Sayısal) Çek ve Dijital Senet	44
2.2.2.3. Dijital Para.....	45
2.2.2.4. Diğer Ödeme Araçları	46
2.2.3. Elektronik Ödeme Sistemlerinde Güvenlik ve Şifreleme	46
2.2.3.1. Şifreleme Algoritmaları.....	49

2.2.3.2. Dijital (Sayısal) İmza	50
2.2.3.3. Anahtar Kontrolü (Key Management)	51
2.2.3.4. Dijital Sertifikalar.....	52
2.2.4. Şifreleme Esaslı Güvenlik Sistemleri.....	52
2.2.4.1. SSL (Secure Socket Layer)	52
2.2.4.2. SET (Secure Electronic Transaction)	55
 BÖLÜM 3 SIS ŞİFRELEME ALGORİTMASI	58
3.1. Tanım	58
3.2. SIS'in Özellikleri.....	59
3.3. Çalışma Sistemi.....	59
3.4. SIS Algoritmasında Matrislerin Kullanılması	63
3.5. Dairesel Hareketle Kaydırma	71
3.6. SIS'de Anahtar Kullanılarak Şifreleme.....	75
3.6.1. Tek Anahtarlı Modeller	75
3.6.2. Çok Anahtarlı Modeller	100
3.6.2.1. Çok Parçalı Anahtar	101
3.6.2.2. Rasgele Anahtar	101
3.6.2.3. Seçici Anahtar	103
3.7. SIS Kullanılarak Tasarlanmış Bir Elektronik Ödeme Sistemi	107
3.7.1. Sistemin İşleyişi	107
3.7.2. Sistemin Özellikleri.....	124
3.7.3. Kullanılan SIS algoritmasının güvenlik analizi	125
 SONUÇ	128
KAYNAKLAR.....	130
EKLER	135
ÖZGEÇMİŞ	145

ÖZET**DOKTORA TEZİ****YER DEĞİŞTİRME ESASLI VE RASGELE ANAHTARLI YENİ BİR
ŞİFRELEME ALGORİTMASI****Mehmet Sinan BAŞAR****Danışman: Yrd. Doç. Dr. Üstün ÖZEN****2004-SAYFA: 129****Jüri: Yrd. Doç. Dr. Üstün ÖZEN****Prof. Dr. Sibkat KAÇTIOĞLU****Doç. Dr. M. Sinan TEMURLENK****Prof. Dr. H. Öner ESEN****Prof. Dr. Hüseyin Aydın**

Çalışmanın amacı yeni bir şifreleme metodunun ortaya konması ve bu yeni metodun elektronik ticarete bir güvenlik aracı olarak kullanılması konusunun araştırılmasıdır. Bu bağlamda birinci bölümde şifreleme kavramı ve şifreleme metotları tanımlanmıştır. Bu bölümde konunun kapsamının genişliği nedeni ile tüm şifreleme metotlarına değinilmemiş, yalnızca temel algoritmalar ile standart olarak kabul edilmiş olan ve elektronik ticarete kullanılan algoritmalar tanıtılmıştır.

İkinci bölümde ise elektronik ticaret ve güvenlik sistemleri şifreleme metotlarının kullanılması çerçevesinde açıklanmıştır. Bu bölümde de elektronik ticaretin ana hatları ile kısaca tanımlanmış, ardından yalnızca güvenlik ve şifreleme ile ilgili ayrıntılara girilmiştir.

Çalışmanın üçüncü bölümünde şifrelemede SIS adını verdiğimiz yeni bir yaklaşımla oluşturulan yeni metotlar ve algoritmalar tanıtılarak mevcut metotlar ile karşılaştırılmış ve üstün veya zayıf yönleri araştırılarak bir güvenlik sistemi elemanı olarak kullanılıp kullanılamayacağı araştırılmıştır.

ABSTRACT**PhD. THESIS****A New Encryption Algorithm Based On Substitution and Random Key****Mehmet Sinan BAŞAR****Supervisor: Assist. Prof. Dr. Üstün ÖZEN****2004-PAGE: 129****Jury: Assist. Prof. Dr. Üstün ÖZEN****Prof. Dr. Sibkat KAÇTIOĞLU****Assoc. Prof. Dr. M. Sinan TEMURLenk****Prof. Dr. H. Öner ESEN****Prof. Dr. Hüseyin Aydın**

The aim of this study is to develop a new encryption algorithm and to research the usability of this new algorithm in electronic commerce as a security tool. In this context, the first chapter defines the concept of encryption and explores the methods of encryption. In the same chapter, due to the broad scope of the subject, not all encryption methods are touched on. Instead, some basic and standardized algorithms and the ones that are used in electronic commerce applications are looked over.

Second chapter describes electronic commerce and security systems with relation to use of encryption methods. This chapter also defines electronic commerce in general, and specifies security and encryption in depth.

Third chapter introduces a new method named SIS and algorithms we developed, compares existing methods with these newly developed algorithms, and inquiries if they could be used as a security component by scrutinizing their poor and powerful aspects.

TEŞEKKÜR

Bu çalışmada ilk günden beri her türlü yardımını esirgemeyen başta danışmanım sayın Üstün Özen olmak üzere tüm hocalarıma teşekkürü borç bilirim.

M. Sinan Başar



ŞEKİLLER DİZİNİ

	SAYFA NO
1.1. İlk Şifreleme Aleti	5
1.2. Simetrik Anahtar	7
1.3. Asimetrik Anahtar	8
1.4. Enigma'da Kullanılan Algoritma (1. Adım)	12
1.5. Enigma'da Kullanılan Algoritma (2. Adım)	13
1.6. Enigma'da Kullanılan Algoritma (3. Adım)	13
1.7. Enigma	14
1.8. Başlangıç Dizilimi (IP) ve Başlangıç Metni	15
1.9. E-tablosu.....	16
1.10. DES Birinci Aşama	16
1.11. DES Son Aşama	17
1.12. State Matris	20
1.13. ShiftRows.....	20
2.14. E-Marketin Çalışması.....	33
3.15. Vektörel Hareketle Kaydırma	71
3.16. Dairesel Hareketle Kaydırma	72
3.17. SIS Kullanılarak Tasarlanmış Bir Elektronik Ödeme Sistemi	108

TABLÖLAR DİZİNİ

	SAYFA NO
3.1. SIS ile şifreleme yapılırken kullanılacak karakterler (I)	60
3.2. SIS ile şifreleme yapılırken kullanılacak karakterler (II).....	61
3.3. SIS Algoritmasının Güvenlik Analizi	126



GİRİŞ

Geride bıraktığımız yirminci yüzyılın özellikle son çeyreğinde hız kazanan teknik gelişmeler gündelik hayatı da önemli ölçüde etkilemiş, gerek yeni davranış ve faaliyet şekilleriyle, gerekse eski davranış ve faaliyetler için yeni metot ve araçlarla insanların yaşamını neredeyse tamamen değiştirmiştir. Şüphesiz ki, gündelik hayatı en çok etkileyen teknolojik gelişmelerin başında bilgisayar ve iletişim teknolojilerindeki gelişmeler gelmektedir.

Teknolojik gelişmelerin yaşantımıza etkisini, kullandığımız dile kazandırdığı yeni kelimelerle anlamak mümkündür. İnternet'te sörf, e-mail, chat, VCD, DVD gibi on yıl önce neredeyse hiç kimsenin bilmediği kelimeler günümüzde çocukların bile anlayacağı şekilde dilimize yerleşmiştir. Bir başka önemli etki ise önceden de yapılan bazı işlerin farklı araçlarla ve farklı metotlarla yapılmaya başlanmasıdır. Bu etkinin en belirgin görülebileceği alanlara örnek olarak alışveriş ve bankacılık işlemleri gibi ticari faaliyetlerin internet üzerinden yapılması gösterilebilir.

Elektronik Ticaret veya E-Ticaret olarak adlandırılan yeni ticaret şekli de söz konusu gelişmelerin bir sonucu olarak ortaya çıkmış, gerek karlılık gerekse yaygınlık açısından gözlemlenen hızlı büyüme ile aynı zamanda teknolojik gelişmeyi motive edici bir nitelik kazanmıştır. Elektronik ortamda yapılan ticari faaliyetlerin artması bir taraftan veri iletişimini hızlandırıcı ve yaygınlaştırıcı yeni teknolojik gelişmelere ihtiyaç duyulmasına yol açmış, diğer taraftan da güvenlik ihtiyacını arttırarak güvenlik teknolojilerinin gelişmesini hızlandırmıştır.

Ağ ortamında çalışan bir bilgisayar ile yapılacak olan İnternet'te gezinme, kişi, belge veya bilgi arama, haber alma gibi sıradan işlemler için duyulan güvenlik ihtiyacı, istenmeyen erişimlerin engellenmesi ve virüs benzeri kötü niyetli yazılımlardan korunmak gibi temel güvenlik konuları ile sınırlı kalabilir. Ancak yapılan işlem para transferi gerektiren veya gizlilik konusunda hassasiyet isteyen bir işlem ise güvenlik çok daha fazla önem kazanacaktır. Bu durumda tarafların birbirlerini tanıması, üçüncü bir tarafın yönetiminde veya kefaleti altında güvenli bir iletişim kurulması, sipariş formu, gönderme talimatı, çek, senet, ödeme emri gibi ticari belgelerin güvenli olarak imzalanması, şifrelenmesi ve kasıtlı bozma, teknik hata sonucu silinme veya

değiştirilme gibi dış müdahalelerden korunarak karşı tarafa ulaştırılması için ek bazı tedbirlere ihtiyaç duyulacaktır.

Elektronik ticarete güvenlik için geliştirilen sistemler içerisinde şifreleme algoritmaları önemli bir işleve sahiptir. Bir yandan mesajlar şifrlenerek korunurken diğer yandan akıllı kartlar, sayısal imza, sayısal sertifika gibi güvenlik araçlarında da şifreleme algoritmaları kullanılmaktadır.

Bu çalışmada elektronik ticarete güvenlik için kullanılan birçok metottan biri olan şifreleme konusu incelenmiş ve güvenlik sistemleri içerisindeki konumu ve önemi vurgulanmaya çalışılmıştır. Ayrıca mevcut şifreleme metotlarından farklı olarak yeni bir yaklaşım ve bu yeni yaklaşımın sonucu olarak yeni bir metot ortaya konulmaya çalışılmış ve bu yeni metodun mevcut güvenlik sistemleri içerisinde kullanılabilme olasılığı araştırılmıştır.



BÖLÜM 1. ŞİFRELEME KAVRAMI VE ŞİFRELEME METOTLARI

1.1. Şifrelemede Temel Kavramlar

1.1.1. Kriptoloji (Cryptology)

Kriptoloji, bilginin yalnızca ulaşması istenen kişiler tarafından okunabilecek şekilde gizlenmesi bilimidir¹. Kriptoloji kriptografi ve kriptanaliz ile ilgili bilim alanıdır.² Bu bilim alanını yeterince tanımlayabilmek için bazı konuların açıklanması gerekmektedir. Bu amaçla sorulacak ilk soru bilgiyi gizleme ihtiyacının kaynağıdır. İnsanlar ellerindeki bir bilgiyi başka bir kişinin öğrenmesini neden istemez veya neden bu bilgiyi yalnızca belirli kişilerin öğrenmesini ister? Bunun birçok sebebi olabilir. Bir kişi veya kurum elindeki bilgiyi gizlemeye; ahlaki nedenlerle, ticari nedenlerle veya güvenlik nedeniyle ihtiyaç duyabilir. Bu ihtiyaç, kişinin bir arkadaşına ikisi arasındaki bir sır hakkında bir şey söylerken diğer kişilerin duymasını istememesi olayından, bir askeri operasyon hakkındaki bilgilerin ilgili olmayan veya karşı tarafta yer alan kişiler tarafından elde edilmesinin istenmemesine kadar geniş bir yelpazede kendisini gösterir.

Burada sözünü ettiğimiz bilginin kriptolojinin ilgi alanına girmesi için elbette başkalarının ulaşma şansının olması gerekir. Bu da bilginin iletilmesi gerekliliğini doğurur. En az iki kişi arasında yapılan bilgi iletişimi ve iletilen bilginin üçüncü kişi tarafından ulaşılsa bile anlaşılamayacak şekilde kodlanması ile bir kriptosistem oluşmaktadır.

1.1.2. Kriptosistem (Cryptosystem)

Bilgi iletişimi yapılan bir ortamda belirli kişilerin anlayacağı diğerlerinin anlayamayacağı bilgiler üreten bir sistemdir. Bir kriptosistem üç temel öğeden oluşur.

- Gerçek metin (plaintext)
- Şifre (chiper)
- Şifreli metin (chiphertext)

Bu bilgiler ışığında basit bir kriptosistem şu şekilde yazılabilir:

¹ <http://www.emmy.nmsu.edu/~crypto>, S.E.T. 26.02.2002.

² Mc. Daniel, George, *IBM dictionary of computing*, MCGraw Hill Inc., Ağustos 1993.

$$(\text{Gerçek Metin}) \Rightarrow F \Rightarrow (\text{Şifreli Metin}) \Rightarrow G \Rightarrow (\text{Gerçek Metin})^3$$

Burada F ve G metni şifreleyen ve şifreli metni çözen fonksiyonlardır. Bu iki fonksiyon kriptolojinin iki ayrı çalışma alanının kapsamına girer. Gerçek metnin şifreli metne dönüştürülmesi (F) kriptoloji, şifreli metnin çözülerek gerçek metne dönüştürülmesi de (G) kriptanaliz olarak adlandırılır.

Bir kriptosistemin yerine getirmesi gereken temel fonksiyonlar [ISO 87] ile standartlaştırılmıştır. Bu fonksiyonlar üç başlık altında toplanmıştır:⁴

1- Gizlilik (secrecy): Gizlilik ulaşması için izin veya yetki verilmemiş kişilerin bilgiye ulaşamamasını sağlar.

2- Güvenilirlik (authenticity): Mesajın kaynağının, yani mesajı gönderen kişinin tanınması anlamında kullanılır. Mesajı gönderen kişi belirsiz ise, tanınmıyorsa yada, yetkisiz bir kullanıcı ise mesaj cevaplandırılmaz ve içerdiği komutlar icra edilmez.

3- Doğruluk, Bütünlük (integrity): Mesajın, kaynağından hedefine ulaşmaya kadar kaza ile veya kötü niyetli bir eylemin sonucu olarak, bir kısmının silinmesi, değiştirilmesi veya bir kısım veriler eklenmesi gibi bozulmalara uğramadan bütünlüğünü ve doğruluğunu koruyup korumadığının denetlenmesidir.

1.1.3. Kriptografi (Cryptography)

Sadece belirli kişiler tarafından anlaşılabilir şekilde yazı yazmanın iki temel metodu “Stenografi” ve “Kriptografi”dir. Kriptografi Yunanca “kryptos” (gizli) ve “graphein” (yazmak) kelimelerinden türetilmiş bir kelimedir^{5,6}. Kriptolojinin gerçek metnin şifreli metne dönüştürülmesi için yapılan işlemler, oluşturulan sistemler, fonksiyonlar ve algoritmalar ile yani şifreleme (encryption) ile ilgilenen çalışma alanına kriptografi adı verilir. Kriptografi bir verinin anlamını gizlemek üzere dönüşüme tabi tutulmasıyla ilgilenen bilim dalıdır⁷. Anlamanın gizlenmesi, bilginin gizliliğinin ve güvenilirliğinin korunması amacını taşır ve istenmeyen kişilerin bilgiye ulaşmasını

³ <http://www.emmy.nmsu.edu/~crypto>

⁴ Nechvatal, James, “Public-Key Cryptography”, *NIST Special Publication 800-2*, Nisan 1991, s. 1.

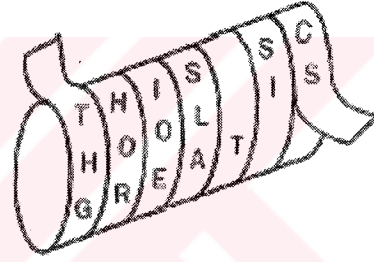
⁵ Petras, Richard T, “Cryptography”, *Mathematics Teacher*, Kasım 2001, Sayı 94/8, s. 689

⁶ Yeh, Wen-Hung, Jing-Jang Hwang, “Hiding Digital Information Using a Novel System Scheme”, *Computers & Security*, 2001, Cilt 20, Sayı 8, ss. 533-538.

⁷ Mc. Daniel, George. a.g.e.

engeller⁸. Kriptografinin ortaya çıkış tarihi tam olarak bilinmemektedir. Üçüncü bir kişiye gönderilen ilk gizli mesajın ne olduğu ve kim tarafından yazıldığı da bilinmeyenler arasındadır. 19. Yüzyılda çok alfabeli şifreleme (polyalphabetic schemes) kullanılmaya başlanmış ve birden fazla alfabe içerisinde hangisinin kullanıldığını belirleyen anahtar kavramı ortaya çıkmıştır.

İlk olarak ne zaman kullanıldığı bilinmese de şifrelemede kullanılan ilk alet basit bir sopadır. Bu sopaya belirli bir açıyla sarılan bez üzerine mesaj yazılır ve bez açıldığında mesaj okunamayacak şekilde karışmış olur. Harflerin arasındaki boşluklar rasgele karakterlerle doldurularak mesaj iyice gizlenebilir (Şekil 1.1). Mesajı alan kişi onu tekrar aynı kalınlıktaki çubuğa aynı açı ile sarar ve mesajı rahatlıkla okur.



Şekil 1.1. İlk Şifreleme Aleti⁹

Elektriğin kullanılmaya başlanmasından sonra elektrikli bir şifreleme makinesi yapma çabaları başlamıştır. En çok bilinen elektrikli şifreleme makinesi, İkinci Dünya Savaşı sırasında Almanların kullandığı “Enigma”dır. Enigma hakkında daha sonra ayrıntılı bilgi verilecektir. Bilgisayar teknolojisinin gelişmesi ve iletişimde kullanılmaya başlaması ile dijital ortamda şifreleme dönemi başlamış ve şifreleme makineleri, yerini programlara ve algoritmalara bırakmıştır.

1.2. Şifreleme Metotları

Şifreleme metotları algoritma veya program (scheme) olarak adlandırılır. Bütün algoritmalarda aşağıdaki üç temel metodun biri veya birkaçı kullanılmaktadır^{10, 11}:

⁸ Kennedy, Gabriella, “Codemakers, Codebreakers Rulemakers Dilemmas in Current Encryption Policies”, *Computer Law & Security Report*, 2000, Cilt 16, Sayı 4, ss. 240-247.

⁹ <http://www.techdirections.com>, S.E.T. 15.04.2002

¹⁰ Highland, Harold Joseph, “Data Encryption: A Non-Mathematical Approach”, *Computers & Security*, 1997, Sayı 16, ss. 369-386.

1- Yer Değiştirme İşlemleri (Substitution) : Gerçek metindeki karakterler farklı bir alfabedeki karakterlerle veya karakter numarası değiştirilerek aynı alfabedeki farklı karakterlerle değiştirilir.

2- Sıra Değiştirme İşlemleri (Transposition): Gerçek metindeki karakterlerin metin içerisindeki sıraları değiştirilir.

3- Cebirsel İşlemler: Gerçek metindeki karakterlere verilen numaralar (genellikle ASCII kodları) karmaşık cebirsel işlemlerle ve fonksiyonlarla dönüştürülür.

Şifreleme algoritmaları gruplandırılırken kullanılan bir kriter de algoritmanın sürekliliğidir. Şifrelenecek metnin tümünün bir defada işlendiği algoritmalara sürekli şifreleyici algoritma (stream chiper), metnin parçalara ayrılıp her parçanın ayrı ayrı işlendiği algoritmalara parçalı şifreleyici algoritma (block chiper) adı verilir¹².

Şifreleme metotları algoritmanın izlediği adımların önceki adımlarla veya herhangi bir bloğun şifreleme metodunun diğer blokların şifrelenmesi ile ilişkisine göre karmaşık (chaotic) veya mantıksal (logistic) olarak gruplandırılabilir¹³.

Şifreleme metotlarına ilişkin bir diğer ayırım da kullanılan sayı sistemleri için yapılabilir. Günümüzde standart olarak belirlenmiş algoritmaların çoğunda ikili sistem (0 ve 1) kullanılmaktadır. Bunların dışında kalanlar onlu, on altılı sistem kullanılan algoritmalar veya sayı sistemi kullanılmayan (Non-Mathematical) algoritmalar şeklinde sınıflandırılabilir¹⁴.

Şifreleme algoritmaları için özetleme temelli (hash based) algoritmalar¹⁵, yetkilendirilmiş (authenticated) şifreleme algoritmaları¹⁶, yay fonksiyonlu (elliptic curve) algoritmalar¹⁷ gibi daha bir çok sınıflandırma mevcuttur. Ancak şifreleme

¹¹ Read, R. C., "Graph Theory and the Amateur Cryptographer", *Computers Math. Application*, 1997, Cilt 34, Sayı 11, ss. 121-127.

¹² Golic, J.Dj., "Stream Chiper Encryption of Random Access Files", *Information Processing Letters*, 1999, Sayı 69, ss. 145-148.

¹³ Kocarev, Ljupco, Goce Jagirovski, "Logistic Map as a Block Encryption Algorithm", *Physics Letters A*, 2001, Sayı 289, ss. 199-206.

¹⁴ Jansen, Cees J. A., Piet van der Vlist, "Message Encryption With Minimal Expansion and Redundancy-Doing Better Than ISO-10126", *Computer & Security*, 1996, Cilt 10, Sayı 7, ss. 627-632.

¹⁵ Peyravian, Mohammad, Allen Roginsky, Nev Zunic, "Hash-Based Encryption System", *Computers & Security*, 1999, Cilt 18, Sayı 4, ss. 345-350.

¹⁶ Hwang, Shin-Jia, Chin-Chen Chang, Wei-Pang Yang, "Authenticated Encryption Schemes with Message Linkage", *Information Processing Letters*, 1996, Sayı 58, ss. 189-194.

¹⁷ Zheng, Yuliang, Hideki Imai, "How to Construct Efficient Signcryption Schemes on Elliptic Curves", *Information Processing Letters*, 1998, Sayı 68, ss. 227-233.

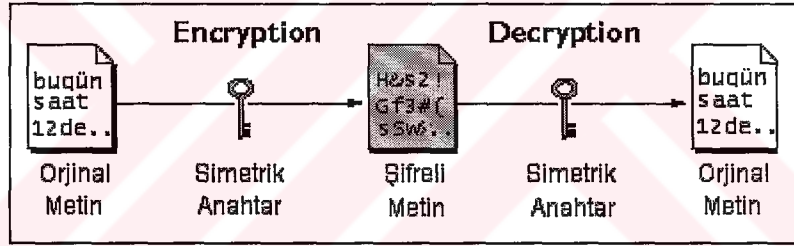
algoritmaları gruplandırılırken kullanılan metot yerine anahtar kullanımı ve anahtar şeklinin esas alınması daha yaygın kabul görmüş bir yaklaşımdır.

1.2.1. Şifrelemede Anahtar Kavramı

Anahtar şifrelemede önemli bir kavramdır. Bir metni şifrelerken kullanılan değiştirme veya dönüştürme metodu anahtar olarak adlandırılır. Örneğin ($a=w, \dots k=a, \dots p=z, \dots i=j, \dots$) basit bir anahtardır ve “kapı” kelimesi bu anahtarla şifrelenirse “awzj” sonucu elde edilir. Elbette şifrelemede kullanılan bütün anahtarlar bu kadar basit değildir. Özellikle modüler aritmetik kullanılan algoritmalarda çok karmaşık ve çözülmesi zor anahtarlar kullanılmaktadır.

Simetrik Anahtar – Asimetrik Anahtar

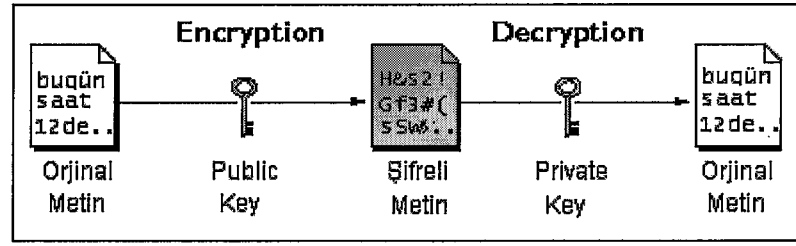
Simetrik anahtar çözücü anahtarın şifreleyici anahtarla aynı olması veya onun bir fonksiyonu olması, yani şifreleyici anahtar kullanılarak çözücü anahtarın hesaplanabilmesi durumunu ifade eder¹⁸.



Şekil 1.2. Simetrik Anahtar

Kapalı anahtarlı şifrelemede bu tür anahtarlar kullanılır. Şifrenin üçüncü şahıslar tarafından çözülmemesi için şifreleyici anahtarın bilinmemesi zorunluluğu kullanılan anahtarın simetrik oluşundan kaynaklanmaktadır. Açık anahtarlı şifrelemede ise simetrik anahtar kullanılmaz. Asimetrik anahtar olarak adlandırılan bu metotta çözücü anahtar şifreleyici anahtar kullanılarak hesaplanamadığından şifreleyici anahtarın üçüncü kişiler tarafından bilinip bilinmemesi çözücü anahtarın bulunması için bir fayda sağlamaz. Bu yüzden sadece çözücü anahtar gizli tutularak şifrenin çözülmesi engellenebilir.

¹⁸ <http://www.docs.sum.com>, S.E.T. 22.08.2002



Şekil 1.3. Asimetrik Anahtar

Kriptografi, şifrelemede kullanılan anahtarın simetrik olup olmaması açısından iki kısma ayrılır:

- Kapalı Anahtarla Şifreleme (Private-Key Cryptography)
- Açık Anahtarla Şifreleme (Public-Key Cryptography)

1.2.2. Kapalı Anahtarlı Şifreleme (Private-Key Cryptography)

Kapalı anahtarlı şifreleme simetrik anahtar kullanılarak yapılır. Simetrik anahtar kullanılan algoritmalar genellikle bir karakterin başka bir karakterle değiştirilmesi esasına (substitution) dayanır. Anlaşılması ve çözümü kolay bir şifrelemedir. Karakterlerin değiştirilmesi farklı metotlarla yapılabilir. Bu metotlardan bir tanesi alfabeyi kaydırmak suretiyle yapılan değiştirmedir (shift transformation). Bu metot “Caesar Chiper” olarak adlandırılmaktadır.¹⁹

1.2.2.1. Caesar Chiper

Bu şifreleme metodunda alfabedeki harflerin sıra numaraları belli bir miktar kaydırılarak değiştirilir. Bu şekilde alfabedeki bir harfin sıra numarası bu yeni alfabede başka bir harfe denk gelecektir. Şifrelenecek metindeki harfler yeni alfabede kendilerine karşılık gelen harfle değiştirilerek şifreli metin elde edilir. Örneğin alfabe üç harf sağa kaydırılsın:

A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z			
			A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z

¹⁹ <http://www.emmy.nmsu.edu/~crypto>

Artan üç harf en baştaki boşluklara yazılarak anahtar tamamlanır.

A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z
V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü

Artık gerçek metnin her harfi hemen altındaki harfle değiştirilerek şifreli metin elde edilebilir. Örneğin:

BU MESAJ GİZLİDİR

Yukarıdaki metin anahtar tabloya göre şifrenirse şu sonuç elde edilir:

YS JCÖVH DĞÜİĞBĞO

Kaydırma işlemi farklı büyüklüklerde yapılarak farklı anahtarlar elde etmek mümkündür. Yirmi dokuz harfli bir alfabede yirmi sekiz değişik kaydırma işlemi yapmak mümkündür. Örneğin yukarıda verilen metnin on bir harf kaydırılarak şifrenmesi durumunda şu sonuç elde edilecektir:

PK DTİÖB ÜAOÇAŞAH

Şifrelenen metni çözmek için ise anahtar tablo tersten kullanılmalıdır. Yani şifreli metindeki harf ikinci satırda aranır ve ilk satırda kendisine karşılık gelen harfle değiştirilir. Bu algorithmada harflerin kaç birim kaydırıldığını bilen bir kişi şifreli metni kolayca çözebilir. Bunun anlamı ise kaydırma miktarının Caesar Chiper için anahtar olduğudur²⁰.

1.2.2.2. Affine Chiper

Shift Transformation çözümü kolay ve bu nedenle fazla güvenli olmayan bir metottur. Ayrıca yirmi sekiz farklı kaydırma imkanı vardır. Bu da şifreleme yaparken çok sınırlı seçeneğe sahip olmak anlamına gelir. Kapalı anahtarla şifrelemede harfleri değiştirmek için kullanılabilecek bir başka metot, Affine Transformation olarak adlandırılan metottur. Bu metotta önce alfabedeki harflere sıfırdan başlayarak numara verilir. Daha sonra şifrelenecek metnin her bir karakterine karşılık gelen numaralar bir fonksiyon ile değiştirilir ve bu karakter elde edilen rakamın ait olduğu karakterle değiştirilir. Affin Chiper ile şifrelemede kullanılacak fonksiyon:

$$C = f(P) = (aP + b) \bmod N$$

²⁰ <http://www.emmy.nmsu.edu/~crypto>

P: Gerçek metinde her bir karaktere karşılık gelen rakam,

N: Alfabedeki karakter sayısı,

a, b: Anahtar tamsayılar.

Aşağıda verilen örnek metni bu fonksiyona göre şifreleyelim: Önce alfabedeki karakterler 0-29 arası numaralandırılır.

BU MESAJI SAKLA

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

İkinci adım anahtar tamsayıların belirlenmesidir.

a=3

b= 8 olsun.

İlk karakter “B” ye karşılık gelen rakam “1”dir. Öyle ise: P=1

Alfabedeki harf sayısı: N=26

$$C = f(1) = (3(1)+8) \bmod 26$$

C=11

Alfabede 11 rakamına karşılık gelen karakter “L” dir. Yani Gerçek metinde “B” yerine şifreli metinde “L” yazılacaktır. Diğer karakterler de aynı şekilde hesaplanarak şifreli metin bulunur.

LQ SUKIUG KIMPI

Affine Chiper ile şifrelenmiş bir metni çözmek için şifrelemede kullanılan fonksiyonun dönüştürülmesi gerekir. Bu durumda yeni fonksiyon:

$$P = f^{-1}(C) = (9(C)+6) \bmod 26$$

1.2.2.3. Random Chiper

Bu metot, alfabedeki harfleri rasgele olarak başka harflerle bire bir eşleyen bir fonksiyon yardımıyla karakterlerin değiştirilmesi suretiyle şifreleme şeklinde tanımlanabilir. Kullanılan fonksiyon matematiksel bir fonksiyon değildir. Bu metotla şifrelenmiş küçük bir metni çözmek Affine Chiper ile şifrelenmiş bir metni çözmekten

daha zordur. Ancak yeterince büyük bir metin olursa daha kolay çözülebilir. Aşağıdaki tablo harfleri rasgele eşleştiren örnek bir fonksiyon olarak düşünülebilir²¹.

A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z
İ	D	Ö	Ü	A	J	P	Z	E	K	F	B	R	G	V	L	S	Ğ	Ş	M	C	T	H	N	Ç	Y	O	U	I

Bu tabloya göre “GİZLİ MESAJ” metni şifrenirse:

“ZBIVB LJTİR” elde edilir

Bu şifreyi çözmek için yukarıdaki tablonun bilinmesi gerekir ancak elde uzun bir metin varsa harflerin kullanılma sıklığına göre bir takım yaklaşımlarla bazı harflerin karşılıkları tahmin edilerek çözüme ulaşılabilir.

1.2.2.4. Vigenere Chiper

16. yüzyıldan önce kullanıldığı bilinen bir şifreleme metodudur. Bu metot Caesar Chiper ile benzer şekilde çalışır ancak anahtar olarak kaydırma miktarı yerine bir kelime kullanılır. Bir kelimenin anahtar olabilmesi için o kelime bir harf iki kere tekrarlanmamış olmalıdır. Alfabe harflerinin karşılığı olarak “A” dan başlamak şartı ile önce anahtar kelime harf harf yazılır. Daha sonra diğer harfler sırayla yerleştirilir. Böylece anahtar tablo elde edildikten sonra şifrelenecek metindeki harfler bu tabloya göre değiştirilerek şifreli metin bulunur. Örnek olarak; şifrelenecek metin “BU MESAJ GİZLİDİR” ve anahtar kelime “BİLEVTAŞI” olsun. Bu durumda tabloya önce anahtar kelime yerleştirilir:

A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z
B	İ	L	E	V	T	A	Ş	I																				

Diğer harfler ise sıra ile yazılır:

A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z
B	İ	L	E	V	T	A	Ş	I	C	Ç	D	F	G	Ğ	H	J	K	M	N	O	Ö	P	R	S	U	Ü	Y	Z

Son olarak bu tabloya göre şifreli metin elde edilir:

İS HTOBF ŞDZĞDVDO

²¹ <http://www.emmy.nmsu.edu/~crypto>

Vigenere Chiper uzun süre geçerliliğini korumuş ve Enigma'ya da temel olmuş bir şifreleme metodudur.

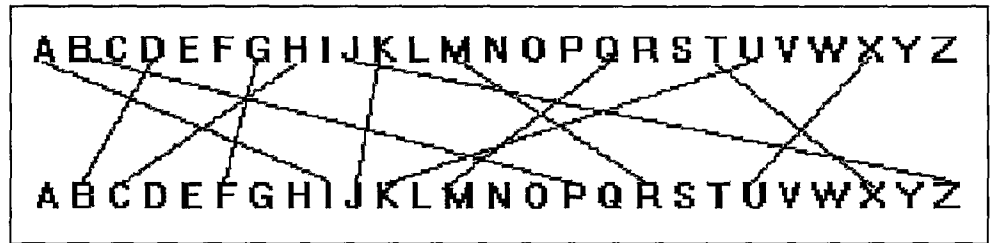
1.2.2.5. Transposition Chiper

Harflerin birbirleri ile değil de metin içerisinde yer değiştirmeleri esasına dayanır. Bu metot ile şifrelemede, Random Chiper'da olduğu gibi, standart bir anahtar yoktur. Örneğin $(1,2,3,4,5,6)=(5,3,4,6,1,2)$ şeklinde bir anahtar belirlenmişse "MAKBUZ" kelimesi "UKBZMA" şeklinde, anahtar $(1,2,3,4,5,6)=(3,6,5,2,1,4)$ ise "KZUAMB" şeklinde şifrelenecektir²².

1.2.2.6. Enigma

En yaygın şekilde İkinci Dünya Savaşında kullanılan Enigma pil ile çalışan, taşınabilir bir şifreleme makinesidir. Enigma şifreleme için harflerin değiştirilmesi (shift transformation) metodunu kullanır ve harflerin yer değiştirmesi çarklardan oluşan bir düzenekle sağlanır²³.

Enigma'ya temel olacak ilk makine 1918'de Arthur Scherbius tarafından Berlin'de yapılmıştır²⁴. Scherbius'un temel düşüncesi karakterleri birbirleri ile değiştirmek için elektrik devrelerinden faydalanmaktır. Üzerinde harfler bulunan yirmi altı elektrik anahtarı ve bu anahtarların yaktığı yine üzerinde harfler bulunan yirmi altı lambadan oluşan bu makine örneğin "Q" harfinin yazılı olduğu tuşa basıldığında "M" harfinin yazılı olduğu lambanın yanması ile gerçek metinde "Q" harfinin şifreli metinde "M" ile değiştirilmesi gerektiğini gösteren basit bir mekanizmaya sahipti (Şekil 1.4.).



Şekil 1.4. Enigma'da Kullanılan Algoritma (1. Adım)

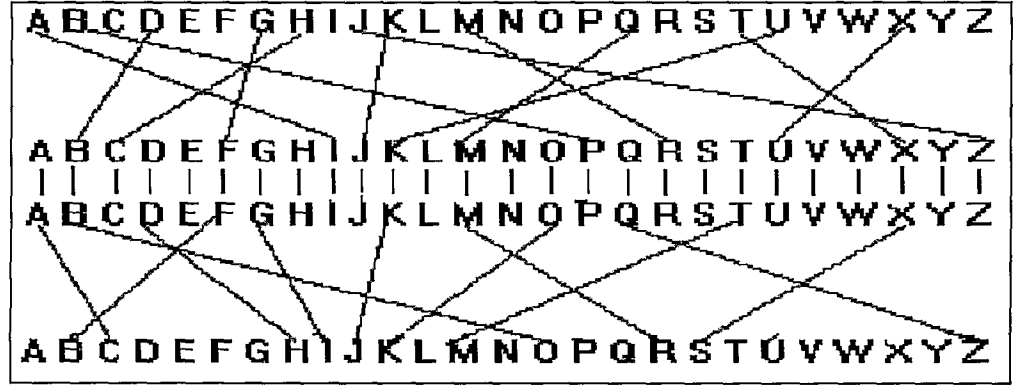
Bu metotla elde edilecek şifrenin kolayca kırılabilmesi düşüncesi ile şifreleme işlemini karmaşıktırmak için makineye ikinci bir kablo seti eklenmiş ve birinci setin

²² <http://www.emmy.nmsu.edu/~crypto>

²³ Petras, Richard T, A.G.E.

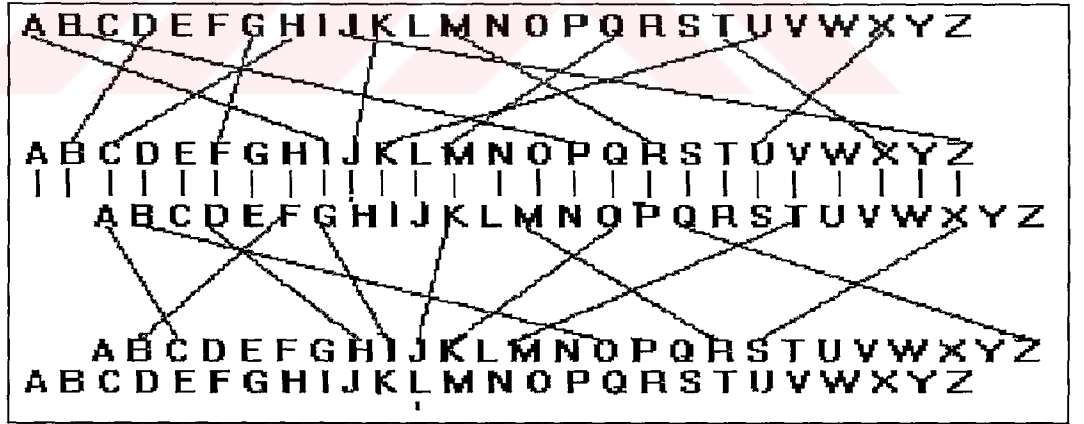
²⁴ <http://www.codesandciphers.org.uk/enigma/enigma1.htm>, S.E.T: 25.08.2002

alt satırı ikinci setin üst satırına bağlanmıştır. Böylece “Q” harfine basıldığında ikinci setteki “M” harfine ait anahtar kapatılıp bu sette “M” anahtarının karşılığı olan “R” harfine ait lambanın yanması sağlanmaktadır (Şekil 1.5.).



Şekil 1.5. Enigma’da Kullanılan Algoritma (2. Adım)

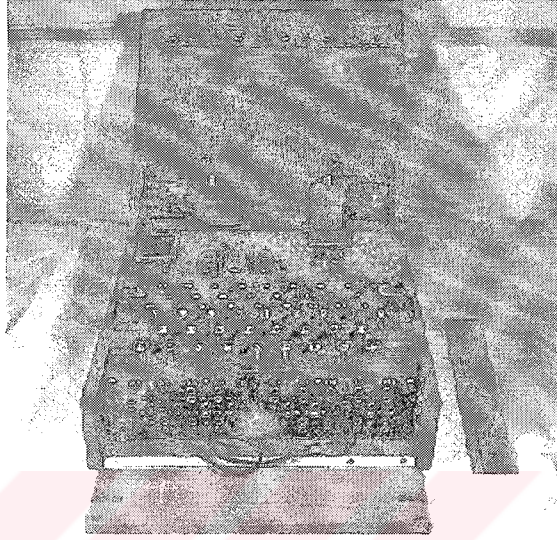
Üçüncü adım olarak ikinci set Caesar Chiper’da olduğu gibi kaydırılmış ve en alta ilk setle aynı hizada bir satır eklenmiş, böylece bir harfin sonuca ulaşınca kadar beş kere değişmesi sağlanmıştır. Örnekteki “Q” harfi “M” anahtarını, “M” anahtarı “K” anahtarını, “K” anahtarı ise “J” anahtarını kapatmakta “J” anahtarı ise “L” harfine ait lambayı yakmaktadır (Şekil 1.6.).



Şekil 1.6. Enigma’da Kullanılan Algoritma (3. Adım)

Üçüncü ve beşinci satır farklı miktarlarda kaydırılabileceğinden bu şekli ile Enigma’da $26 \times 26 = 676$ farklı kaydırma yapılabilir ve setlerin başlangıç noktaları ile kaydırmanın yönü ve miktarı çarklar (rotors) yardımıyla ayarlanabiliyordu. Daha sonra Willi Korn sisteme bir reflektör eklemiş ve $26 \times 26 \times 26 = 17576$ farklı alfabeyle ulaşılmıştır. Ayrıca reflektör sayesinde sistem karşılıklı olarak aynı sonucu verir hale

gelmiştir. Yani çarklar aynı düzende iken “A” harfinin sonucu “Q” ise şifre çözme modunda “Q” harfinin sonucu da “A” olarak bulunmaktadır. Son olarak setlerin içerisindeki rasgele eşleştirmeleri değiştiren bir fiş mekanizması (Plugboard) eklenmiştir.



Şekil 1.7. Enigma

Kaynak: <http://www.swimmer.org/morton/enigma.html> S.E.T. 22.08.2002.

İkinci Dünya Savaşında kullanılan Enigma, 1928 yılında, Varşova’da bir fabrikada seri olarak üretilmeye başlanmıştır (Şekil 1.7.). Ancak henüz İkinci Dünya Savaşından önce (1934) Poznan Üniversitesi’nde matematik öğrencisi olan Rajewski, Rozycki ve Zygaliski Enigma sinyallerini çözmeyi başarmıştır²⁵.

1.2.2.7. DES (Data Encryption Standart)

DES 1977 tarihinde Amerikan Hükümetinin isteği ile IBM firması tarafından geliştirilmiş bir şifreleme algoritmasıdır. IBM firması bir çok şifreleme algoritması geliştirdiği halde DES özel bir önem kazanmış ve kapalı anahtarlı algoritmaların içerisinde en çok tanınan ve en çok kullanılanı olmuştur^{26,27}. DES’in çalışma sisteminde temel olarak şu adımlar izlenir:

- Gerçek metni oluşturan karakterlerin ASCII kodlarının alınması.

²⁵ <http://www.ugrad.cs.jhu.edu/~russell/classes/enigma/history.html> S.E.T. 22.08.2002

²⁶ Coppersmith, Don, Chris Holloway, Stephen M Matyas, Nev Zunic, “Data Encryption Standart”, *Information Security Technical Report*, 1997, Sayı 2, No 2, ss. 22-24.

²⁷ Shepherd, Simon J., “A High Speed Software Implementation of the Data Encryption Standart”, *Computers & Security*, 1995, Sayı 14, ss. 349-357.

- Elde edilen sayı dizisinin 64-bit (8 karakter) uzunluğunda bloklara ayrılması.
- Her bloğun kendi içerisinde 32-bit uzunluğunda iki parçaya bölünmesi
- Her bloğun 16 aşamalı bir algoritma ile dönüştürülmesi
- Bu işlemlerin 64-bitlik her blok için uygulanması
- Bloklar birleştirilerek şifreli metnin elde edilmesi

Daha iyi anlaşılabilmesi için DES algoritmasının şekil üzerinde gösterilmesinde yarar vardır. Ancak on altı aşamalı algorithmada ilk ve son aşama dışındaki tüm adımlar aynı işlemlerin tekrarlanması şeklinde gerçekleşir. Bu yüzden ilk ve son aşamaların gösterilmesi yeterli olacaktır.

Şifrelenecek metnin ASCII kodları soldan sağa doğru $b_1, b_2, b_3, \dots, b_{64}$ değişkenlerine aktarılır. Elde edilen bu diziye “Initial Permutation (Başlangıç Dizilimi)” veya kısaca “IP” adı verilir. Daha sonra bu değişkenler Şekil 1.8’de gösterilen sıra ile sistematik olarak dizilir. Elde edilen ikinci dizi “Initial Text (Başlangıç Metni)” olarak adlandırılır ve T_0 ile gösterilir. Sekiz satır sekiz sütun şeklinde yazılan başlangıç metni ilk dört satırı sol yarı (L_0) ikinci dört satırı sağ yarı (R_0) olmak üzere iki kısma ayrılır.

1	2	3	4	5	6	7	8	58	50	42	34	26	18	10	2	L_0
9	10	11	12	13	14	15	16	60	52	44	36	28	20	12	4	
17	18	19	20	21	22	23	24	62	54	46	38	30	22	14	6	
25	26	27	28	29	30	31	32	64	56	48	40	32	24	16	8	
33	34	35	36	37	38	39	40	57	49	41	33	25	17	9	1	R_0
41	42	43	44	45	46	47	48	59	51	43	35	27	19	11	3	
49	50	51	52	53	54	55	56	61	53	45	37	29	21	13	5	
57	58	59	60	61	62	63	64	63	55	47	39	31	23	15	7	
IP								T_0								

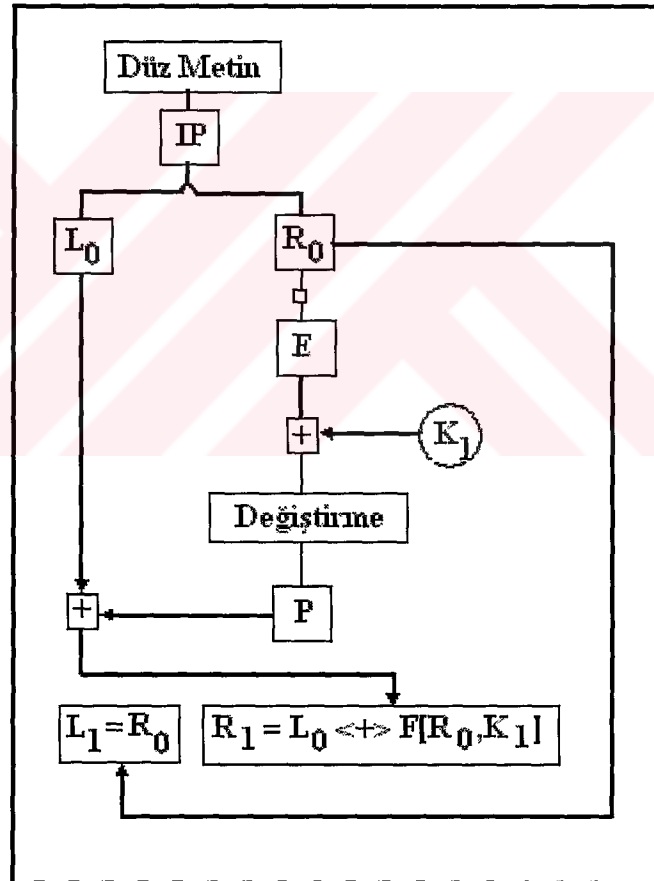
Şekil 1.8. Başlangıç Dizilimi (IP) ve Başlangıç Metni (T_0)

32 bit uzunluğundaki sağ yarı (R_0) dört aşamalı bir fonksiyon (F) ile dönüştürülür. İlk aşamada 32 bit olan R_0 , 48 bit uzunluğunda yeniden derlenir. 48 bitlik bu seri E-tablosu olarak adlandırılır (Şekil 1.9). İkinci aşamada E-tablosu 64 bitlik anahtardan elde edilen 48 bit uzunluğundaki ilk anahtar (K_1) ile (XOR) mantıksal işlemine girer. Elde edilen dizi üçüncü aşamada 32 bit uzunluğunda yeniden işlenir ve

bu dizi (P) sol yarı (L_0) ile (XOR) işlemine tabi tutulur. Bu işlemin sonucu olan dizi (R_1)dir. (R_0) ise (L_1) olarak yazılır ve dört aşamalı fonksiyon ile birlikte algoritmanın da birinci aşaması tamamlanır (Şekil 1.8).

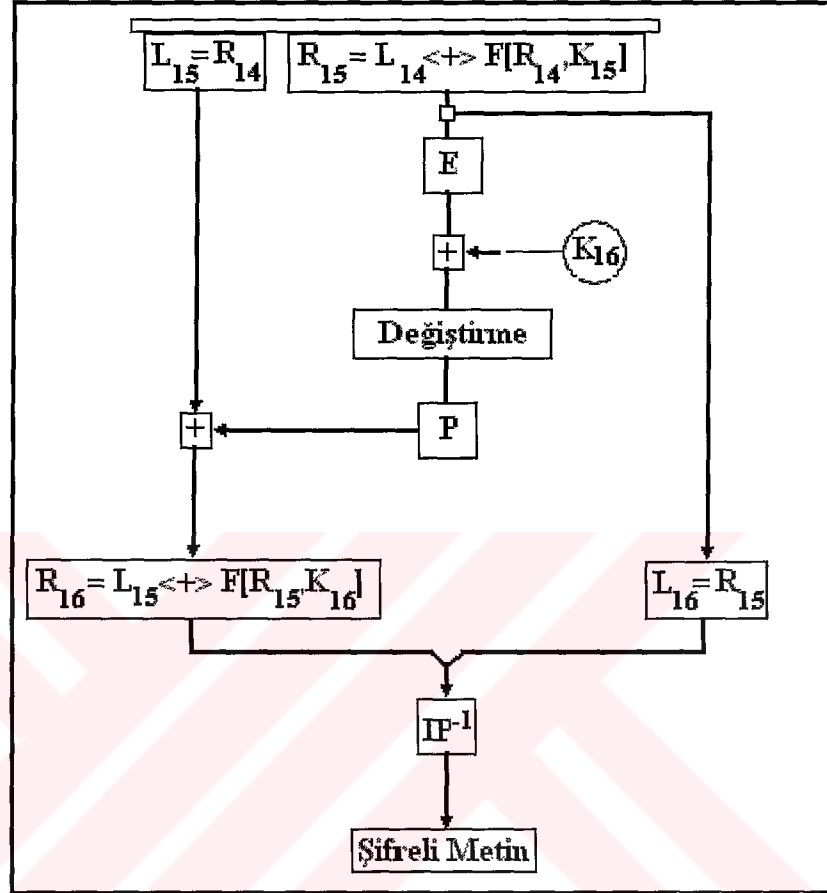
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Şekil 1.9. E-tablosu



Şekil 1.10. DES Birinci Aşama

Bu şekilde tekrarlanan 16 aşamanın sonunda elde edilen (L_{16}) ve (R_{16}) birleştirilerek başlangıç diziliminin dönüştürülmüş şekli (IP^{-1}) elde edilir ve ASCII tablosu kullanılarak şifreli metne dönüştürülür (Şekil 1.11)^{28,29}.



Şekil 1.11. DES Son Aşama

DES algoritmasının gelişimi ilk ortaya çıktığı 1977 tarihinden sonra devam etmiş ve son ulaştığı şekline Triple-DES ismi verilmiştir. Triple-DES de üç farklı almortmaya ayrılır.

- 1- DES-EEE3: Metin üç ayrı anahtar kullanılarak üç kez şifrelenir.
- 2- DES-EDE3: Metin birinci anahtarla şifrelenir, ikinci anahtarla deşifre edilir ve üçüncü anahtarla tekrar şifrelenir.

²⁸ Ford, Warwick, *Computer Communications Security*, Prentice Hall PTR, 1994, ss. 238-253.

²⁹ FIPS Pub 46-3, "Data Encryption Standard (DES)", *Federal Information Processing Standards Publication*, 25 Ekim 1999, ss. 8-15.

3- DES-EDE2: İkinci algoritmadan farkı ilk ve son adımlarda aynı anahtarın kullanılmasıdır³⁰.

1.2.2.8. AES (Advanced Encryption Standard)

AES şifreleme algoritması Belçikalı iki bilim adamı tarafından (Dr. Vincent Rijmen ve Dr. Joan Daemen) geliştirilmiş ve NIST tarafından 2 Nisan 1997 tarihinde tanıtılmıştır³¹. FIPS, 26 Kasım 2001 tarihli bir yayınla AES'i "128 bitlik veri bloklarını 128, 192, 256 bitlik anahtarlarla şifreleyen" kayıtlı şifreleme algoritması olarak ilan etmiştir^{32,33}. NIST'in bir algoritmayı standart olarak belirlemesi için algoritmanın bir çok değerlendirme kriterine uyması gerekir. Bu kriterler temel olarak üç ana başlık altında toplanabilir:

1- Güvenlik Şartları: En önemli değerlendirme kriteri algoritmanın kriptanalize karşı dirençli olmasıdır.

2- Maliyet Şartları: Algoritmanın kullanım maliyetlerinin düşük olması gerekir.

3- Algoritmanın Uygulanabilirliği: Algoritma için yalnızca şifreleme yapması yeterli bir ölçü değildir. Algoritma, veri iletişimi güvenlik teknolojileri (Sayısal Sertifika v.b.) ile uyumlu olması ve bu teknolojilerde kullanılabilmelidir^{34,35}.

AES ile DES algoritmalarının özellikleri karşılaştırmalı olarak şu şekilde sıralanabilir:

- İkisi de simetrik anahtarlı (Private Key) algoritmalarıdır. DES 56 bit anahtar kullanırken AES için anahtar uzunluğu 128,192 veya 256 bit olabilir. DES'in 56 bit anahtar uzunluğu 5.1×10^{33} farklı anahtara izin verirken AES için 128 bit anahtar uzunluğunun izin verdiği farklı anahtar sayısı $= 3,4 \times 10^{38}$ dir.

³⁰ Syed, Furqan, "Children of DES: A Look at the Advanced Encryption Standard", *Network Security*, Eylül 2000, ss. 11-12.

³¹ Palmer, Chloe, "DES Replacement Announced", *Computer Fraud & Security*, Kasım 2000, s. 1.

³² GPO, Federal Register, Ocak 1997, Sayı 62, No 1, ss. 93-94, www.access.gpo.gov, S.E.T. 03.04.2002.

³³ FIPS Pub 197, "Announcing the Advanced Encryption Standard (AES)", *Federal Information Processing Standards Publication*, 26 Kasım 2001.

³⁴ Wright, Marie A., "The Evolution of the Advanced Encryption Standard", *Network Security*, Kasım 1999, ss. 11-14.

³⁵ Murphy, Sean, "The Advanced Encryption Standard", *Information Security Technical Report*, 1999, Sayı 4, ss. 12-17.

- İki de gerçek metni bloklar halinde şifreler. DES 64 bitlik bloklar kullanır ve her 64 bit de 32 bitlik iki blok olarak işleme alınır. AES’de ise şifrelenecek metin 128 bitlik bloklara ayrılır^{36,37}.

- İki algoritmada da tekrarlanan aşamalar (iterasyon) sonucunda çözüme ulaşılmaktadır. DES algoritmasında tekrarlanma adedi sabittir. Dört aşamalı bir fonksiyon on altı kez tekrarlanır. AES’te ilk dikkati çeken özellik üç farklı anahtar uzunluğudur. AES’te bir aşamayı oluşturan esas işlemler anahtar uzunluğuna göre artan sayıda defalarca tekrarlanır. AES, tekrarlanma sayısı, dolayısıyla anahtar uzunluğu oranında karmaşıklaşan bir algoritmadır³⁸.

Anahtarın Genişletilmesi

AES algoritmasında ilk adım anahtarın 32 bit uzunluğunda tablolar halinde genişletilmesidir. Gerçek metin aşamalar halinde şifrelenirken 32 bit uzunluğundaki anahtar tablolardan her aşama için dört adet kullanılır. Bu da 128 bit uzunluğundaki anahtar için 10 aşama ve 44 adet anahtar tablosu anlamına gelir. Yani 128 bitlik anahtar $44 \times 32 = 1408$ bit uzunluğuna genişletilmektedir. Genişletilmiş anahtar uzunluğu 192 bitlik anahtar için 12 aşama ve $52 \times 32 = 1664$, 256 bitlik anahtar için 14 aşama ve $60 \times 32 = 1920$ bit olmaktadır.

“State” Matris ve Şifreleyici Fonksiyonlar

Metinde şifrelenecek 128 bit uzunluğundaki blok “State” adı verilen 4×4 matrise yerleştirilir (Şekil 1.12). Matristeki her alan 1 byte (8 bit) veriye karşılık gelmektedir. Şifrelemede bu aşamadan sonraki işlemler “State” matrisi üzerinde yapılacaktır.

“State” Matrisin her satırı 32 bit uzunluğundadır ve aynı uzunluktaki anahtar tabloları kullanılarak dönüştürülür. Dönüştürme işlemleri için dört temel fonksiyon aşağıdaki sıra ile kullanılır.

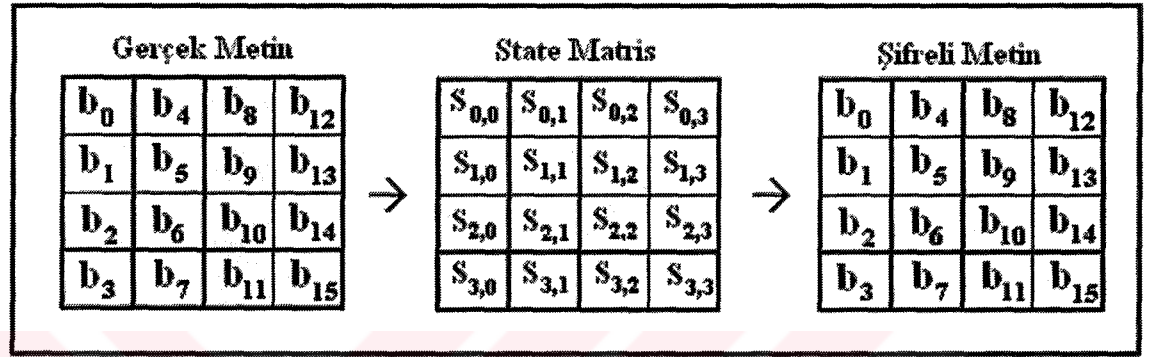
1- SubBytes: S-Box adı verilen ve doğrusal olmayan bir fonksiyon yardımı yer değiştirme işlemleri icra eder.

³⁶ Syed,Furqan. A.g.e.

³⁷ Wright, Marie A., “The Advanced Encryption Standard”, *Network Security*, Ekim 2001, ss. 11-13.

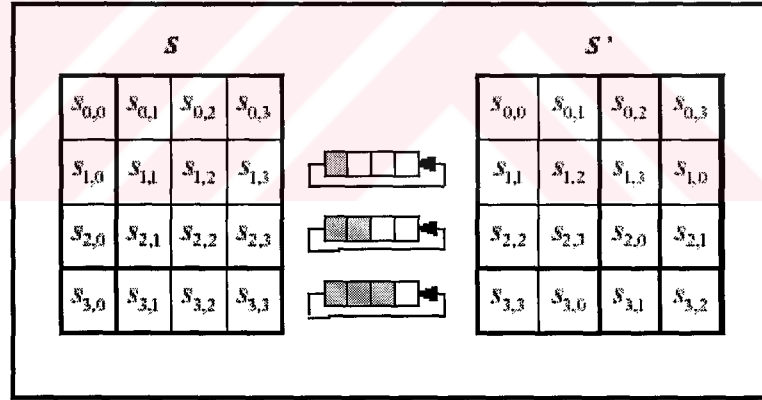
³⁸ Alman, Stuart, “Encryption and security: the Advanced Encryption Standard”, *EDN*, 31 Ekim 2002, ss. 26-30.

- 2- ShiftRows: State matrisinin son üç satırındaki hücreleri dairesel olarak öteler (Şekil 1.13).
- 3- MixColumns: GF(28) adı verilen bir işlemle state matrisin sütunları üzerinde yer değiştirme işlemleri icra eder.
- 4- AddRoundKey: “State” matrisin her hücresini icra edilen aşamaya ait anahtar ile (XOR) işlemine tabi tutar.



Şekil 1.12. State Matris

Kaynak: FIPS Pub 197. s. 9.



Şekil 1.13. ShiftRows

Kaynak: FIPS Pub 197. s. 17.

Sonuç Algoritmaları

AES’de son aşama dönüştürme işlemleri için farklı yöntemler uygulanabilir. Bu yöntemlerden beş tanesi NIST tarafından Ağustos 1999 tarihli bir yayınlı standart olarak ilan edilmiştir. Bu yöntemler:

- Mars,
- RC6,

- Rijndael,
- Serpent ve
- Twofish'dir.

MARS, IBMC (Armong, New York) adlı bir şirket tarafından geliştirilmiş ve dijitaler arasında bir çok yer değiştirme tekniğini kapsayan bir metottur. RC6, RSA (Bedford, Massachusetts) laboratuvarlarında geliştirilmiştir. RIJNDAEL algoritmasının geliştiricileri Joan Daemen ve Vincent Rijmen adında iki Belçikalı kriptoloji uzmanıdır. SERPENT, Ross Anderson (İngiltere), Eli Biham (İsrail) ve Lars Knudsen (Norveç) tarafından geliştirilmiştir. TWOFISH ise altı Amerikalı (Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Neils Ferguson) tarafından geliştirilmiştir^{39,40}.

Bunların dışında var olan bir çok yöntem ve yeni yöntemler geliştirmek için yoğun çabalar harcanması AES'in simetrik anahtarlı şifreleme algoritmalarının geleceğinde önemli bir yer tutacağı konusunda ümit vermektedir⁴¹. Söz konusu yöntemlerden bazıları şu şekilde sıralanabilir:

- Cast 256
- Crypton
- Deal
- DFC
- E2
- Frog
- HPC
- LOKI97
- Magenta
- Safer +

³⁹ Asenjo, Juan C., "The Advanced Encryption Standard: Implementation and Transition to a New Cryptographic Benchmark", *Network Security*, 1 Temmuz 2002, Sayı 7, ss. 7-9.

⁴⁰ Wright, Marie A. A.G.E. (1)

⁴¹ Forte, Dario, "The Future of the Advanced Encryption Standart", *Network Security*, Haziran 1999, ss. 10-13.

1.2.3. Açık Anahtarlı Şifreleme (Public-Key Cryptography)

Kapalı anahtarlı şifrelemede güvenlik, gönderici ve alıcı arasında bir uzlaşma ile sağlanır. Bu uzlaşma, şifrelemede kullanılan anahtarların üçüncü bir kişi tarafından bilinmemesini sağlamaya yönelik, iki tarafın da uyacağı tedbirler alınması ile ortaya çıkmaktadır. Ancak değiştirme esaslı şifrelemede üçüncü kişilerin anahtarı bilmese de şifreli metni çözme şansı yüksektir. Örneğin basit Shift Transformation ile şifrelenmiş bir metin için yirmi beş farklı anahtar seçeneği tek tek denenerek kolayca çözülebilir. Ayrıca bu tür şifrelemede üçüncü kişilerin şifreleyici anahtarları bilmesi durumunda mesajın çözülmesini engelleyebilecek herhangi bir koruma yoktur.

Açık anahtarlı şifreleme 1970'lerin sonlarına doğru ortaya çıkan yeni bir yaklaşım ve bu yeni yaklaşımdan hareket edilerek geliştirilmiş bir çok algoritmayı ifade eder. Açık anahtarlı şifreleme açık anahtarlı kriptosistemlerde ise şifreleyici anahtarın bilinmesi üçüncü kişilere şifrenin çözümü için herhangi bir kolaylık sağlamaz. Hatta kullanılan şifreleyici anahtarlar genellikle açıklanır⁴².

1.2.3.1. RSA (Rivest, Shamir, Adleman Cryptography)

Rivest, Shamir ve Adleman 1977'de açık anahtarlı bir kriptosistem ortaya koymuş ve bu sisteme isimlerinin baş harflerinden oluşan RSA ismini vermişlerdir⁴³. RSA temel olarak aralarında asal sayılara ve modüler aritmetiğe dayanır. İlk önce p ve q gibi iki sayı belirlenir. Bu iki sayının büyüklüğü şifrenin çözülmesinin de zorluk derecesini belirler. Daha sonra $N = p \cdot q$ ve $k \equiv 1 \pmod{(p-1)(q-1)}$ sayıları bulunur. Bu aşamada birden fazla k sayısı elde edileceğinden bu sayılardan bir tanesi seçilerek kullanılacaktır. Seçilen k sayısından $k = e \cdot d$ olmak üzere e ve d sayıları elde edilir. Bu durumda şifreleyici anahtar e ve N, çözücü anahtar ise d olacaktır. E ve N sayıları açık anahtar sistemi gereği ilan edilir, d ise kapalı anahtar olarak saklı tutulur⁴⁴. Şifreleyicinin kullanacağı fonksiyon şu şekildedir:

$$C = E(P) \equiv P^e \pmod{N}$$

⁴² Diffie, Whitfield, "The National Security Establishment and the Development of Public-Key Cryptography", *Designs Codes and Cryptography*, 1996, Sayı 7, ss. 9-12.

⁴³ Heinlein, Edwin B., "The RSA Security Conference 1995", *Computers & Security*, 1995, Sayı 14, ss. 24-26.

⁴⁴ Chang, Chin-Chen, Shin-Jia Hwang, "A Simple Approach for Generating RSA Keys", *Information Processing Letters*, 1997, Sayı 63, ss. 19-21.

Alıcı ise bu şifreyi çözmek için şu fonksiyonu kullanır:

$$P = D(C) \equiv C^d \text{ mod } N$$

Örnek olarak şifrelenecek metnin ilk karakteri $B=2$ olsun. $p = 2$ ve $q = 11$ seçilirse:

$$N = 2.11 = 22 \text{ olacaktır.}$$

$$k \equiv 1 \text{ mod } (2 - 1)(11 - 1)$$

$$k \equiv 1 \text{ mod } 10$$

Bulunacak ilk iki k değeri 11'dir. Ancak 11 asal sayı olduğundan seçilemez.

21 = 7. 3 seçilirse $e = 7$ ve $d = 3$ olarak belirlenir.

$$C = E(2) \equiv 2^7 \text{ mod } 22 \equiv 18 \text{ mod } 28 \text{ olur.}$$

Şifre çözülürken $d=3$ kapalı anahtarı kullanılacaktır.

$$P = D(3) \equiv 18^3 \text{ mod } 22 \equiv 2 \text{ mod } 22$$

Yukarıda verilen örnekte RSA şifreleme tekniğinin mantığı basit işlemlerle kullanılmıştır. İşlemler daha karmaşık olarak yapılabilir ancak temelde aynı mantık kullanılmaktadır⁴⁵. Şifrenin kırılabilmesini güçleştirmek için yapılabilecek işlemlere bir örnek de harflerin gruplandırılarak şifrlenmesidir. "HERE" kelimesi "HE-RE" olarak ayrılıp ilk iki karakter $H=07$ ve $E=04$ birlikte şifrenirse $HE=0704=704$ ve $RE=1704$ kullanılacaktır.

$$p = 101 \text{ ve } q = 29 \text{ olsun;}$$

$$N = 101.29 = 2929$$

$$k \equiv 1 \text{ mod } (101 - 1)(29 - 1)$$

$$k \equiv 1 \text{ mod } (2800)$$

$$k = \{28001, 56001, \dots\}$$

$$k = 5601 \text{ seçilirse } e = 3 \text{ ve } d=1867$$

İlk iki karakter için kullanılacak değer $P=704$ idi

⁴⁵ Lee, Wei-Bin, Chin-Chen Chang, "Using RSA With Low Exponent in a Public Network", *Computer Communications*, 1998, Sayı 21, ss. 284-286.

$$C(704)=704^3 \bmod 2929 \equiv 2397 \bmod 2929$$

Sonraki iki karakter için $P = 1704$

$$C(1704)=1704^3 \bmod 2929 \equiv 1136 \bmod 2929$$

Şifrelemede Kullanılan Matematiksel Metotlar

Şifrelemede en çok kullanılan matematiksel metot modüler aritmetiktir. Modüler aritmetik, saat aritmetiği olarak da bilinir. Bilindiği gibi saat 14:00 iken aynı zamanda 2:00 PM olarak da ifade edilebilir. Bu ifadenin matematikteki karşılığı $14 \equiv 2 \pmod{12}$ şeklindedir. Tanım olarak: a, b, c, m tamsayı ve $m \geq 0$ olmak üzere

$a = c.m + b$ eşitliği $a \equiv b \pmod{m}$ olarak yazılır ve “ $a, b \bmod m$ ile benzerdir” şeklinde okunur.

Modüler aritmetik için aşağıdaki özellikler tanımlanabilir:

$$\mathbb{Z}_m = \{ 0, 1, \dots, m-1 \} \text{ için;}$$

$$a, b \in \mathbb{Z}_m \text{ ise } a + b \in \mathbb{Z}_m$$

$$a, b \in \mathbb{Z}_m \text{ ise } ab \in \mathbb{Z}_m$$

$$a, b \in \mathbb{Z}_m \text{ ise } a + b \equiv b + a$$

$$a, b \in \mathbb{Z}_m \text{ ise } ab \equiv ba$$

$$a, b, c \in \mathbb{Z}_m \text{ ise } (a + b) + c \equiv a + (b + c)$$

$$a, b, c \in \mathbb{Z}_m \text{ ise } (ab)c \equiv a(bc)$$

$$a \in \mathbb{Z}_m \text{ ise } a + 0 = 0 + a \equiv a$$

$$a \in \mathbb{Z}_m \text{ ise } a1 \equiv 1a \equiv a$$

$$a \in \mathbb{Z}_m \text{ ise } a + (m - a) \equiv (m - a) + a \equiv 0$$

$$a \in \mathbb{Z}_m \text{ ise } (a + b)c \equiv (ab) + (ac) \text{ ve } a(b + c) \equiv (ab) + (ac)$$

$ax \equiv b \pmod{m}$ benzerliği herhangi bir $a \in \mathbb{Z}_m$ için her $b \in \mathbb{Z}_m$ durumunda bir ve yalnız bir $x \in \mathbb{Z}_m$ çözümüne sahipse bu durum $\gcd(a, m) = 1$ olarak ifade edilir. Bu eşitlik a ve m sayıları aralarında asaldır şeklinde ifade edilir. Bir $m \in \mathbb{Z}$ için bütün aralarında asal sayıların kümesi $\mathcal{O}(m)$ olarak gösterilir. Örneğin $m=26$ için $26=1 \times 26$, $26 = 2 \times 13$ eşitlikleri vardır. Bu durumda 1, 2 veya 13'ün katı olmayan her $a \in \mathbb{Z}_m$ için $\gcd(a, m) = 1$ doğrudur. $\mathcal{O}(26) = \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$

$a \in \mathbb{Z}_m$ için $aa^{-1} \equiv a^{-1}a \equiv 1 \pmod{m}$ denkleğini sağlayan a^{-1} sayısına a 'nın çarpma işlemine göre tersi denir.⁴⁶

1.2.3.2. RABIN

Birbirine yakın büyüklükte rasgele iki sayı (p , q) üretilir. Bu sayıların çarpımı $n=pq$ algoritmanın açık anahtarıdır. Kapalı anahtar ise p ve q sayılarıdır.

Şifrelenecek mesaj (m), şifrelenmiş mesaj (c) ise: $c = m^2 \pmod{n}$ olarak hesaplanır.

Şifreli mesaj deşifre edilirken ilk aşamada kök adı verilen dört farklı m değeri hesaplanır. İkinci aşamada kök değerlerden hangisinin gerçek m değeri olduğuna karar verilir.

$$r \equiv c^{(p+1)/4} \pmod{p}.$$

$$s \equiv c^{(q+1)/4} \pmod{q}.$$

$$x \equiv (aps + bqr) \pmod{n}.$$

$$y \equiv (aps - bqr) \pmod{n}.$$

$$m_1 = x$$

$$m_2 \equiv -x \pmod{n}$$

$$m_3 \equiv y$$

$$m_4 \equiv -y \pmod{n}.$$

⁴⁶ Stinson, Douglas R., *Cryptography: Theory and Practice*, CRC Press Inc., 1995, ss. 9-10.

1.2.3.3. ELGAMAL

Algoritmanın üç tane açık anahtarı vardır: (p) , (α) ve $(\alpha a \bmod p)$. Kapalı anahtar ise a ($1 \leq a \leq p-2$) olarak belirlenir.

Şifrelenecek mesaj ($0 \leq m \leq p-1$), şifrelenmiş mesaj (c) ise:

Rasgele bir k ($1 \leq k \leq p-1$) sayısı belirlenir.

$\gamma = \alpha^k$ ve $\delta = m \cdot (\alpha a)^k$ hesaplanır.

$c = (\gamma, \delta)$ olarak belirlenir.

Şifreli mesaj deşifre edilirken.

$\gamma^{p-1-a} = \gamma^{-a} = \alpha^{-ak}$

$(\gamma^{-a}) \cdot \delta = \alpha^{-akm} \alpha^{ak} = m$

eşitliklerinden yararlanılarak $m = (\gamma^{-a}) \cdot \delta \bmod p$ olarak bulunur.

1.2.3.4. McELIECE

Açık anahtar uzunluğu ve işlem sayısı hayli fazla olan bir algoritmadır. Anahtarlar matrislerle ifade edilir. Bu algoritma kullanılırken önce sisteme ait üç değişkenin (k, n, t) değeri belirlenir ve bu değerler sürekli sabit tutulur. Açık anahtar $(\hat{G}, t)$ 'dir. $\hat{G}$ matrisi $k \times n$ büyüklüğündedir ve S ($k \times k$) G ($k \times n$) ve P ($n \times n$) matrisleri kullanılarak hesaplanır ($\hat{G} = SGP$). Kapalı anahtar ise S, G, P matrisleridir. Ayrıca n uzunluğunda bir vektör de anahtar olarak kullanılır. ($c = m\hat{G} + z$) olarak hesaplanan şifreli mesaj vektörü deşifre edilirken önce ($\hat{c} = cP^{-1}$) hesaplanır ve bu vektör ile G matrisi kullanılarak yapılan dönüştürme işlemleri sonucunda M vektörü ve son olarak deşifre edilmiş metin ($m = MS^{-1}$) bulunur⁴⁷.

⁴⁷ Menezes, Alfred J., Paul C. van Oorschot, Scott A. Vanstone, *Handbook of Applied Cryptography*, CRC Pres, 3. Baskı, 2001, ss. 292-300.

1.3. Kriptanaliz (Cryptanalysis)

Kriptanaliz şifreli metnin gerçek metne dönüştürülmesi işlemleri ile ilgilenir. Bu dönüştürme iki farklı yoldan yapılabilir. Birincisi şifrelemede kullanılan algoritmanın ve anahtarların bilinmesi durumunda şifreleyici fonksiyonun geriye işletilerek şifrenin çözülmesi yoludur. Bu yolla yapılan çözümlemeye dekripsiyon (decryption) adı verilir. İkinci yol şifreli metnin anahtarlar ve/veya algoritmalar kullanılmadan çözülmesidir. İkinci yolla yapılan çözümlemeye ise şifre kırma (code breaking) adı verilmektedir. Ancak yaygın uygulama kriptanaliz kavramının dekripsiyon dışındaki matematiksel veya istatistiksel şifre çözme metotları için kullanılması yönündedir⁴⁸. Belirli bir şifreleme algoritması ile şifrelenmiş metnin çözülmesi için şifreleyici anahtar ya da algoritma kullanılmadan oluşturulan metoda, veya şifre kırma algoritmasına, saldırı (attack) adı verilir.

Kriptanaliz konusu sınıflandırılması zor, karmaşık metotların bir araya gelmesi ile oluşmuştur. Örneğin anahtar uzunluğuna veya bloklara ayrılıp ayrılmamasına göre farklılaşan metotlar vardır ancak bu metotların bir çoğu tek bir algoritmayı kırmak için geliştirilmiş saldırılardır.

1.3.1. Dilbilgisi Kuralları ve Kriptanaliz

Kriptanalizde en çok kullanılan dilbilgisi kuralları harflerin veya kelimelerin tekrar oranlarıdır (redundancy). Örneğin İngilizce metinlerde en çok kullanılan harf “e” (%14), en az kullanılan harfler ise “q” ve “z” dir (%1’den az)⁴⁹. Bu oranlarla Şifreli metinde kullanılan harflerin tekrarlanma oranları istatistiksel metotlarla karşılaştırılarak gerçek metne ulaşmak için önemli ipuçları elde edilebilir.

Harflerin tekrar oranları dışında zamir, edat, zarf olarak kullanılan kısa kelimelerin kullanım oranları da şifre çözmede önemli ipuçları vermektedir. Örneğin “e” harfi ile biten üç harfli bir kelimenin “the” olma olasılığı çok yüksektir.

1.3.2. Anahtar Tahmini ve Kriptanaliz

Eğer şifreleyici algoritma biliniyorsa kullanılan anahtarın bulunması şifrenin çözülmesi için yeterli olacaktır. Kriptanaliz çalışmaları büyük çoğunlukla bu alanda

⁴⁸ Menezes Menezes, Alfred J., a.g.e., s. 15.

⁴⁹ Menezes Menezes, Alfred J., a.g.e., s. 16.

yapılmaktadır. Anahtar tahmini için istatistiksel metotlar yanında özellikle açık anahtarlı kriptosistemlerde matematiksel yaklaşımlar da kullanılmaktadır.

1.3.3. Matematiksel Fonksiyonlar ve Kriptanaliz

Eğer şifreleme ya da anahtar üretimi matematiksel fonksiyonlar kullanılarak yapılıyorsa, şifreyi çözmek ve anahtarı bulmak için kullanılan matematiksel fonksiyonu bulmak gerekir.

Yukarıda da belirtildiği gibi kriptanaliz metotlarının sınıflandırılması zordur. Bir kriptanaliz metodu genellikle bir tek algoritmanın kırılması için geliştirilir ve yukarıdaki metotların hepsi aynı algorithmada kullanılabileceği gibi farklı yaklaşımların kullanılması da mümkündür.



BÖLÜM 2 ELEKTRONİK TİCARETTE GÜVENLİK VE ŞİFRELEME

2.1. Elektronik Ticaretin Tanımı

2.1.1. Elektronik Ticaretin Tanımı ve Kapsamı

Son on-on beş yılda bilgisayar ve iletişim teknolojilerinde çok önemli gelişmeler gözlenmektedir. Bu gelişmeler elektronik teknolojilerindeki ilerlemelerle birlikte giderek daha yüksek kapasiteli bilgisayarların daha düşük maliyetlerle piyasaya sürülmesi ile iyice yaygınlaşmış ve hız kazanmıştır. Bunun sonucu olarak kişisel bilgisayarların yaygınlaşması ve neredeyse her evde bir bilgisayar bulunması mümkün olabilmektedir. Bu dönemde göze çarpan ikinci önemli gelişme yazılım ve iletişim hizmetlerinin göreceli öneminin donanımına göre hızla artmasıdır. Bu gelişmenin sonucunda bilgisayarlar kullanıcı açısından kolay erişilebilir ve anlaşılabilir bir çalışma aracı haline gelmiştir. Üçüncü önemli gelişme ise açık ağ teknolojilerinde yaşanmış ve Internet gelişmiş ülkelerden başlayarak hızla tüm dünyada yaygınlaşmıştır. Hatta günümüzde bilgisayar kavramı Internet'i de kapsayarak kullanılmakta, artık Internet'e bağlı olmaması bir bilgisayar için çok büyük bir eksiklik olarak kabul edilmektedir.

Bilgisayar ve iletişim teknolojileri bu gelişmeler sonucunda hayatın her alanında kullanılabilir hale gelmiş, özellikle haberleşme, eğitim ve ticarete önemli gelişmelere neden olmuştur. Bu gelişmelerin bir başka etkisi de her alanda yeni oluşumların ve bunların karşılığı olan yeni kavramların ortaya çıkmasıdır. Haberleşme alanında internet gazetesi, elektronik posta, eğitim alanında web tabanlı uzaktan eğitim, web üniversitesi gibi yeni kavramlar ortaya çıkarken, bu konuda en çok zenginleşen alan ticaret olmuştur. Dijital Para, Dijital Çek, Elektronik Banka, E-Market, Elektronik Fon Transferi ve daha bir çok yeni kavram ticari alanda kullanılmaya başlamış, tüm bu yenilikleri ifade eden Elektronik Ticaret (E-Ticaret) kavramı son yılların en dikkat çekici konusu haline gelmiştir.

E-Ticaret üzerinde farklı tanımlamalar yapılsa da bu tanımlar benzer kavramlar üzerine kurulmuş farklı ifadeler olarak karşımıza çıkmaktadır. OECD'nin 1997 yılında yaptığı bir tanıma göre E-Ticaret; hem kişileri, hem kurumları ilgilendiren ticari etkinliklere ait her türlü işlemlerin bilgisayar ağları üzerinden yapılmasıdır. Japonya E-

Ticaret Çalışma Grubu (ECOM), E-Ticareti, her türlü bilgisayar ağları üzerinden, ürünün tasarımı, üretilmesi, tanıtımının yapılması ve bunlarla ilgili olası tüm işlemler olarak tanımlar. Birleşmiş Milletler Yönetim, Ticaret ve Ulaştırma Usullerini Kolaylaştırma Merkezi (UN-CEFACT)'ne göre yönetim ve tüketim etkinliklerinin yürütülmesinde kullanılan tüm iş bilgilerinin üreticiler, tüketiciler, kamu kurumları ve diğer organizasyonlar arasında yapılması E-Ticaret anlamına gelir.⁵⁰ Türkiye Elektronik Ticaret Koordinasyon Kurulu (ETKK)'nin Mayıs 1998 tarihli hukuk çalışma grubu raporunda, E-Ticaret; bireylerin ve kurumların açık ağ ortamında (Internet) veya sınırlı sayıda kullanıcı tarafından ulaşılabilen kapalı ağ ortamlarında (Intranet) yazı, ses ve görüntü niteliğindeki sayısal bilgilerin işlenmesi, iletilmesi ve saklanması temeline dayanan ve bir değer yaratmayı amaçlayan ticari işlemlerin tümünü ifade etmektedir.

İletişim açısından elektronik ticaret, bilgilerin, malların, hizmetlerin veya ödemelerin telefon hatları, bilgisayar ağları veya diğer elektronik ortamlar kullanılarak dağıtılmasıdır. İş dünyası açısından elektronik ticaret iş ve bilgi akışının otomasyonu olarak düşünülebilir. Elektronik ticaretin bir hizmet olarak müşteri isteklerinin daha az maliyetle ve daha kısa zamanda karşılanmasına yönelik teknoloji kullanımı şeklinde tanımlanması da mümkündür⁵¹.

E-Ticaret en genel tanımı ile elektronik ortamda yürütülen tüm ticari amaçlı faaliyetleri kapsar. E-Ticaret kapsamındaki faaliyetleri farklı yaklaşımlar kullanarak sınıflandırmak mümkündür. E-Ticarete ticari faaliyetin tarafları şu şekilde sıralanabilir:

- Alıcı,
- Satıcı,
- Üretici,
- Bankalar,
- Komisyoncular,
- Sigorta şirketleri,
- Nakliye şirketleri,

⁵⁰ OECD, *Information Technology Outlook*, OECD Publications, Paris, 1997, s. 2.

⁵¹ Kalakota, Ravi, Andrew B. Whinston, *Electronic Commerce: A Manager's Guide*, Addison Wesley, 1997, s. 3.

- Sivil toplum örgütleri,
- Üniversiteler,
- Onay kurumları, elektronik noterler,
- Kamu kurumları.

Ticari faaliyetin tarafları açısından yapılan sınıflandırmada e-ticaret beş başlık altında incelenir:

- İşletme ile müşteri arasında yapılan faaliyetler,
- İki işletme arasındaki faaliyetler,
- İki kişi arasındaki faaliyetler,
- İşletme ile devlet arasındaki faaliyetler,
- Kişilerle devlet arasındaki faaliyetler.

Ticari faaliyetin türü açısından sınıflandırılırsa⁵²:

- İşletme içi faaliyetler (Muhasebe, Stok, Personel Yönetimi, Raporlama),
- Bilgi ve Haber Alma (Herhangi bir ürüne ait bilgi ve haberler, pazara ait bilgi ve haberler, rakiplerle ilgili bilgi ve haberler, ortaklarla ilgili bilgi ve haberler, mevzuat ile ilgili bilgi ve haberler),
- Reklam ve tanıtım faaliyetleri,
- Perakende mal ve hizmet satışı,
- Eğitim faaliyetleri,
- Bankacılık faaliyetleri,
- Borsa,
- Vergi gibi devlete karşı mükellefiyetlerin yerine getirilmesi veya kamu kuruluşlarından izin, ruhsat, ehliyet vb belge temin edilmesi⁵³,
- Proje takibi, ücret karşılığı elektronik ortamda veri aktarımı,

⁵² Turban, Efraim, Jae Lee, David King, H. Michael Chung, *Electronic Commerce: A Managerial Perspective*, Prentice-Hall Inc., 1999, s. 3.

⁵³ Kienan, Brenda, *İşletmeler İçin Çözümler: E-Ticaret*, Arkadaş Yayınları. 2002. s. 4.

- Devletin yapacağı faaliyetler.

2.1.2. Elektronik Ticaretin Araçları

Elektronik ticaretin temel araçları şunlardır:

- Telefon,
- Fax,
- Televizyon (Analog, Dijital, Kablolu),
- Elektronik veri değişimi (Electronic Data Interchange-EDI),
- Internet,

Gerçekte, çoğu zaman E-Ticaret, Internet ve diğer ağlar üzerinden yapılan ticaret olarak algılanmakta ve çalışmalar bu araçlar üzerinde odaklanmaktadır. Elektronik ticaret aslında çok yeni bir kavram değildir. Ancak, Internet ortamının sunduğu, ticari işlemlerde bir veya daha fazla insan tarafından ses, görüntü ve yazılı metinlerin aynı anda inter-aktif bir biçimde iletilmesi, zaman ve mekan sınırının olmayışı ve nispeten daha düşük maliyetlerle çalışılabilmesi gibi olanaklar, elektronik ticaret kavramını Internet'ten sonra hızla gündeme getirmiştir. Internet ortamı iletişim ve ticaretin önündeki engelleri azaltmakta, bu olanaklar Internet'in diğer elektronik ticaret araçlarına göre daha esnek olmasını sağlamaktadır⁵⁴. Bu çerçevede E-Ticaret ile ilgili faaliyetler üç ana başlık altında incelenebilir:

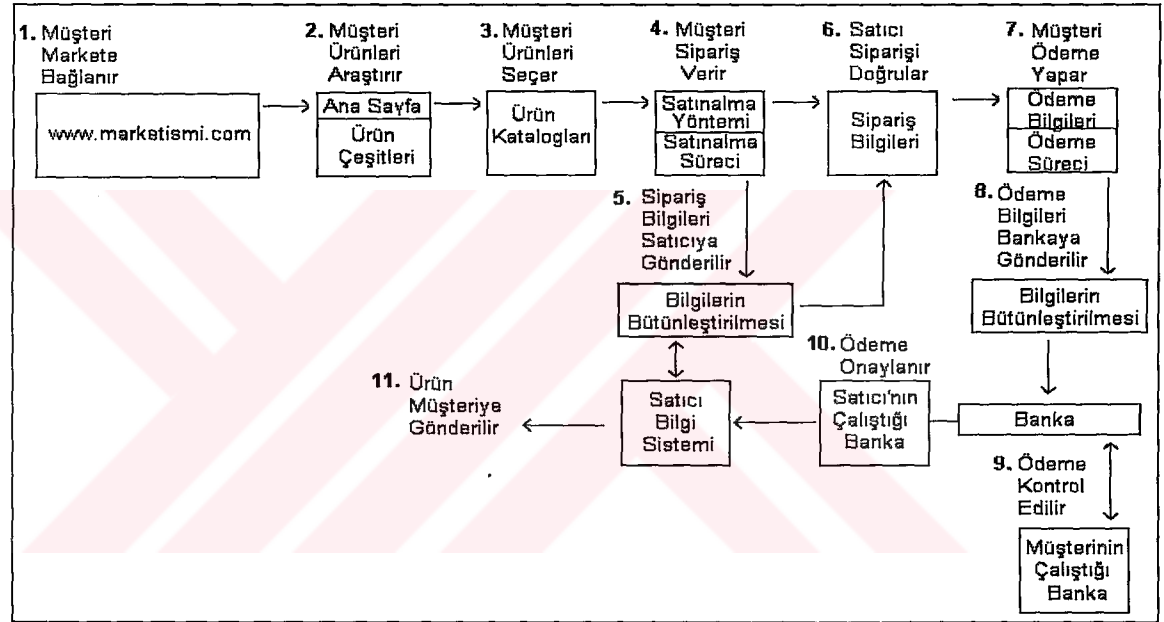
- Mal alım satımı (E-Market)
- Hizmetler (Site aboneliği, Internet bankacılığı, v.b.)
- Ödeme sistemleri

2.1.3 Perakende Mal Alım Satımı ve E-Ticaret

Ürünlerin tanıtılması ve sergilenmesi, müşterilerin bu ürünler hakkında bilgilendirilmesi ve ürünün sipariş edilerek ücretinin ödenmesi işlemlerinin Internet kullanılarak yapılması e-ticaretin birinci ana işlevidir. Elektronik pazarlama ve satış (E-Marketing) olarak adlandırılan bu işlevlerin yerine getirildiği internet siteleri ile bu sitelerin sahibi olan firmalara "E-market" veya "E-dükkan" adı verilir. E-marketler

⁵⁴ Ziya, Rüçhan, *A Study on the Internet as a Commerce Medium*, MSc Thesis 1997, s. 1.

gerçek marketlere benzer şekilde düzenlenmiş web siteleri olarak müşteri karşısına çıkarlar. Web sayfaları e-marketler için hem vitrin hem de tezgah görevi yaparlar. Müşteri bir e-marketin deposuna giderek dolaşma ve ürünlere bakma imkanına sahip olmadığından satılan ürünler müşteriye resim, hareketli resim, grafik ve etiket bilgileri şeklinde tanıtılır. Bir e-market sayfasına giren müşteriye genellikle sanal bir alışveriş sepeti sunulur. Müşteri seçtiği ürünleri bir komut ile bu sanal sepete koyar ve satın alma kararı vermiş ise ödeme işlemlerini yapacağı sayfaya geçer. Ödeme işlemi onaylandıktan sonra ürünler müşteriye gönderilir. Bir e-marketin çalışması grafik olarak Şekil 2.14.'de verilmiştir.



Şekil 2.14. E-Marketin Çalışması

Kaynak: Turban, Efraim. a.g.e. s. 12.

Elektronik ortamda alışveriş yapılan e-marketlerin tümü aynı tarzda çalışmaz. Bu işletmeler gerçek hayatta olduğu gibi yapısal farklılıklar veya farklı uygulamalar nedeni ile çeşitlilik gösterirler. Bu bağlamda e-marketler ve işlevleri değişik kriterlere göre sınıflandırılabilir⁵⁵:

- **Direkt ve Dolaylı Pazarlama:** Direkt pazarlamada üretici firma ürünlerini elektronik ortamda satışa sunar. Dolaylı pazarlama ise satıcının farklı üreticilerin ürünlerini satması durumudur.

⁵⁵ Turban, Efraim. a.g.e., s. 46.

- **Tam E-Market ve Kısmi E-Market:** Yalnız elektronik ortamda faaliyet yapan marketler tam e-marketlerdir. Kısmi e-marketler ise elektronik ortamın yanı sıra fiziksel ortamda satış yapan mağazalara da sahiptirler.
- **Dağıtıcı E-Market ve Komisyoncu E-Market:** Dağıtıcı e-market satacağı ürünleri üreticiden veya toptancıdan satın alır ve kendi karını da ekleyip yeniden fiyatlandırarak elektronik ortamda satışa sunar. Komisyoncu e-market ise müşteri ile satıcı firma arasında komisyon karşılığında aracılık görevi yapar.
- **Elektronik Mağaza (E-Store) ve Elektronik Alışveriş Merkezi (E-Mall):** Elektronik mağaza bir sitede bir tek mağazanın faaliyet yapması olayıdır. Bir sitede birden fazla mağazanın ürünlerine ulaşılabiliriyorsa bu site “Elektronik Alışveriş Merkezi” olarak adlandırılır.
- **Genel E-Market ve Özel E-Market:** Genel e-marketlerde birden fazla çeşit veya marka ürüne ulaşılabilir. Buna karşılık özel e-marketlerde tek ürün veya tek marka satış söz konusudur.
- **Global E-Market ve Yerel E-Market:** Global e-market ülkeler arası geniş bir tüketici kitlesine hizmet verir. Yerel e-market ise yalnızca belirli alandaki (ülke, şehir, v.b.) müşterilere satış yapar.
- **Satış ve Müşteri Hizmetleri:** Bazı e-marketler ürün satışını da elektronik ortamda gerçekleştirirken bazıları satış işlemini fiziksel mağazalarda yapar ancak satış öncesi ve satış sonrası müşteri hizmetlerini elektronik ortamda yürütür.

2.1.4. Hizmet Sektörü ve E-Ticaret

Elektronik ortamda sadece fiziksel ürünler satılmamakta, müşterilere bedel karşılığı bir çok hizmet de sunulabilmektedir. Geleneksel hizmet sektörünün satışlarını internetten yapmalarının yanı sıra internet ve bilgisayar teknolojilerinin kullanımı ile ortaya çıkan ve yalnızca internet üzerinden verilebilen hizmetler de vardır. Örneğin internet bankacılığı fiziksel ortamda sunulan bankacılık hizmetlerinin internet ortamına taşınması ile oluşmuştur. Ancak kullanıcılara abonelik ücreti karşılığı izin verilen sitelerin sunduğu hizmetler yalnızca internet ortamında var olabilen yeni bir sektör

olarak ortaya çıkmıştır. Elektronik ortamda müşterilere sunulan hizmetler ana başlıkları ile şu şekilde sıralanabilir⁵⁶:

- Süreli yayınlar ve elektronik kütüphaneler,
- Komisyonculuk hizmetleri,
- Seyahat ve turizm hizmetleri,
- İş ve işçi bulma hizmetleri,
- Elektronik ortamda eğlence hizmetleri,
- Elektronik ortamda taşınmaz mal (gayrimenkul) satışı,
- Elektronik ortamda menkul kıymet satışı,
- Elektronik ortamda açık arttırma ile satış,
- Elektronik bankacılık ve finansman hizmetleri,
- Elektronik yayın hizmetleri.

2.1.5. E-Ticaretin Yararları

Elektronik ticaretin yararları müşterilere, işletmelere ve topluma sağladığı yararlar olarak üç başlık altında incelenebilir.

2.1.5.1. İşletmelere Sağladığı Yararlar

Gerek mal alım satımında gerekse hizmet sektöründe elektronik ortamın kullanılması işletmelere pek çok avantaj sağlayacaktır. Bu yararların başlıcalarını şu şekilde sıralamak mümkündür:

- Düşük elde etme maliyetleri,
- Düşük dönüşüm/cevaplama zamanları,
- Daha verimli müşteri hizmeti,
- Düşük reklam, satış ve pazarlama maliyetleri,
- Yeni satış olanakları,
- Sınırsız yer ve kitlesel erişim olanağı,

⁵⁶ Turban, Efraim. a.g.e., s. 157.

- Kesintisiz işlem,
- Rekabetin yaygınlaşması,
- Daha az kırtasiye ve bürokrasi,
- Nitelikli ticaret⁵⁷.

2.1.5.2. Müşterilere Sağladığı Yararlar

Elektronik ortamın kullanılması yalnızca işletmelere değil, ticari faaliyetin diğer tarafı olan müşterilere de avantajlar sağlamaktadır. Bu yararların başlıcaları şunlardır:

- Kesintisiz hizmet alma,
- Müşteri ile satıcının aynı coğrafi konumda bulunma zorunluluğunun olmaması,
- Ürün ve çeşit çokluğu, karşılaştırma ve seçim yapma imkanı,
- Açık arttırma ile alışveriş imkanı,
- Hızlı erişim, sipariş ve teslim imkanı.

2.1.5.3. Toplumsal Yararlar

Elektronik ticaretin çevreye ve sosyal hayata yaptığı katkılar toplumsal yararlarını ortaya koymaktadır. Bu yararların bazıları şunlardır:

- Trafik yoğunluğu ve hava kirliliğinin azalmasına katkı,
- Yaşam standardının yükselmesi,
- Fiziksel olarak ulaşılması mümkün olmayan mal ve hizmetlere erişim,
- Kamu hizmetlerinin ulaştırılması.

2.1.6. E-Ticaretin Dezavantajları

E-ticaretin dezavantajları teknik olup olmamalarına göre sınıflandırılabilir.

2.1.6.1. Teknik Dezavantajları

- Güvenlik,
- Bant genişliği,
- Yazılım geliştirme araçlarındaki değişim,

⁵⁷ Turban, Efraim. a.g.e., s. 15.

- Yazılım ve donanımın entegrasyonu zorluğu,
- Özel web sunucuları gereksinimi.

2.1.6.2. Teknik Olmayan Dezavantajları

- Seçim zorluğu,
- Kalite sorunu,
- Karşılıklı güven sorunu,
- Uluslararası siparişlerde ülkelerin vergi uygulamaları,
- Müşteri devamlılığını sağlamak,
- Sunulan tekliflerin sık sık değiştirilmesi ,
- Durumsal olarak farklı fiyat ve teklif verme zorluğu,
- Fiziksel etkileşim kurulmasının gerekebilmesi^{58,59,60}.

2.1.7. E-Ticarete Standartlar, Hukuksal ve Ekonomik Boyut

E-ticaret konusuna tüm iş çevrelerinin dikkat etmesi ve bunu ciddiye almaları gerekir. Çünkü e-iş ve e-ticaret modelleri şirketlerin yeni pazarlara açılmasına yardım etmektedir. Bu yeni pazar, hayatlarının önemli bir kısmında internet kullanan milyonlarca insandan oluşmaktadır ve burada herhangi bir coğrafi sınır da yoktur. Ayrıca, iletişim teknolojilerinin sağladığı hız, ucuzluk ve güven, pazarlama stratejileriyle birleştiğinde, global olarak, işletmelerin karlılığını arttırmaktadır. Ticaret ve iş ilişkilerinde elektronik ortamların ve özellikle internet teknolojilerinin kullanılmasıyla:

- Mevcut iş imkanları büyüyecektir.
- Ürünlerin satışı daha kolaylaşacak ve reklam, ürün tanıtımı, satış öncesi ve sonrası destek ve benzeri kanallar tamamen elektronik ortamda daha efektif kullanılacaktır.

⁵⁸ Turban, Efraim. a.g.e., ss. 16-17

⁵⁹ Office of Fair Trading. *E-Commerce and Its Implications for Competition Policy*. Discussion Paper. 2000 ss. 14-17. <http://www.oft.gov.uk>, S.E.T. 26.11.2003.

⁶⁰ Özen, Üstün, *Firma Müşteri Boyutuyla E-Ticaret: İnternet Kullanıcılarının Elektronik Alışveriş Davranışları*, Aktif Yayınevi, İstanbul, 1998, ss. 14-21.

- Otomatik bilgi dağıtım sistemi yardımıyla, müşterilere ve daha geniş kitlelere kolayca ulaşılacaktır.
- Global olarak iş dünyasıyla olan etkileşim artacaktır.
- İş verimlilik analizleri ve planlamalar daha kolay yapılacaktır,
- Uluslararası pazarlara kolayca ulaşabilme imkanı olacaktır.

E-Ticaret, 2000'li yıllarda, uzmanların tahmininden 2-3 kat daha hızlı büyüyen bir ekonomi mekanizmasıdır. Ticari işletmeler böyle bir ortamda yer almak zorundadırlar. Aksi takdirde pazar payları düşecek ve kimseyle iş yapamaz hale geleceklerdir. Yakın gelecekte, e-dükkanı olmayan, e-posta kullanmayan ticari kuruluşlar işlerini geliştirmede ve yeni iş bağlantıları kurmada çok zorlanacaklardır.

E ticaretin makroekonomik etkileri ise özet olarak şöyle sıralanabilir:

- 1- Fiyatlara Etkisi:** E-ticarete konu olan malların büyük çoğunluğunun ilk üretim maliyetleri yüksek ama yeniden üretim maliyetleri çok azdır. Ancak maliyet azalmasının fiyatlarda düşüş olarak yansması otomatik olarak gerçekleşmez. Bunun için yeterli rekabet olması gereklidir. Elektronik ticaretten kaynaklanan fiyat indirimi, şu aşamada çok az sayıda sektörde gözlenmektedir.
- 2. İstihdam ve İşgücüne Etkisi:** Kısa dönemde firmalar net istihdam artışları da yaşarlar. Orta dönemde öncelikle bazı sektörlerden kaynaklanan istihdam düşüşleri olabilir. Uzun dönemde ise yeni ürünlerin ortaya çıkması, pazar çapının genişlemesi, gelirin artması ve üretkenlik artışının sonucu olarak fiyatların düşmesi ile istihdam artacaktır. Ancak bu durum, ülkelerin elektronik ticaretteki konumuna göre farklılaşabilir.
- 3. Büyüme ve Üretkenlik:** Firmaların iş süreçlerinde bilgisayar kullanma düzeyi arttıkça ve yatırımlar büyüdükçe üretkenlik artışı beklenebilir. Üretkenlik artışı ise ekonomide büyüme olarak kendisini gösterecektir⁶¹.

⁶¹ Ersoy, Zeynep, "Elektronik Ticaretin Ekonomik ve Sosyal Etkileri", *Görüş*, Mart 2000, s. 26.

2.2. Elektronik Ticarete Güvenlik

Bilgi sistemlerinde güvenlik, sistemi oluşturan donanım, yazılım ve iletişim alt yapısının yetkisiz veya kötü maksatlı olarak kullanılmasıyla, saklanan, işlenen veya iletilen bilginin gizlilik, bütünlük ve hazır bulunabilirliğine yönelik tehditlerin belirlenmesi ve engellenmesi faaliyetlerini kapsar.

Bilgi sistemi güvenlik esaslarının metodolojik olarak sistem mühendisliği faaliyetleri esnasında belirlenmesi en etkin yoldur. Güvenlik ile ilgili ihtiyaçlar, analiz, tasarım, gerçekleştirme, test ve bakım aşamaları için eksiksiz ve doğru olarak belirlenebilir ve böylece değişen ihtiyaçlara göre esnek güvenlik sisteminin tesisi sağlanabilir. Güvenlik sistemi, bilgi sisteminin bir alt yapısı olarak gerçekleştirilmelidir. Bu sebeple güvenlik faaliyetlerinin, sistemin donanım, yazılım ve ağ mühendisliği faaliyetleri kapsamında oluşturulması gerekmektedir.

2.2.1. Bilgisayar Ağlarında Güvenlik

Bilgi sistemlerinin güvenliği bilgisayar ağları açısından üç temel kriterle değerlendirilir:

- **Hazır Bulunabilirlik (Availability):** Bilgi sistemlerine istenilen zamanda, istenilen biçimde ulaşılabilmesi ve kullanıma hazır olmasıdır.
- **Gizlilik (Confidentiality):** Veri ve bilgilerin izin verilen zamanlarda ve izin verilen usullerle yalnızca yetkili kişiler, varlıklar ve yöntemler tarafından kullanılabilmesidir.
- **Bütünlük (Integrity):** Veri ile bilginin doğruluğunun ve eksiksizliğinin korunmasıdır.

Hazır bulunabilirlik, gizlilik ve bütünlüğün göreceli önceliği ve önemi bilgi sistemine bağlı olarak değişir. Bir bilgisayar ağında, sistemi oluşturan bütün bileşenlerin problemleri ve zayıf yönleri bulunur. Ağlar, sık olarak, değişik firmaların ürünlerini aynı zamanda desteklemek zorunda kaldıklarından, zarar görebilecek alanların sayısı artabilir. Bunun sebebi, değişik sistemlerin her birinin kendine has işletim sistemlerinin ve uygulama paketlerinin olması ve yine hepsinin kendilerine özgü tasarım hatalarının bulunmasıdır. Ağların amaçları ve kullanımları, kendilerine bağlı olan kullanıcıları ve sistemleri, bağlı olmayanlardan daha değişik davranmaya iter. Bu da kasıtlı veya kaza sonucu zarar görebilecek yeni alanlar açılmasına neden olur. Bir ağın tek veya beraber

olarak zarar görebilir bileşenlerinin ötesinde bilginin izleyebileceği değişik yollar (bağlantılardan ağ geçit konfigürasyonları vasıtasıyla) da ek zayıf tarafları oluşturur.

Ağlar arasındaki güvenlik duvarları (Firewall), irtibat kurulan değişik noktalardan saptanması daha zor ve daha tehlikeli hale gelebilecek tehditlerin eklenmesine, yani risklerin artmasına sebep olacak fiziksel bağlantılardır. Ayrık ağlar kendi içlerinde güvenli olabilirler, ancak bağlandıklarında birbirlerinin güvenliklerini tehlikeye sokarlar.

Genel olarak bir ağı oluşturan bütün bileşenler zarar görme noktalarıdır. Bu noktaların en önemlileri şu şekilde sıralanabilir:

- Yönlendiriciler (Routers),
- Sunucular (Servers),
- Çalışma İstasyonları (Workstations),
- Bağlantı noktaları (Connection Points),
- Kablolar (Cabling).

Güvenli bir ağ ortamı için doğru bir şekilde planlanması, geliştirilmesi ve uygulanması gereken temel politikalar şunlardır:

- Sunucu erişimi kontrol politikası,
- Şifreleme (Cryptography) politikası,
- Sunucuya girişleri (logging) izleme politikası,
- Disk kullanım politikası,
- Yedekleme politikası,
- Uzaktan erişim politikası,
- Fiziksel güvenlik politikası,
- Hassas erişim politikası,
- Ticari ürün kullanım politikası,
- Virüslerle mücadele politikası,
- Kaçak kullanıcılarla mücadele politikası.

2.2.1.1 Güvenli Bilgisayar Sistem Değerlendirme Kriterleri (TCSEC)

Dünya genelinde kabul gören bilgi işlem güvenliği temel kavramları A.B.D.'de yayımlanmış olan the Government's Trusted Computer System Evaluation Criteria TCSEC-Orange Book'da ortaya konulmuştur. Bu belge bir sistemin "güvenli" olarak onaylanabilmesi için sahip olması gereken özellikleri belirler.

TCSEC geliştirilirken ortaya konan amaçlar şunlardır:

- Ölçme:** Kullanıcılara güvenli bilgiyi işleyebilecekleri sistemlerin güvenilirliğini ölçebilecek bir yöntem sağlamak.
- Yardım:** Üreticilere ticari güvenli ürünlerinde duyarlı bilgiyi işlemek için sağlamaları gereken koşulları sunmak.
- Tedarik:** Alıcıların sistem tedarik ederken gereksinim özelliklerini ifade edebilecekleri bir tedarik standardı sağlamak.

2.2.1.2. TCSEC Değerlendirme Sınıfları

TCSEC kriterleri, A, B, C ve D olmak üzere 4 temel kısma, bunlardan C ve B sınıfları daha alt sınıflara ayrılmıştır:

- Kısım D-Minimum Koruma.
- Kısım C-Seçici Koruma (Discretionary Protection).
 - Sınıf C1-Seçici Güvenlik Koruması.
 - Sınıf C2 - Kontrollü Erişim Koruması.
- Kısım B - Zorunlu Koruma (Mandatory Protection).
 - Sınıf B1-Etiketli Güvenlik Koruması.
 - Sınıf B2 - Yapısal Koruma (Structured Protection).
 - Sınıf B3 - Güvenlik Tanım Kümeleri (Security Domains).
- Kısım A - Kanıtlanmış Koruma (Verified Protection).
 - Sınıf A1-Kanıtlanmış Tasarım.

2.2.1.4. Bilgi Teknolojisi Güvenliği Değerlendirme Kriterleri (ITSEC)

ABD’de geliştirilen TCSEC (Information Technology Security Evaluation Criteria) yalnız ABD ürünlerinin değerlendirmesine açık olması dolayısıyla Avrupa’nın bilgi teknolojisi alanındaki söz sahibi ülkeleri İngiltere, Almanya, Fransa ve Hollanda TCSEC benzeri bir standart geliştirmişlerdir. Bu kriterlerin altı temel amacı vardır:

- Kabul edilmiş terminoloji kümesinin yayınlanması,
- Kriterlerin ticari, hükümet ve savunma sektörlerinin tümüne uygun olması,
- Hem ürünlerin hem de sistemlerin kapsanması,
- Kriterlerin her sınıftaki güvenlik politikasını kapsamaması,
- Gizlilik, bütünlük ve hazır bulunurluğun tümünün kapsanması,
- ABD TCSEC ile uyumluluğunun sağlanması⁶².

2.2.1.5. Veri İletişiminde Güvenlik

Bir sistem birden fazla terminalden oluşuyorsa ve bu terminaller arasında direkt kablo ile veya modem, uydu bağlantısı, v.b. yollarla erişim sağlanabiliyorsa, veri iletişiminin güvenli olarak yapılabilmesi, tüm sistemin güvenliği açısından önemli bir problem olacaktır. Veri iletişimde güvenlik, özellikle dışarıdan erişimin tam olarak kontrol edilemediği açık ağ ortamlarında askeri ve sivil istihbarat bilgileri ile e-ticarete para transferi ve ödeme bilgileri gibi değerli verilerin nakledilmesinde çok önemli bir önceliğe sahiptir. Veri iletişimi güvenliğinin amaçları genel olarak şu şekilde sıralanabilir:

- Gizli bir mesajın yetkisiz kişilerce okunup yayımlanarak ifşa edilmesinin önlenmesi,
- Gönderilen mesajın yetkisiz kişilerce değiştirilmesi, bir kısmının veya tamamının silinmesi gibi durumların önlenmesi, önlenemeyen tahriplerin fark edilmesi,
- Veri trafiğini engelleyici saldırıların önlenmesi,
- Sahte veya kötü niyetli kurumların fark edilmesi⁶³.

62 NITSEC, “NATO Information Technology Security Evaluation Criteria”, *NITSEC Publications AC/35*, 1996.

63 Wright, Marie A., “Encryption Alternatives for Network Security”, *Computer Fraud & Security*, Mart 1996, ss. 15-17.

Veri iletişimi güvenliğini oluşturan unsurlar dokuz ana başlık altında sıralanabilir:

- Kimlik tesbiti ve doğrulanması,
- Yetkisiz erişim (Parola) kontrolü,
- Yetki hesaplarının denetlenmesi,
- Şifreleme,
- Nesnelerin bütünlüğünün korunması,
- Sistem bütünlüğü,
- Sistem mimarisi,
- Etiketler
- Zorunlu erişim kontrolü⁶⁴.

2.2.2. Elektronik Ticaret'te Ödeme Araçları

İnternet ortamında yapılan alışverişlerde genelde ödemelerin de elektronik ortamda yapılması gerekir. Elektronik ortamda ödeme fiziksel ödeme araçlarının sayısal benzerleri kullanılarak gerçekleştirilir. Elektronik ödeme genel olarak ikiye ayrılır:

- Geleneksel ödeme araçlarının (para, çek v.b.) elektronik ortamda uzaktan kontrolü,
- Elektronik ödeme araçlarının (dijital para v.b.) kullanılması⁶⁵.

Ödeme olayı üç kişi (müşteri, satıcı, banka) arasında gerçekleşir. Elektronik ödemenin bu üç taraf arasındaki seyri iki farklı şekilde meydana gelebilir:

- Müşteri bankadan elektronik ortamda geçerli bir ödeme aracı (elektronik para, çek v.b.) alır ve bunu satıcıya verir.
- Müşteri satıcı ile anlaştıktan sonra bankaya ödeme emri gönderir. Banka satıcı ile veya satıcının bankası ile iletişime geçerek ödeme işlemini gerçekleştirir⁶⁶.

64 Guttman, Barbara, "Computer Security Considerations in Federal Procurements: A Guide for Procurement Initiators, Contracting Officers and Computer Security Officials", *NIST Special Publication 800-4*, Mart 1992, s. 63.

65 Schudelar, A.A.P., "Electronic Payments", *Computer Law & Security Report*, 2001, Cilt 17, Sayı 2, ss. 105-109.

66 Varadharajan, Vijay, Khanh Quoc Nguyen, Yi Mu, "On the design of efficient RSA-based on-line electronic cash schemes", *Theoretical Computer Science*, 1999, Sayı 226, ss. 173-184.

2.2.2.1. Kredi Kartları ve Akıllı Kartlar (Smart Card)

Elektronik ödeme araçları içerisinde en yaygın kullanılanı kredi kartı ile ödemedir. Ancak güvenlik sorunlarının insanları kredi kartı numarasını Internet'e vermekten alıkoyması bu ödeme şeklinin de ek prosedürlerle fiziksel kullanımından farklılaşmasına neden olmuştur. Kredi kartı ile alışveriş, internet ortamındaki ödeme sistemleri içerisinde üzerinde en çok çalışılan sistemdir. Fiziksel kullanımında kredi kartını kullanan kişinin aynı zamanda kartın sahibi olup olmadığının ve kredi kartının yapılan harcamayı karşılayacak bakiye veya limite sahip olup olmadığının belirlenmesi gerekir. Aynı şekilde internet ortamında da kredi kartı numarasını veren kişi ve kredi kartı hakkında doğru bilgiye ulaşmak için çeşitli uygulamalar geliştirilmiştir.

Akıllı kartlar fiziksel kullanımda güvenliği artırılmış kredi kartlarıdır. Güvenliği arttıran unsur ise kartın üzerine yerleştirilen ve çip (chip) denen küçük bilgi depolama birimleridir. Bu depolama birimlerinde kullanıcıya ait kimlik bilgileri ile kriptografik bilgiler saklanır⁶⁷. Akıllı kartların internette kullanılması için bilgisayara kartın üzerindeki çipi okuyacak bir donanım eklenmesi gerekmektedir. Bu donanım kullanılmadan akıllı kart ve sıradan kredi kartı aynı işleve sahip olacaktır.

Akıllı kart teknolojisi, diğer güvenlik teknolojilerine göre daha ucuz olması, güvenlik gerektiren bilgilerin taşınabilir olması ve bu bilgilerin istendiğinde kolayca kullanımını sağlaması gibi avantajları nedeniyle hızla yayılmaktadır⁶⁸.

Kredi kartı veya akıllı kartlarla yapılan ödemeler üç farklı sistemle gerçekleştirilebilir:

- Kredi kartı detaylarının açık olarak kullanılması,
- Kredi kartı detaylarının şifrelenmiş olarak kullanılması,
- Ödeme için bir onay kurumu veya üçüncü tarafın kullanılması.

2.2.2.2. Dijital (Sayısal) Çek ve Dijital Senet

Sayısal çekler bir onay kurumu tarafından sayısal olarak imzalanmış ve ödeme aracı olarak kullanılan özel yazılımlardır. Söz konusu onay kurumlarına "Güvenilir

⁶⁷ Borst Johan, Bart Preneel, Vincent Rijmen, "Cryptography on Smart Cards", *Computer Networks*, 2001, Sayı 36, ss. 423-435.

⁶⁸ Stirland, Mark, "Smartcards in Secure Electronic Commerce", *Information Security Technical Report*, 1998, Sayı 3, No 2, ss. 41-54.

Üçüncü Taraf" (Trusted Third Party, TTP) adı verilir. Güvenilir üçüncü taraf için iki farklı yaklaşım mevcuttur. Kurumsal yaklaşıma göre üçüncü taraf diğer taraflarca kabul edilmiş yetkilere sahip bir onay kurumu olabilir. Kurumsal olmayan yaklaşım ise kişilerin birbirine kefil oldukları bir kefiller zinciri kurulmasıdır⁶⁹. Uygulamada en çok rastlanan durum ise bankaların bu görevi üstlenmesidir. Bankalar diğer kurumlardan daha önce, güçlü ve yaygın bir sistem kurmuş oldukları için bu konuda en elverişli imkanlara da bankalar sahiptir⁷⁰. Güvenilir üçüncü taraf konusunda son yıllarda özellikle ABD ve Avrupa ülkelerinde önemli hukuksal çalışmalar yapılmış, üçüncü taraf olabilecek kuruluşlar üzerinde özel izin ve standartlara uygunluk gibi denetimler getirilmiştir. Bu konuda en ileri ülkeler ABD ve İngiltere'dir^{71,72}.

Dijital çek ve senetler gerçek yaşamda kullanılan çek ve senetlerle aynı modeli ve mantığı kullanırlar. Dijital ortamda çeklerin onaylanması veya ciro edilmesi dijital imza kullanılarak gerçekleştirilir ve ödeme yapan kişinin, ödeme yapan bankanın ve banka hesabının tanımlanması ve yetkilendirilmesi için dijital sertifikalar kullanılır⁷³.

2.2.2.3. Dijital Para

E-para, kişide bulunan elektronik bir araca yüklenmiş mali değer veya kişisel fonu ifade eder. Elektronik araca yüklenmiş olan bu değer kişi aracı kullandıkça azalır ve yüklenmiş olan değer bitimi sonucu tekrar değer yüklenilmesi gerekir. Dijital paranın geçerli ve güvenilir olması için şu niteliklere sahip olması gerekir⁷⁴:

- Parasal değer ifade etmesi,
- Değiş tokuş yapılabilmesi,
- Geri kazanılabilmesi,
- Güvenli olması.

⁶⁹ ETKK, *Türkiye Elektronik Ticaret Koordinasyon Kurulu Elektronik Ticaret Raporu*, 1998, s. 9.

⁷⁰ Rove Heather, "Securing Payments Through Effective Authentication: Evaluating Trusted Third Party Proposals for a Thrust Hierarchy in the UK", *Computer Law & Security Report*, 1998, Cilt 14, Sayı 3, ss. 151-158.

⁷¹ Bigelow, Robert, "Encryption Controls are US Government Priority", *Information Security Thecnical Report*, 1997, Cilt 2, Sayı 1, ss. 62-65.

⁷² Hickson, Nigel, "Encryption Policy: A UK Perspective", *Computers & Security*, 1997, Sayı 16, ss. 583-589.

⁷³ Kalakota, Ravi. a.g.e. s. 164.

⁷⁴ Kalakota, Ravi. a.g.e. s. 160.

Dijital paranın çalışma mantığı ile bir şirketin verdiği değere karşılık olarak yapılacak ödemelerin gerçekleşmesi için tüketiciye verdiği telefon kartı ve benzeri araçlar arasında benzerlik görülse de dijital paranın amacı bu tür kartlar gibi tek işlemle ilgili bir ödeme değil, her türlü ödemenin yapılabilmesidir. Dijital paranın en önemli özelliği küçük çaplı ve hızlı ödeme imkanı da sağlamasıdır.

Dijital paranın gerçek paradan bir farkı da yapılacak ödemeyi ileri bir tarihe atma imkanı sunmasıdır. Bu özellik çeklere benzese de aradaki fark çekin vadesi gelince paraya çevrilmesi, dijital paranın ise vadesi geldiğinde cari olmasıdır. Bu tür dijital ödeme aracına tarih eklenebilir (Date Attachable) dijital para adı verilir⁷⁵.

2.2.2.4. Diğer Ödeme Araçları

-Internet üzerinde yapılan harcamaların Internet Servis Sağlayıcıların (ISS) faturalarına borç kaydedilmesi,

-Tüketicilerin internet üzerinden satın aldıkları ürün ve hizmetlerin bedellerinin telefon faturalarına borç kaydedilmesi,

-E-Ticarete gerçekleşen ödemelerin üçüncü bir kuruluştaki toplanıp ilgili taraflara dağıtılması.

2.2.3. Elektronik Ödeme Sistemlerinde Güvenlik ve Şifreleme

Elektronik ticaret güvenlik açısından çok geniş olarak incelenmesi gereken bir konudur. Ancak bu çalışmanın konusu gereği şifreleme üzerinde yoğunlaşılacak, diğer uygulamalar yalnızca isim olarak belirtilecektir. İlk adımda tüm e-ticaret güvenlik uygulamaları iki ana başlık altında toplanabilir.

Sistem Güvenliği: Sistemi oluşturan donanım ve yazılım birimlerinin fiziksel olarak veya kullanım ve lisans hakları açısından dış etkilere karşı korunması ve sistemin sürekli ve etkin olarak çalışması için gerekli önlem ve uygulamaları kapsar.

Bilgi Güvenliği: Sistemde kullanılan, saklanan, iletilen bilgilerin bozulması, silinmesi istenmeyen erişimler, kopyalamalar, gizlilik ihlalleri, gibi hasarlara uğramasını engellemek için gerekli önlem ve uygulamalar bilgi güvenliği başlığı altında incelenir.

⁷⁵ Fan, C. W Chen, Y. Yeh, "Date Attachable Electronic Cash", *Computer Communications*, 2000, Sayı 23, ss. 425-428.

Bu iki ana başlık incelendiğinde bilgi güvenliğinin şifrelemenin kullanılması konusunda daha ön planda olduğu görülecektir. E-Ticarette bilgi güvenliği ise özellikle ödeme sistemlerinde ön plana çıkmaktadır. E-Ticarette bu anlamda güvenlik sağlanması için dört temel şartın yerine getirilmesi gerekir:

-Gizlilik (Confidentiality): İşlem bilgilerinin üçüncü partiler tarafından değil sadece doğru kişi veya kuruluş tarafından görülebilmesi.

-Bilgi Bütünlüğü (Integrity): Bilginin kaynağında üretildiği şekliyle, değişmeden alıcıya ulaştırılması.

-Kimliğin Kanıtlanması (Authentication): İşlemin geçerliliğinin ve tarafların kimliklerinin doğruluğunun kanıtlanması.

-İnkâr Edememe (Non-repudiation): Alıcının veya satıcının yaptığı sipariş, ödeme, vb. işlemleri sonradan inkâr edememesi^{76,77}.

Elektronik ödeme sistemleri farklı kriterlerle de değerlendirilebilir. Bu kriterlerden ilki ödemenin dijital ortamda yapılmasının güvenlik dışında getireceği fayda veya maliyetlerdir. Örneğin bir ödeme fiziksel araçlarla yapıldığında 1.000.000 TL maliyete sahipse ve eğer dijital ödeme kullanıldığında bu maliyet on katına çıkıyorsa, dijital ödeme sistemleri her ne kadar zaman kaybını minimuma indirmek gibi önemli avantajlar getirse de 5.000.000 TL tutarında bir ödeme için 10.000.000 TL masrafa katlanmanın müşteri için ekonomik olmayacağı açıktır. İkinci kriter güvenlik ihtiyacı ile güvenlik önlemlerinin kullanıcıların hareket alanında meydana getirdiği daralma arasındaki dengedir. Çok sayıda ve uzun süren prosedürleri takip etmek, güvenlik noktalarında karmaşık sorgulamalardan geçmek gibi zorunluluklar kullanıcıyı elektronik ortamda para transferinden caydıracaktır. Üçüncü önemli kriter güvenilirliktir. Oluşturulacak sistemin güvenliği sağlamanın yanında kullanıcıların güvenini de kazanması gerekmektedir. Bunun için kullanıcının sistem hakkında doğru ve açık olarak bilgilendirilmesi ve ikna edilmesi gerekmektedir.

Globe-Online(R) isimli bir proje çerçevesinde Avrupa'da yapılan anket çalışmaları sonucuna göre elektronik ortamda mal veya hizmet satan tüccarlar ile mal ve

⁷⁶ www.ykb.com, S.E.T. 07.02.2003.

⁷⁷ Koops, Bert-Jaap, "Crypto Regulation in Europe: Some Key Trends and Issues", *Computer Networks and ISDN Systems*, 1997, Sayı 29, ss. 1823-1831.

hizmet alımı yapan müşterilerin güvenlik konusundaki ihtiyaçları ve talepleri ayrı ayrı belirlenmeye çalışılmıştır. Bu çalışmaya göre⁷⁸:

Tüccarların Talepleri:

- En azından çekler ve kredi kartları gibi geleneksel ödeme araçlarında olduğu kadar bir ödeme garantisi,
- Müşterilerin yaptıkları işlemi daha sonra reddetmemelerinin sağlanması,
- Hem çok küçük hem de çok büyük miktarlarda ürün satışı yapmaya uygun olması,
- Birden fazla ödeme aracı kullanılmasına imkan vermesi ve gerektiğinde vergi ve masrafların kolayca hesaplanabilmesi,
- Hesapların denetlenebilmesi,
- Tüm işlemlerin güvenli olarak kaydedilmesi,
- Coğrafi konum veya müşteri profillerine göre farklı fiyatların uygulanabilmesi,
- Kolay anlaşılır ve kullanılabilir istatistiklerin doğru olarak hesaplanması ve gerektiğinde ulaşılabilmesi.

Müşterilerin Talepleri:

- Tüccarın kimliğinin garanti edilmesi,
- Yapılan ödemenin kaydedilmesi ve inkar edilememesi,
- Hem çok küçük hem de çok büyük miktarlarda ödeme yapmaya uygun olması,
- Gerçek kimliğin kabul edilebilir bir düzeyde saklanma imkanı,
- Birden çok ve opsiyonel gizlilik seçeneklerinin olması,
- Global alışveriş ama yerel ödeme imkanları,
- Alışveriş kartı, banka kartı, kredi kartı v.b. ödeme araçlarının ayrı ayrı veya birlikte kullanılabilme imkanı,
- Hesaplarını kontrol edebilme yetkisi,
- Bir hesaba bağlı alt hesaplar oluşturulabilmesi.

⁷⁸ Pays, Poul-Andree, "Fabrice de Comarmond. An intermediation And Payment System Technology", *Computer Networks and ISDN Systems*, 1996, Sayı 28, ss. 1197-1206.

Elektronik ödemede kullanılan güvenlik araçlarını şifreleme kullanılıp kullanılmamasına göre iki guruba ayrılabilir:

- Şifreleme kullanılmayanlar (Firewall, Parola Koruması, v.b.)
- Şifreleme kullanılanlar (Dijital İmza, Dijital Sertifika, v.b.)

Şifreleme kullanılan araçlar şu şekilde sıralanabilir:

- Şifreleme Algoritmaları
- Verilerin Özetlenmesi (Hashing) ve Dijital İmza
- Anahtar Kontrolü (Key Management)
- Dijital Sertifikalar
- Dijital Çekler ve Ödeme Emirleri

2.2.3.1. Şifreleme Algoritmaları

Şifreleme konusu birinci bölümde ayrıntılı olarak incelendiğinden burada sadece şifreleme algoritmalarının standardizasyonu üzerinde durulacaktır. Bir güvenlik sistemi oluşturulurken kullanılan şifreleme algoritmalarının tanımlanması ve yeterince güvenli olup olmadığının ölçülmesi gerekir. Ancak algoritmaların güvenilirliğini sistemi satın alan veya kullanan her kişinin ayrı ayrı test etmesi mümkün değildir. Şifreleme algoritmasının belirli standartlara uygunluğunun standartları üreten kuruluş tarafından onaylanması bu problemin çözümü için en etkili ve kısa yol olacaktır.

Şifreleme algoritmaları için standart geliştirme çalışmaları ilk olarak yetmişli yılların başında Amerika Ulusal Standartlar Enstitüsü (ANSI) ve Amerikan hükümetinin ortak çalışmaları ile başlamıştır. 1980 yılında bir uluslararası standart kuruluşu olan ISO, ISO TC97 adı altında bir çalışma gurubu kurmuştur. 1984-1985 yıllarında şifreleme algoritmalarının standardizasyonu için ISO TC97/SC20 alt çalışma grubu tarafından ve “Data Encryption Standart –DES” isimli bir proje geliştirilmiştir. 1990 yılında ise veri güvenliği standartları oluşturmak için JTC1 isimli yeni bir çalışma grubu kurulmuş ve şifreleme algoritmaları JTC1/SC27 isimli alt komitenin çalışma alanına dahil edilmiştir⁷⁹. ISO, ayrıca, bir şifreleme algoritmasının tescili için gerekli prosedürü

⁷⁹ Beckett, Brian, *Introduction to Cryptography and PC Security*, McGraw-Hill Int., 1997, s. 242.

ISO/IEC 9979 standardı ile belirlemiştir. Bu standarda göre tescilli bir şifreleme algoritması aşağıdaki öğelerden oluşmalıdır:

- Algoritmayı onaylayan kurum tarafından tanımlama ve sınıflandırma amaçlı olarak verilen kayıt ismi,
- Algoritmanın sahibi tarafından verilen ismi.
- Algoritmanın uygulama alanının ve uygulanabilirliğinin (Gizlilik, veri bütünlüğü v.b.) tanımlanması,
- Parametreler: Şifrelenecek metnin (input size) ve şifreli metnin (output size) büyüklüğü, anahtar uzunluğu, v.b.
- Onaylayan kuruluşun adı,
- Kayıt ve değiştirme tarihleri,
- Varsa ihracat lisansı ve patent şartları,
- Algoritmanın tanımlanması, kullanma şekli ve diğer teknik detaylar (opsiyonel).

2.2.3.2. Dijital (Sayısal) İmza

Mesajın sayısal olarak imzalanmasının temel olarak iki amacı vardır. Birinci amaç veri bütünlüğünün (Integrity) korunmasıdır. Bunun için gönderilen mesaj bir fonksiyon kullanılarak özetlenir. Bu özetleme işlemine “Hashing” denir. Mesajı alan taraf aynı fonksiyonu (Hashing Algorithm) kullanarak mesajı yeniden özetler ve kendisine gelen özetle (Message Digest) karşılaştırır. İki özet birbirinin aynı ise mesajın herhangi bir kayba veya değişikliğe uğramadığı anlaşılır. İkinci amaç ise mesajı gönderen tarafın kimliğinin kanıtlanmasıdır (Authentication). Kimlik kanıtlama bir mesajın yetkili bir kişi tarafından gönderilip gönderilmediği, göndericinin kimlik bilgilerinin doğru olup olmadığı veya mesajın söz konusu kişi namına düzenlenip düzenlenmediği konularını kapsar⁸⁰. Bu amaç için açık anahtarlı şifreleme kullanılır. Mesaj özeti alıcının kapalı anahtarına karşılık gelen bir açık anahtarla şifrelenir. Alıcı mesajı ve imzalanmış mesaj özetini aldığı anda mesajı yeniden özetleyip imzalı mesaj özetini kendi kapalı anahtarı ile çözümledikten sonra elde ettiği iki sonucu karşılaştırır. Böylece hem veri bütünlüğünü, hem de göndericinin kimliğini denetleme imkanı elde

⁸⁰ Pounder, Chris, “Further Developments in the Field of Encryption and Digital Signatures”, *Computers & Security*, 1998, Sayı 17, ss. 308-312.

eder^{81,82}. Göndericinin mesajı sayısal olarak imzalaması ayrıca mesajı gönderdiğini sonradan inkar etmesini de engelleyecek bir araçtır.

Sayısal imza ve özetleme konusunda belirlenen standartlar (Digital Signature Standart-DSS) ve (Secure Hash Standart-SHS) isimleri ile bilinir⁸³. Bu standartlara uygunluğu tescil edilmiş ilk algoritmalar ise SHA-1 ve DSA'dır. Bu standartları da kapsayan ISO/IEC 9796 ismi verilen JTC1 standardında mesajın özetlenmesi ve özetin şifrlenmesi metodunun yanı sıra çok kısa mesajların özetlenmeden imzalanması metodu da öngörülmüştür^{84,85}.

2.2.3.3. Anahtar Kontrolü (Key Management)

Bir kriptografik sistemin güvenliği kullanılan anahtarların üçüncü şahıslara karşı gizliliğinin korunmasına bağlıdır. Aynı anahtarın uzun süre kullanılması da güvenlik açısından sakıncalar doğurabilir. Bu nedenle anahtar kontrolü yalnızca bir anahtarın gizliliğini korumakla sınırlı değildir. Anahtar kontrolü anahtarların üretilmesini, dağıtımını, kullanılmasını ve imha edilmesini kontrol eden bir süreç olarak tanımlamak daha uygundur⁸⁶.

Anahtar kontrolü için "Key Management Using ANSI X9.17" isimli bir standart belirlenmiş ve 1992'de bir yayınlı (FIPS PUB 171) duyurulmuştur. Bu yayına göre anahtar kontrolü, "Kriptografik sistemlerde anahtarların tanımlanması ve sürdürülmesi için gerekli prosedürlerin yönetimini sağlar. Bir anahtar kontrolü metodunda bulunması gereken minimum özellikler şunlardır:

- Anahtarların kullanılma sürecinde yetkilendirilmemiş taraflarca elde edilmesini, değiştirilmesini veya açıklanmasını önlenmek.
- Taraflar arasında güvenli iletişimin uygulanabilirliğini sağlayacak anahtar dağıtımını yapmak.

⁸¹ <http://csrc.nist.gov> S.E.T. 07.02.2003.

⁸² Mitchell, Chris, "Authentication Using Cryptography", *Information Security Technical Report*, 1997, Cilt 2, Sayı 2, ss. 25-32.

⁸³ FIPS Pub. 180-1, "Announcing the Standard for SECURE HASH STANDARD", *Federal Information Processing Standards Publication*, 17 Nisan 1995, s. 1.

⁸⁴ Beckett, Brian. a.g.e., s. 247.

⁸⁵ Barcelo, Julia, "Towards a European Framework For Digital Signatures And Encryption", *Computer Law & Security Report*, 1998, Sayı 14, No 2, ss. 79-86.

⁸⁶ NIST Special Publications. SP800-4. s. 70.

- Üretilmesi, saklanması, kaydedilmesi, kullanılması ve imha edilmesi süreçlerinden oluşan yaşam süresi boyunca anahtarın doğruluğunu ve bütünlüğünü korumak.
- Anahtar kontrolü sürecinde meydana gelebilecek bir başarısızlık veya anahtarın doğruluğunun şüpheli hale gelmesi gibi durumları önlemek veya zararlarının önüne geçmek”⁸⁷.

2.2.3.4. Dijital Sertifikalar

Ağ üzerinde kullanıcı veya sunucu (server) bilgisayarların kimliğini tanımlamak ve kanıtlamak için kullanılan ve sertifika otoritesi adı verilen kurumlar tarafından üretilen özel yazılımlardır⁸⁸. Dijital sertifikalar gerçek hayattaki kimlik kartlarının elektronik ortamdaki benzerleridir. Dijital sertifikanın elektronik olarak gösterilmesiyle sertifika sahibi kimliğini ve erişim iznini kanıtlayabilir. Dijital sertifikalarda sertifika sahibinin kimliğini kanıtlamak için açık anahtarlı şifreleme, yayımcının kimliği ile sertifikanın geçerliliğini kanıtlamak için ise sayısal imza kullanılır. Yayımcı kuruluşun da kendi dijital sertifikası vardır ve bu sertifikaya “Kök Sertifika” adı verilir⁸⁹. Dijital sertifikalarda sertifika sahibinin açık anahtarı, DN numarası (Distinguished Number), Sertifikanın geçerlilik süresi, yayımcı kuruluşun (CA, Certificate Authority) DN numarası ve yayımcı kuruluşun dijital imzası gibi bilgiler bulunur⁹⁰. Böylece, kişi ve kuruluşların ticari ve kişisel işlemlerini iletişim ağları üzerinde güvenli bir şekilde gerçekleştirmeleri sağlanır.

2.2.4. Şifreleme Esaslı Güvenlik Sistemleri

Şifreleme algoritmalarının asıl öge olarak kullanıldığı bir çok güvenlik sistemi vardır. Bu sistemler içerisinde en çok kullanım alanı bulan SSL sistemidir. Bu bölümde, bir bilgi transferi güvenlik sistemi olan SSL’den başka, elektronik ödeme güvenlik sistemi olarak tasarlanmış olan SET’de incelenecektir.

2.2.4.1. SSL (Secure Socket Layer)

SSL, web üzerindeki iletişim güvenliği için kullanılan ve bilgi transferinin gizliliğini ve bütünlüğünü sağlayan güvenlik protokolüdür. Web siteleri ve tarayıcılar

⁸⁷ FIPS Pub. 171, “Specifications for Key Management Using ANSI X9 17”, *Federal Information Processing Standard Publication*, 27 Nisan 1992.

⁸⁸ Parmar, S.K., “An Introduction To Security”, *RCMP Publication*, s. 280.

⁸⁹ Özen, Üstün. a.g.e., s. 99.

⁹⁰ Senger, Matt, *Providing Security through Secure Socket Layer*, www.mrs.umn.edu, S.E.T. 10. 03.2003.

tarafından yaygın olarak desteklenen SSL, müşteri ve mağaza arasındaki mesajların şifrelenmesini ve sadece doğru adreste deşifre edilmesini sağlar⁹¹. SSL, web sunucularına bir modül olarak yüklenir ve böylece web sunucuları güvenli erişime uygun hale gelir⁹².

Netscape Communications Corporation tarafından geliştirilen SSL teknolojisinde hem istemci hem de sunucu bilgisayarda bir doğrulama (authentication, iki bilgisayarın karşılıklı olarak birbirini tanıması) mekanizması kullanılır.

Bilgisayarların birbirlerini tanıma işlemi, açık anahtarlı (public key) şifreleme ile sağlanır ve web sunucusunu tanımak için, dijital olarak imzalanan sertifikalar kullanır. İstemci bilgisayar, SSL destekleyen bir sunucuya bağlandığı anda, (bu, https:// ile başlayan URL satırları ile gerçekleşir) doğrulama işlemi başlar. İstemci, kendi açık anahtarını sunucuya gönderir. Sunucu ise, bu anahtarı kullanarak şifrelediği bir mesajı istemciye geri gönderir. Bir sonraki adımda istemci sadece kendinde olan kapalı (private) anahtarı kullanarak gelen şifreli mesajı çözer ve sunucuya geri gönderir. Mesajı alan sunucu ise, bunu kendisinin gönderdiği orijinal mesaj ile karşılaştırır ve eğer iki mesaj "aynı" ise "doğrulama" işlemi başarıyla tamamlanmıştır ve sunucu bu noktadan itibaren "doğru bilgisayarla/kişiyle" iletişimde olduğunu anlar. Daha sonra sunucu istemciye o an gerçekleşen web oturumunda kullanılacak tüm önemli anahtarları gönderir ve güvenli iletişim başlar⁹³. SSL protokolünün daha kapsamlı olarak anlaşılması için SSL ile yapılan ve "El Sıkışma" olarak adlandırılan güvenlik kontrolü adım adım şu şekilde açıklanabilir⁹⁴:

-Müşteri SSL versiyon numarasını, şifre ayarlarını, rasgele üretilmiş bir kısım verileri ve iki bilgisayarın iletişimi için gerekli bazı bilgileri ana bilgisayara (server) gönderir.

-Ana bilgisayar bu bilgilere karşılık kendisine ait bilgileri ve müşteriyi doğrulayabilmek için bu bilgilere ek olarak kendi sertifikasını müşteriye gönderir.

-Müşteri sertifika bilgilerini kullanarak ana bilgisayarı ve yetkilerini doğrular. Sertifikada yer alan bilgiler şunlardır:

⁹¹ www.ykb.com.

⁹² www.eng.bahcesehir.edu.tr/css/bolum11, S.E.T. 12. 03.2003.

⁹³ Birch, Dave, "The Certificate Business Public Key Infrastructure Will Be Big Business", *Computer Law & Security Report*, 1997, Sayı 13, No 6, ss. 454-456.

⁹⁴ Senger, Matt. a.g.e.

- Ana bilgisayarın açık anahtarı,
- Sertifika seri numarası,
- Sertifikanın geçerlilik süresi,
- Ana bilgisayarın DN numarası (Distinguished Number),
- Yayımcı kuruluşun (CA, Certificate Authority) DN numarası,
- Yayımcı kuruluşun dijital imzası.

-Müşteri sertifika bilgilerinde ek olarak ana bilgisayarın alan adı (Domain Name) bilgilerini de kendi elindeki bilgilerle karşılaştırır ve ana bilgisayarın yetkili olup olmadığını anlar.

-Müşteri ana bilgisayarın yetkisini doğruladıktan sonra bir gizli mesajı ana bilgisayarın açık anahtarı ile şifreler ve gönderir. Eğer ana bilgisayar bu gizli mesaja cevap verirse müşterinin elindeki anahtarın kendisi tarafından üretildiğini de ispat etmiş olur. Bu durumda müşteri de ana bilgisayara kendi sertifikasını gönderir.

-Ana bilgisayar öncelikle müşterinin açık anahtarını ve sayısal imzasını kontrol eder. Bunlar doğrulandıktan sonra müşterinin sertifikasının geçerliliği test edilir.

-Müşterinin ve yayıncı kuruluşun DN numaraları, sertifikanın geçerlilik süresi ve yayıncı kuruluşun sayısal imzası doğrulandıktan sonra SSL protokolü ana bilgisayara, müşterinin yetkili olduğunu kabul etmesi ve bağlantıyı sürdürmesi için izin verir.

-Ana bilgisayar müşterinin yetki seviyesini kontrol eder. Bu aşamada ana bilgisayar erişimi yasaklanan sertifikaların listesini kontrol edip müşteri sertifikasının bu listede olmadığını da doğrular.

-Müşteri ana bilgisayarın deşifre ettiği ön şartları taşıdığını kanıtladıktan sonra ana gizlilik kurallarını oluşturur ve ana bilgisayarla birlikte bu kuralları kullanarak oturum için gerekli simetrik anahtarları üretirler.

-Müşteri ana bilgisayara simetrik anahtarla şifrelenmiş bir mesaj gönderir.

-Ana bilgisayar bu mesajı aynı anahtarla şifrelenmiş bir mesajla cevaplar.

-Bu mesajla SSL el sıkışması tamamlanmış olur ve müşteri ile ana bilgisayar arasında oturum başlar.

2.2.4.2. SET (Secure Electronic Transaction)

Internet üzerinden kredi kartı ile yapılan ödeme sistemleri arasında tüm dünyanın kabul ettiği mevcut en güvenli standart olan SET protokolü, Visa ve Mastercard'ın içinde bulunduğu bir konsorsiyum tarafından elektronik ticarete güvenliği sağlamak amacıyla geliştirilmiştir ve bir endüstri standardı haline gelmiştir.

SET, özellikle on-line (gerçek zamanda) kredi kartı bilgileri iletimi için geliştirilmiş bir standarttır. SET, kredi kartı ile yapılan on-line ödemelerde, bilgilerin internet üzerinden aktarımında gizliliği ve güvenliği sağlar. SET protokolü sadece müşteri (ürün siparişi veren kredi kartı sahibi) ile sanal dükkan (e-dükkan) ve kredi kartı şirketi arasındaki iletişimi şifreler. SET ile, ödeme işlemine taraf olan herkes (müşteri, dükkan sahibi, kredi kartı şirketi) birbirlerini tanırlar (authentication) ve bu ispatlanabilir⁹⁵. Açık Anahtar Şifrelemesini (Public Key Cryptography) ve DES (Data Encryption Standard), RSA (Rivest, Shamir, Adleman) şifreleme metotlarının birleşimini kullanan SET protokolünde tarafların birbirini tanıması ve alışveriş işlemleri, SSL'dekine benzer bir dijital sertifikasyon sistemi ile yapılır.

SET Altyapı Bileşenleri

Sanal Cüzdan (Virtual Wallet): Bir ağ üzerinden güvenli ödeme kartı işlemlerinin yapılmasını sağlayan ve on-line müşteriler tarafından kullanılan üründür. Kart sahibinin kart bilgilerini, anahtarlarını ve şifreleme bilgilerini saklamak için kullanılır. Yazılım kart sahibinin bilgisayarına yüklenir ve her alışverişte kart bilgilerinin girilmesi ihtiyacını ortadan kaldırır.

Sanal POS (Virtual POS): Ödeme kartı ve yetkilendirme işlemlerini gerçekleştirmek için on-line mağazalar tarafında kullanılan üründür. Mağazanın kart bilgilerini, anahtarlarını ve şifreleme bilgilerini saklamak için kullanılır.

Ödeme Çıkış Yolu (Payment Gateway): Mağaza bankası veya üçüncü bir parti tarafında kullanılan, mağazanın ve ödeme bilgilerinin doğruluklarının kanıtlanması için gönderilmesi gereken özel finansal ağına ara yüzlük yapan üründür.

Sertifika Otoritesi (Certificate Authority): Bir kişi veya kuruluşun internet üzerinde doğruluğunun kanıtlanması için kullanılan dijital sertifikaları üretmeye ve onaylamaya

⁹⁵ www.eng.bahcesehir.edu.tr/css/bolum11/bolum11.html

yetkili bir finansal kuruluş veya onaylanmış üçüncü bir parti tarafından kullanılan üründür.

SET sisteminde provizyon işlemi, alışveriş seçimini yaptıktan sonra müşterinin sanal cüzdanı ile mağazanın Sanal POS'unun birbirlerinin gerçekliklerini dijital sertifikalar aracılığıyla kontrol etmeleri ile başlar. Müşteri tarafından gönderilen bilgilerin mağazaya ulaşması ve mağazanın sipariş tutarını ve sanal cüzdanda bulunan ve kendisinin göremediği kredi kartının sertifika bilgilerini bankaya iletmesi ile devam eder. Banka bu bilgileri kontrol ederek provizyon verir. Sanal mağaza bankadan onayı aldıktan sonra ürünü müşteriye gönderir⁹⁶.

SET İşlem Akışı

- Kart sahibi satın alacağı ürünü seçer ve on-line sipariş formunu doldurur.
- Kart sahibi SET ile ödemeyi seçer.
- Kullanıcı ismi ve şifre girildikten sonra SET elektronik cüzdanı açılır ve kart sahibi hangi kredi kartı markası ile (Visa, Mastercard) ödeme yapacağını belirler.
- Elektronik cüzdan mağazaya kart sahibinin hangi kredi kartı markası ile ödeme yapacağını bildiren mesajı gönderir.
- Mağaza, kendisi ve bankasının kimlik bilgilerini , kart sahibinin tercih ettiği kredi kartı markasının sertifikasını ve bankasının açık anahtarını içeren mesajı kart sahibine gönderir.
- Elektronik cüzdan mağazanın ve bankasının sertifikasını onayladıktan sonra sipariş ve ödeme bilgilerini içeren mesajı şifreleyerek gönderir. Ödeme ve sipariş bilgileri beraber gönderildiği halde farklı anahtarlarla şifrelendiğinden ödeme bilgileri yalnızca banka, sipariş bilgileri ise yalnızca mağaza tarafından görülebilmektedir.
- Mağaza mesajın gerçekliğini belirledikten sonra sipariş bilgilerini deşifre eder.
- Mağaza şifreli ödeme bilgilerini bankasına gönderir.
- Banka ödeme bilgilerini deşifre eder, kart sahibinin sertifikasının doğruluğunu kontrol eder ve kart bilgilerini doğruluğunu kanıtlaması için kart sahibinin bankasına gönderir.

⁹⁶ www.ykb.com.

- Kartın ait olduđu banka kredi kartı bilgilerini kontrol ettikten sonra mağazanın bankasına bilgilerin doğruluđuyla ilgili mesajı gönderir.
- Mağaza bankası da mağazaya kredi kartı bilgilerinin doğruluđu ile ilgili mesajı gönderir.
- Mağaza, sonucu kart sahibine iletir.
- Verilen kart bilgileri doğru ise mağaza ürünü gönderir veya hizmeti gerçekleştirir.
- Mağaza normal tahsilat süreciyle bankasından sipariş tutarını tahsil eder⁹⁷.



⁹⁷ www.ykb.com.

BÖLÜM 3 SIS ŞİFRELEME ALGORİTMASI

3.1. Tanım

Mevcut şifreleme algoritmaları genel olarak iki farklı yaklaşıma dayandırılabilir: Birincisi şifrelenecek metindeki karakterlerin birbirleri ile yer değiştirmesi, ikincisi ise başka karakterlerle değiştirilmesidir. Karakterler değiştirilirken sınırlı sayıda algoritma dışındaki çoğu algoritmada karakterler birden veya sıfırdan başlayarak numaralandırılmakta ve değiştirme veya dönüştürme işlemleri için karakterler yerine bu sayısal ifadeler kullanılmaktadır. Farklı bir yaklaşım olarak bazı algoritmalarda karakterlerin ikili veya on altılı sayı sistemi kullanılarak sayısal ifadelere dönüştürüldüğü de görülmektedir. Yeni bir algoritma ortaya koymak için bu yaklaşımlardan yararlanmak mümkündür. Ancak bu durumda ortaya çıkacak algoritma ile aynı yaklaşımı kullanan diğerleri arasında çok belirgin ve temel benzerlikler olacağı da açıktır. Bu yüzden yeni bir algoritmanın diğerlerinden farklı olması için farklı bir temel yaklaşımdan hareket etmesi gerekmektedir. Bu çalışmada tanıtılacak yeni şifreleme metodu da yeni bir yaklaşımdan hareketle ortaya çıkmıştır ve bu metoda kullanılan yeni yaklaşımın ismi verilmiştir. SIS, (string, integer, string) kelimelerinin ilk harflerinden oluşan bir isimdir. Bu kelimelerin İngilizce olarak seçilmesinin nedeni ise bilgisayar programlama dillerinde değişken türleri tanımlanırken kullanılan evrensel kavramlar olmalarıdır. SIS, bir karakterin (string) önce iki basamaklı sayısal bir değere (Integer) çevrilmesi, daha sonra bu sayısal değer iki karaktere (String) bölünmesi yaklaşımı üzerine kurulmuş bir tekniktir. Örneğin $x = 29$ olsun; diğer şifreleme metodlarında x 'in sayısal değeri, yani 29 üzerinde işlem yapılır ve bu değer ikiye bölünmesinden $a + b = 29$ veya $a.b=29$ v.b. şartlarından birini sağlayan iki sayısal değer bulunması işlemi anlaşılır. SIS yaklaşımında ise 29 sayısı string bir değer olarak alınır; yani $29 = 2 \times 10 + 9$ yerine “29”=“2”&“9” kabul edilir. Daha sonra “2” ve “9” üzerinde değiştirme veya dönüştürme işlemleri ayrı ayrı yapılır. Bu işlemlerde aritmetiksel bir işlem söz konusu olursa sonuç değerinin yine tek rakam olması için modüler aritmetik (mod 10) kullanılır.

3.2. SIS'in Özellikleri

- SIS aslında tek bir algoritma olarak tanımlanamaz. Çünkü SIS ile ortaya konan teknikler kullanılarak yeni algoritmalar geliştirmek mümkündür. Bu özelliği ile SIS bir şifreleme tekniği veya algoritma geliştirme tekniği olarak düşünülebilir.
- SIS yer değiştirme esasına dayandığı için matematiksel modellerin kullanılmasına gerek yoktur ama istenirse matematiksel bir algoritma da tasarlanabilir.
- SIS algoritmalarında şifrelenecek metnin parçalara ayrılma zorunluluğu yoktur. Metin bütün olarak şifrelenebileceği gibi sekiz, on altı, otuz iki veya on beş, yirmi sekiz vb. karakterlik bölümlere ayrılarak da şifreleme yapılabilir. Bu özelliği ile SIS örneğin "16 Bit" bir algoritma olarak tanımlanamaz.
- SIS anahtar kullanma bakımından da esneklik sağlayan bir tekniktir. Verilecek örnek algoritmalarda görüleceği gibi, SIS, birçok anahtarın ayrı ayrı veya bir arada kullanılma imkanları son derece geniş ve anahtar sayısı sınırlandırılmamış bir şifreleme tekniği olarak karşımıza çıkmaktadır.
- SIS mevcut güvenlik sistemleri (SSL, SET) ve bu sistemlerin kullandığı araçlarla (Dijital Sertifika vb.) birlikte kullanılabileceği gibi farklı sistemler geliştirmeye de elverişli bir tekniktir.

3.3. Çalışma Sistemi

SIS temel olarak şu çalışma sistemine sahiptir:

- Karakterlerin iki basamaklı sayılarla ifade edilmesi.
- Bu sayılar yan yana veya matris şeklinde yazılarak bir sayı dizisi elde edilmesi.
- Oluşturulan sayı dizisinde rakamlar için sistematik yer değiştirme işlemleri yapılması
- Rakamların tekrar iki basamaklı sayılar şeklinde gruplandırılması.
- Elde edilen sayıların karakterlere çevrilmesi

Birinci Adım (Karakterlerin iki basamaklı sayılarla ifade edilmesi):

Bu işlem için öncelikle her karaktere karşılık gelen iki basamaklı sayıları gösteren bir tabloya ihtiyaç vardır. Bu tabloyu oluştururken dikkat edilmesi gereken bazı noktalar vardır: Öncelikle iki basamaklı sayılar 10-99 arasında doksan tane dir.

Ancak şifreleme işlemi sonunda örneğin (07) gibi bir değer elde edilme olasılığı vardır ve bu durumda (07) ye karşılık gelen bir karakter bulunamayacaktır. Bu noktada yapılması gereken 0-99 arasında numaralandırılmış yüz karakter kullanmak ve 0-10 arası sayıları 00, 01, 02... şeklinde iki basamaklı olarak yazmaktır. Şifrelemede kullanılacak örnek bir tablo Tablo 3.1’de gösterilmiştir.

Tablo 3.1. SIS ile şifreleme yapılırken kullanılacak karakterler (I)

00	a	10	ı	20	q	30	y	40	Ğ	50	Ö	60	W	70	6	80	.	90	\
01	b	11	i	21	r	31	z	41	H	51	P	61	X	71	7	81	,	91	^
02	c	12	j	22	s	32	A	42	I	52	Q	62	Y	72	8	82	:	92	=
03	ç	13	k	23	ş	33	B	43	İ	53	R	63	Z	73	9	83	;	93	<
04	d	14	l	24	t	34	C	44	J	54	S	64	0	74	#	84	!	94	>
05	e	15	m	25	u	35	Ç	45	K	55	Ş	65	1	75	\$	85	?	95	“
06	f	16	n	26	ü	36	D	46	L	56	T	66	2	76	%	86	+	96	‘
07	g	17	o	27	v	37	E	47	M	57	U	67	3	77	&	87	-	97	(
08	ğ	18	ö	28	w	38	F	48	N	58	Ü	68	4	78	@	88	*	98	)
09	h	19	p	29	x	39	G	49	O	59	V	69	5	79	€	89	/	99	~(Boşluk)

Bu tabloyu daha anlaşılır ve hızlı kullanmaya elverişli olarak Tablo 3.2’deki gibi de düzenleyebiliriz. Tablo 3.2’de karaktere ait iki basamaklı sayı önce satır, sonra sütun numarası yazılarak elde edilir. Bu şekilde hem kağıt üstünde hem de bir programlama dili ile yazılırken kullanım kolaylığı sağlanacaktır. Tablo 3.1 ve Tablo 3.2 aynı sonuçları veren iki tablodur ve bundan sonraki işlemlerde bu tablolar kullanılacak; bu iki tablodan bundan sonra yalnızca “tablo” olarak söz edilecektir.

Burada açıklanması gereken bir nokta boşluk karakteridir. Şifreleme sonucu elde edilecek metinde iki veya daha fazla boşluk karakteri arka arkaya gelebileceğinden, kaç boşluk karakteri olduğunu sayarken veya en sonda yer alacak boşluk karakterlerinin görülmemesinden dolayı ortaya çıkabilecek sakıncaları önlemek için, gerçek metinde boşluk karakteri, şifreli metinde ise “~” kullanılması daha uygundur. Bu durumda şifrelenecek metin tablodan iki basamaklı sayılar şeklinde kolayca yazılabilir. Örneğin “Bilgisayar” kelimesi: “33-11-14-07-11-22-00-30-00-21” şeklinde elde edilecektir.

Tablo 3.2. SIS ile şifreleme yapılırken kullanılacak karakterler (II)

	0	1	2	3	4	5	6	7	8	9
0	a	b	c	ç	d	e	f	g	ğ	H
1	ı	i	j	k	l	m	n	o	ö	P
2	q	r	s	ş	t	u	ü	v	w	X
3	y	z	A	B	C	Ç	D	E	F	G
4	Ğ	H	I	İ	J	K	L	M	N	O
5	Ö	P	Q	R	S	Ş	T	U	Ü	V
6	W	X	Y	Z	0	1	2	3	4	5
7	6	7	8	9	#	\$	%	&	@	€
8	.	,	:	;	!	?	+	-	*	/
9	\	^	=	<	>	“	‘	(	)	~(Boşluk)

İkinci Adım (İki basamaklı sayıların birleştirilmesi):

Elde edilen iki basamaklı sayılar herhangi bir matematiksel işleme tabi tutulmayacağı için bu sayıların bitişik olarak yazılmasında herhangi bir sakınca yoktur. Böylece rakamlardan oluşan bir dizi veya matris elde edilir. “Bilgisayar” kelimesi örneği üzerinde bu işlem yapılırsa, yeni sayı dizisi; “33111407112200300021” olacaktır.

Üçüncü Adım (Yer değiştirme işlemleri):

Bu aşamada önemli olan sayıların sıralamasının değişmesidir. Aksi takdirde ikiye ikiye gruplandırıldığında yine aynı sayılara ulaşılır. İkinci önemli nokta da diziye yeni rakam eklemek istenirse eklenen rakam adedinin çift olması gerektiğidir. Çünkü dizi bir sonraki aşamada yeniden ikiye ikiye gruplandırılacak ve artan tek rakam kalmaması gerekecektir. SIS şifreleme tekniğinin özellikleri anlatılırken tek bir algoritma olmadığı söylenmişti. İşte bu aşamada rakamların sıralamasını değiştirmek için çok farklı sistemler kullanma imkanı vardır ve kullanılan her farklı sistem aslında yeni bir şifreleme algoritması olarak ortaya konabilir. Yine “Bilgisayar” kelimesi üzerinde çalışarak birkaç farklı sistemle bu sayı dizisini değiştirelim:

Sayı dizisi: “33111407112200300021”

Örnek Sistem(1): Sayı dizisinin son rakamı başa alınırsa bütün rakamların sıralaması değişecektir. Bu durumda sonuç: “13311140711220030002”

Örnek Sistem(2): Sayı dizisinin başına ve sonuna “0” eklenirse “0331114071122003000210”

Örnek Sistem(3): Sayı dizisinin sondan birinci rakamı baştan ikinci sıraya, sondan ikinci rakamı baştan dördüncü sıraya sondan üçüncü rakamı baştan altıncı sıraya alınır. Bu işlem dizideki karakter sayısının yarısının bir eksiği olan $20/2=10-1=9$ rakamına ulaşıncaya kadar tekrarlanır. Bu durumda sonuç: “31321010104300701212”

Örnek Sistem(4): Sayı dizisinde sıra numarası tek olan rakamlar çıkarılıp dizinin sonuna yazılır. Bu durumda sonuç: “31101203023147120001”

Örnek Sistem(5): Dördüncü örnekte yapılan işlem iki kere tekrarlanır. Bu durumda sonuç: “31100341001023217201”

Örneklerden görülebileceği gibi, rakamları farklı şekillerde de karıştırmak mümkündür ve her seferinde farklı sonuçlar elde edilmektedir.

Dördüncü Adım (Rakamların tekrar iki basamaklı sayılar şeklinde gruplandırılması):

Bu aşamada ikinci adımda yapılan işlemin tersi gerçekleştirilir ve rakamlardan oluşan dizi tekrar iki basamaklı sayılar haline getirilir. Sonuçları karşılaştırmak için yukarıda örneklenen her sistem için bu işlem yürütülürse; “Bilgisayar” kelimesi için

Örnek(1) “13-31-11-40-71-12-20-03-00-02”

Örnek(2) “03-31-11-40-71-12-20-03-00-02-10”

Örnek(3) “31-32-10-10-10-43-00-70-12-12”

Örnek(4) “31-10-12-03-02-31-47-12-00-01”

Örnek(5) “31-10-03-41-00-10-23-21-72-01” sayı dizileri elde edilir.

Beşinci Adım (Elde edilen sayıların karakterlere çevrilmesi):

Bu aşamada ise birinci adımda yapılan işlemin tersi, yani, sayıların tablodan karakterlere çevrilmesi işlemi yapılır.

Örnek(1) “kziĞ7jqçac”

Örnek(2) “çziĞ7jqçacı”

Örnek(3) “zAııİa6jj”

Örnek(4) “zıjçczMjab”

Örnek(5) “zıçHaısr8b”

Görüldüğü gibi üçüncü adımda rakamların yerleri değiştirilirken kullanılan farklı sistemler sonuç olarak farklı şifreli metinler elde edilmesine yol açmıştır. Buradan çıkarılacak sonuç: Genel olarak SIS tekniği kullanılsa da her sistemin kendi başına bir algoritma olduğudur. Ayrıca on karakterlik “Bilgisayar” kelimesi istenirse bölünerek “Bilgi” ve “sayar” şeklinde ayrı ayrı şifrelenebilir. Ancak bölme işlemi şifrenin kırılmasını kolaylaştıracağından bu yola çok uzun metinler şifrlenirken başvurulması daha verimli olacaktır.

3.4. SIS Algoritmasında Matrislerin Kullanılması

Şifrelenecek metnin uzunluğu arttıkça daha karmaşık yer değiştirme işlemleri yapma imkanı da artacaktır. Ancak karmaşıklık arttıkça daha pratik çözümlere de ihtiyaç duyulacaktır. İşte serileri matris olarak yazmak daha az hamle ile daha çok yer değiştirme imkanı sağlayan bir pratik çözüm olarak ortaya konabilir. Örneğin yüz karakterlik bir seride “birinci ile üçüncü yer değiştir” şeklinde anlatılan bir işlem iki karakterin yerinin değişmesini ifade ederken bu serinin 10x10 matris olarak yazılıp “birinci ile üçüncü sütun yer değiştir” denirse bu değişiklikten etkilenecek karakter sayısı yirmi olacaktır. Ayrıca matris şeklinde yazılan rakamların tamamı örneğin matrisin transpozesi alınarak tek bir işlemle değiştirilebilir.

Örnek Algoritma 1 (Encryption):

Şifrelenecek Metin:

E-mail: sinan@x.com Hesap: 817342 Şifre: 173gd23f5

Adım 1: Karakterlerin iki basamaklı sayılarla ifade edilmesi

37-87-15-00-11-14-82-99-22-11-16-00-16-78-29-80-02-17-15-99-41-05-22-00-19-82-99-72-65-71-67-68-66-99-55-11-06-21-05-82-99-65-71-67-07-04-66-67-06-69

Adım 2: İki basamaklı sayıların birleştirilmesi

3787150011148299221116001678298002171599410522001982997265716768669955
110621058299657167070466670669

Adım 3: Sayıların matris olarak yazılması

Bu noktada yüz adet rakamdan oluşan seri 10x10 matris olarak yazılacaktır. Matrisin boyutları belirlenirken serideki rakam sayısından büyük veya eşit bir kare bulunmalıdır. Eğer matris seriden büyükse seriye matrisin boyutuna ulaşınca kadar “9” rakamı eklenir. Matrisin büyüklüğünün örneğin $9 \times 9 = 81$ gibi tek sayı olduğu durumlarda serinin eleman sayısı mutlaka çift olacağından şifreli metin çözümlenirken en az bir rakam artacak ve sondaki bir rakam mutlaka atılacaktır. Birden fazla rakam eklemesi yapılmışsa eklenen diğer rakamlar da boşluk karakteri olarak çözüleceğinden metnin sonundaki boşluklar atılarak gerçek metne ulaşılabilir.

Sayılar 10x10 matris olarak yazılırsa:

3	7	8	7	1	5	0	0	1	1
1	4	8	2	9	9	2	2	1	1
1	6	0	0	1	6	7	8	2	9
8	0	0	2	1	7	1	5	9	9
4	1	0	5	2	2	0	0	1	9
8	2	9	9	7	2	6	5	7	1
6	7	6	8	6	6	9	9	5	5
1	1	0	6	2	1	0	5	8	2
9	9	6	5	7	1	6	7	0	7
0	4	6	6	6	7	0	6	6	9

Adım 4: Yer değiştirme işlemleri:

1- Tek numaralı sütunlar matrisin sonuna sıra ile taşınacak

7	7	5	0	1	3	8	1	0	1
4	2	9	2	1	1	8	9	2	1
6	0	6	8	9	1	0	1	7	2
0	2	7	5	9	8	0	1	1	9
1	5	2	0	9	4	0	2	0	1
2	9	2	5	1	8	9	7	6	7
7	8	6	9	5	6	6	6	9	5
1	6	1	5	2	1	0	2	0	8
9	5	1	7	7	9	6	7	6	0
4	6	7	6	9	0	6	6	0	6

2- Tek numaralı satırlar matrisin sonuna sıra ile taşınacak

4	2	9	2	1	1	8	9	2	1
0	2	7	5	9	8	0	1	1	9
2	9	2	5	1	8	9	7	6	7
1	6	1	5	2	1	0	2	0	8
4	6	7	6	9	0	6	6	0	6
7	7	5	0	1	3	8	1	0	1
6	0	6	8	9	1	0	1	7	2
1	5	2	0	9	4	0	2	0	1
7	8	6	9	5	6	6	6	9	5
9	5	1	7	7	9	6	7	6	0

Adım 5: Rakamların tekrar iki basamaklı sayılar şeklinde gruplandırılması

Bu adımda matrisin önce satır satır yazılarak seri haline dönüştürülmesi gerekir. Daha sonra rakamlar iki basamaklı sayılar halinde gruplandırılabilir.

4292118921027598011929251897671615210208467690660677501381016068910172
152094020178695666959517796760

42-92-11-89-21-02-75-98-01-19-29-25-18-97-67-16-15-21-02-08-46-76-90-66-06-77-
50-13-81-01-60-68-91-01-72-15-20-94-02-01-78-69-56-66-95-95-17-79-67-60

Adım 6: Elde edilen sayıların karakterlere çevrilmesi

I=i/rc\$)bpxuö(3nmrcğL.%\2f&Ök,bW4^b8mq>cb@5T2""o€3W

Örnek Algoritma 1 (Decryption):

Bu şifreli metni çözmek için aşağıdaki işlemlerin yapılması gerekir:

Adım 1: Karakterlerin iki basamaklı sayılarla ifade edilmesi

4292118921027598011929251897671615210208467690660677501381016068910172
152094020178695666959517796760

Adım 2: İki basamaklı sayıların birleştirilmesi

42-92-11-89-21-02-75-98-01-19-29-25-18-97-67-16-15-21-02-08-46-76-90-66-06-77-
50-13-81-01-60-68-91-01-72-15-20-94-02-01-78-69-56-66-95-95-17-79-67-60

Adım 3: Sayıların matris olarak yazılması

4	2	9	2	1	1	8	9	2	1
0	2	7	5	9	8	0	1	1	9
2	9	2	5	1	8	9	7	6	7
1	6	1	5	2	1	0	2	0	8
4	6	7	6	9	0	6	6	0	6
7	7	5	0	1	3	8	1	0	1
6	0	6	8	9	1	0	1	7	2
1	5	2	0	9	4	0	2	0	1
7	8	6	9	5	6	6	6	9	5
9	5	1	7	7	9	6	7	6	0

Adım 4: Yer deęiřtirme iřlemleri

1- Sıra numaraları 1,2,3,4,5,6,7,8,9,10 olan sütunlar 6,1,7,2,8,3,9,4,10,5 şeklinde dizilecek

7	7	5	0	1	3	8	1	0	1
4	2	9	2	1	1	8	9	2	1
6	0	6	8	9	1	0	1	7	2
0	2	7	5	9	8	0	1	1	9
1	5	2	0	9	4	0	2	0	1
2	9	2	5	1	8	9	7	6	7
7	8	6	9	5	6	6	6	9	5
1	6	1	5	2	1	0	2	0	8
9	5	1	7	7	9	6	7	6	0
4	6	7	6	9	0	6	6	0	6

2- Sıra numaraları 1,2,3,4,5,6,7,8,9,10 olan satırlar 6,1,7,2,8,3,9,4,10,5 şeklinde dizilecek

3	7	8	7	1	5	0	0	1	1
1	4	8	2	9	9	2	2	1	1
1	6	0	0	1	6	7	8	2	9
8	0	0	2	1	7	1	5	9	9
4	1	0	5	2	2	0	0	1	9
8	2	9	9	7	2	6	5	7	1
6	7	6	8	6	6	9	9	5	5
1	1	0	6	2	1	0	5	8	2
9	9	6	5	7	1	6	7	0	7
0	4	6	6	6	7	0	6	6	9

Adım 5: Rakamların tekrar iki basamaklı sayılar şeklinde gruplandırılması

3787150011148299221116001678298002171599410522001982997265716768669955
110621058299657167070466670669

37-87-15-00-11-14-82-99-22-11-16-00-16-78-29-80-02-17-15-99-41-05-22-00-19-82-
99-72-65-71-67-68-66-99-55-11-06-21-05-82-99-65-71-67-07-04-66-67-06-69

Adım 6: Elde edilen sayıların karakterlere çevrilmesi

E-mail: sinan@x.com Hesap: 817342 Şifre: 173gd23f5

Örnek Algoritma 2 (Encryption):

Değiştirme işlemleri sadece sütunların veya satırların yer değiştirmesi olarak düşünülmemelidir. Bu amaçla birçok farklı sistem kullanılabilir. Örneğin elde edilen matris bir yap-boz (Puzzle) olarak düşünülebilir ve sistemli şekilde kaydırmalar yapılabilir. Farklı teknikler sonucu elde edilecek şifreli metinlerin karşılaştırılabilmesi için bundan sonraki örneklerde de (Örnek Algoritma 1)'de kullanılan metin şifrelenecektir.

Şifrelenecek Metin: "E-mail: sinan@x.com Hesap: 817342 Şifre: 173gd23f5"

Adım 1: Karakterlerin iki basamaklı sayılarla ifade edilmesi

37-87-15-00-11-14-82-99-22-11-16-00-16-78-29-80-02-17-15-99-41-05-22-00-19-82-
99-72-65-71-67-68-66-99-55-11-06-21-05-82-99-65-71-67-07-04-66-67-06-69

Adım 2: İki basamaklı sayıların birleştirilmesi

3787150011148299221116001678298002171599410522001982997265716768669955
110621058299657167070466670669

Adım 3: Sayıların matris olarak yazılması: Bu aşamada işlemlerin daha kolay görülebilmesi için matris tablo olarak düzenlenebilir.

3	7	8	7	1	5	0	0	1	1
1	4	8	2	9	9	2	2	1	1
1	6	0	0	1	6	7	8	2	9
8	0	0	2	1	7	1	5	9	9
4	1	0	5	2	2	0	0	1	9
8	2	9	9	7	2	6	5	7	1
6	7	6	8	6	6	9	9	5	5
1	1	0	6	2	1	0	5	8	2

9 9 6 5 7 1 6 7 0 7
0 4 6 6 6 7 0 6 6 9

Adım 4: Yer deęiřtirme İřlemleri

1-Sıra numarası çift olan satırlar bir sıra saęa:

3 7 8 7 1 5 0 0 1 1
1 4 8 2 9 9 2 2 1 1
1 6 0 0 1 6 7 8 2 9
8 0 0 2 1 7 1 5 9 9
4 1 0 5 2 2 0 0 1 9
8 2 9 9 7 2 6 5 7 1
6 7 6 8 6 6 9 9 5 5
1 1 0 6 2 1 0 5 8 2
9 9 6 5 7 1 6 7 0 7
0 4 6 6 6 7 0 6 6 9

2- Sıra numarası çift olan sütunlar bir satır ařaęıya

3 8 1 0 1
7 4 7 2 5 9 0 2 1 1
1 1 0 8 1 9 7 2 2 1
6 0 0 2 6 7 8 5 9 9
4 8 0 0 2 1 0 1 1 9
1 2 5 9 2 2 0 5 9 1
6 8 6 9 6 7 9 6 5 7
7 1 8 6 6 1 9 5 5 2
9 1 6 0 7 2 6 0 0 8
9 4 5 6 1 7 7 6 7 9
0 6 6 0 6

3- Sıra numarası çift olan satırlar bir sıra sola:

3 8 1 0 1
7 4 7 2 5 9 0 2 1 1
1 1 0 8 1 9 7 2 2 1
6 0 0 2 6 7 8 5 9 9
4 8 0 0 2 1 0 1 1 9
1 2 5 9 2 2 0 5 9 1
6 8 6 9 6 7 9 6 5 7
7 1 8 6 6 1 9 5 5 2

9	1	6	0	7	2	6	0	0	8
9	4	5	6	1	7	7	6	7	9
	0		6		6		0		6

4- Sıra numarası çift olan sütunlar bir satır yukarıya

3	4	8	2	1	9	0	2	1	1
7	1	7	8	5	9	0	2	1	1
1	0	0	2	1	7	7	5	2	9
6	8	0	0	6	1	8	1	9	9
4	2	0	9	2	2	0	5	1	1
1	8	5	9	2	7	0	6	9	7
6	1	6	6	6	1	9	5	5	2
7	1	8	0	6	2	9	0	5	8
9	4	6	6	7	7	6	6	0	9
9	0	5	6	1	6	7	0	7	6

Adım 5: Rakamların tekrar iki basamaklı sayılar şeklinde gruplandırılması

3482190211717859021110021775296800618199420922051118592706976166619552
718062905894667766099056167076

34-82-19-02-11-71-78-59-02-11-10-02-17-75-29-68-00-61-81-99-42-09-22-05-11-18-
59-27-06-97-61-66-61-95-52-71-80-62-90-58-94-66-77-66-09-90-56-16-70-76

Adım 6: Elde edilen sayıların karakterlere çevrilmesi

C:pci7@Vciico\$x4aX,~lhseiöVvf(X2X"Q7.Y\Ü>2&2h\Tn6%

Örnek Algoritma 2 (Decryption):

Bu sistemde şifreli metni çözmek için değiştirme işlemleri tersten ve her bir işlemin tersi olarak yapılmalıdır. İşlem sırası dörtten bire doğru yürütülürken her işlemin de tersi yani işlem sola ise sağa, yukarıya ise aşağıya doğru kaydırılarak yapılmalıdır.

4- Sıra numarası çift olan sütunlar bir satır aşağıya

3		8		1		0		1	
7	4	7	2	5	9	0	2	1	1
1	1	0	8	1	9	7	2	2	1
6	0	0	2	6	7	8	5	9	9
4	8	0	0	2	1	0	1	1	9

1	2	5	9	2	2	0	5	9	1
6	8	6	9	6	7	9	6	5	7
7	1	8	6	6	1	9	5	5	2
9	1	6	0	7	2	6	0	0	8
9	4	5	6	1	7	7	6	7	9
	0		6		6		0		6

3- Sıra numarası çift olan satırlar bir sıra sağa:

3		8		1		0		1	
	7	4	7	2	5	9	0	2	1 1
1	1	0	8	1	9	7	2	2	1
	6	0	0	2	6	7	8	5	9 9
4	8	0	0	2	1	0	1	1	9
	1	2	5	9	2	2	0	5	9 1
6	8	6	9	6	7	9	6	5	7
	7	1	8	6	6	1	9	5	5 2
9	1	6	0	7	2	6	0	0	8
	9	4	5	6	1	7	7	6	7 9
	0		6		6		0		6

2- Sıra numarası çift olan sütunlar bir satır yukarıya

3	7	8	7	1	5	0	0	1	1
	1	4	8	2	9	9	2	2	1 1
1	6	0	0	1	6	7	8	2	9
	8	0	0	2	1	7	1	5	9 9
4	1	0	5	2	2	0	0	1	9
	8	2	9	9	7	2	6	5	7 1
6	7	6	8	6	6	9	9	5	5
	1	1	0	6	2	1	0	5	8 2
9	9	6	5	7	1	6	7	0	7
	0	4	6	6	6	7	0	6	6 9

1- Sıra numarası çift olan satırlar bir sıra sola:

3	7	8	7	1	5	0	0	1	1
1	4	8	2	9	9	2	2	1	1
1	6	0	0	1	6	7	8	2	9
8	0	0	2	1	7	1	5	9	9
4	1	0	5	2	2	0	0	1	9

8	2	9	9	7	2	6	5	7	1
6	7	6	8	6	6	9	9	5	5
1	1	0	6	2	1	0	5	8	2
9	9	6	5	7	1	6	7	0	7
0	4	6	6	6	7	0	6	6	9

Görüldüğü gibi elde edilen matris şifrelenecek metne ait matristir ve rakamlar ikişerli gruplandırılarak tablo değerlerine çevrilirse başlangıçtaki metin elde edilecektir.

Adım 5: Rakamların tekrar iki basamaklı sayılar şeklinde gruplandırılması

3787150011148299221116001678298002171599410522001982997265716768669955
110621058299657167070466670669

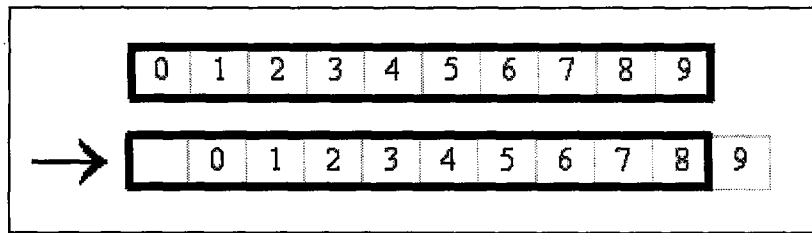
37-87-15-00-11-14-82-99-22-11-16-00-16-78-29-80-02-17-15-99-41-05-22-00-19-82-
99-72-65-71-67-68-66-99-55-11-06-21-05-82-99-65-71-67-07-04-66-67-06-69

Adım 6: Elde edilen sayıların karakterlere çevrilmesi

E-mail: sinan@x.com Hesap: 817342 Şifre: 173gd23f5

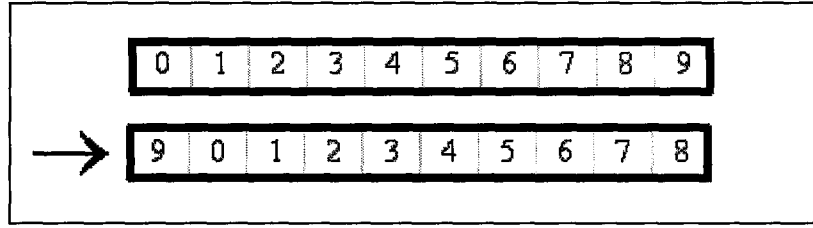
3.5. Dairesel Hareketle Kaydırma

Matris şeklinde yazılmış rakamların yerleri değiştirilirken kullanılacak bir başka sistem de dairesel hareketle yapılacak kaydırmalardır. Dairesel hareket için satırın veya sütunun bir daire üzerine yazıldığı varsayımından hareket edilir. Vektörel harekette bir birim kaydırma sonucu ilk karakterin yeri boş kalır ve sonda bir karakter artar (Şekil 3.15).



Şekil 3.15. Vektörel Hareketle Kaydırma

Dairesel harekette ise yapılacak bir birimlik kaydırma sonucu sondaki bir rakam sıranın en başına kayacaktır (Şekil 3.16).



Şekil 3.16. Dairesel Hareketle Kaydırma

Dairesel kaydırma hareketi kullanılarak birçok farklı algoritma geliştirilebilir. Örneğin önce sütunların daha sonra satırların sıra numaraları kadar kaydırılarak bir şifreleme yapılabilir.

Örnek Algoritma 3 (Encryption):

Şifrelenecek Metin: “E-mail: sinan@x.com Hesap: 817342 Şifre: 173gd23f5”

Adım 1: Karakterlerin iki basamaklı sayılarla ifade edilmesi

37-87-15-00-11-14-82-99-22-11-16-00-16-78-29-80-02-17-15-99-41-05-22-00-19-82-
99-72-65-71-67-68-66-99-55-11-06-21-05-82-99-65-71-67-07-04-66-67-06-69

Adım 2: İki basamaklı sayıların birleştirilmesi

3787150011148299221116001678298002171599410522001982997265716768669955
110621058299657167070466670669

Adım 3: Sayıların matris olarak yazılması:

3	7	8	7	1	5	0	0	1	1
1	4	8	2	9	9	2	2	1	1
1	6	0	0	1	6	7	8	2	9
8	0	0	2	1	7	1	5	9	9
4	1	0	5	2	2	0	0	1	9
8	2	9	9	7	2	6	5	7	1
6	7	6	8	6	6	9	9	5	5
1	1	0	6	2	1	0	5	8	2
9	9	6	5	7	1	6	7	0	7
0	4	6	6	6	7	0	6	6	9

Adım 4: Yer değiştirme İşlemleri

1- İlk sütun bir satır aşağıya, ikinci sütun iki satır aşağıya, vb.

0	9	0	8	7	2	1	8	1	1
3	4	6	6	6	2	0	5	2	1
1	7	6	5	2	6	6	0	9	9
1	4	8	6	7	1	9	5	1	9
8	6	8	7	6	1	0	9	7	9
4	0	0	2	1	7	6	5	5	1
8	1	0	0	9	5	0	7	8	5
6	2	0	2	1	9	0	6	0	2
1	7	9	5	1	6	2	0	6	7
9	1	6	9	2	7	7	2	1	9

Bu aşamada dikkat edilmesi gereken bir nokta da kaydırma miktarının satır sayısına eşit olması durumudur. Onuncu sütuna dikkat edilirse herhangi bir değişiklik olmadığı görülür. Çünkü dairesel hareket gereği on birimlik bir seride her bir birim kaydırma $360/10=36$ derecelik bir dönüş ifade eder. Eğer sütun 10 birim kaydırılırsa $36 \times 10 = 360$ derecelik bir dönüş gerçekleşecek ve başlangıçtaki noktaya dönülecektir. Fazladan işlem yapmayı önlemek için 10×10 matriste 10 birim $10 \equiv 0 \pmod{10}$ olarak ifade edilebilir. Bu durumda onuncu sütun hiç kaydırılmayacaktır.

Genel Olarak: $n \times n$ bir matris için a birim kaydırma işlemi yapılsın. Eğer $a \equiv b \pmod{n}$ ise, a birim kaydırma ile b birim kaydırma işlemleri aynı sonucu verecektir.

2- İlk satır bir sütun sağa, ikinci satır iki sütun sağa, vb.

1	0	9	0	8	7	2	1	8	1
2	1	3	4	6	6	6	2	0	5
0	9	9	1	7	6	5	2	6	6
9	5	1	9	1	4	8	6	7	1
1	0	9	7	9	8	6	8	7	6
1	7	6	5	5	1	4	0	0	2
0	9	5	0	7	8	5	8	1	0
0	2	1	9	0	6	0	2	6	2
7	9	5	1	6	2	0	6	7	1
9	1	6	9	2	7	7	2	1	9

Adım 5: Rakamların tekrar iki basamaklı sayılar şeklinde gruplandırılması

1090872181213466620509917652669519148671109798687617655140020950785810
021906026279516206719169277219

10-90-87-21-81-21-34-66-62-05-09-91-76-52-66-95-19-14-86-71-10-97-98-68-76-17-65-51-40-02-09-50-78-58-10-02-19-06-02-62-79-51-62-06-71-91-69-27-72-19

Adım 6: Elde edilen sayıların karakterlere çevrilmesi

ı\~r,rC2Yeh^%Q2"pl+7ı()4%o1PĞchÖ@ÜıcpfcY€PYf7^5v8p

Örnek Algoritma 3 (Decryption):

Şifreli metni çözmek için yine dönüştürme işlemleri sondan başa ve her işlemin tersi olarak yapılır.

2- İlk satır bir sütun sola, ikinci satır iki sütun sola, vb.

1- İlk sütun bir satır yukarıya, ikinci sütun iki satır yukarıya, vb.

Ancak dairesel hareketin bir özelliği olarak şifreleme yaparken k birim hareket edilmiş ise, şifreyi çözerken aynı yönde n x n matris için (n – k) birim hareket ederek de aynı noktaya varılabilir. Bu durumda çözüm aşamaları şu şekilde olacaktır:

2- İlk satır 10-1=9 sütun sağa, ikinci satır 10-2=8 sütun sağa, vb.

0	9	0	8	7	2	1	8	1	1
3	4	6	6	6	2	0	5	2	1
1	7	6	5	2	6	6	0	9	9
1	4	8	6	7	1	9	5	1	9
8	6	8	7	6	1	0	9	7	9
4	0	0	2	1	7	6	5	5	1
8	1	0	0	9	5	0	7	8	5
6	2	0	2	1	9	0	6	0	2
1	7	9	5	1	6	2	0	6	7
9	1	6	9	2	7	7	2	1	9

1- İlk sütun 10-1=9 satır aşağıya, ikinci sütun 10-2=8 satır aşağıya, vb.

3	7	8	7	1	5	0	0	1	1
1	4	8	2	9	9	2	2	1	1
1	6	0	0	1	6	7	8	2	9
8	0	0	2	1	7	1	5	9	9
4	1	0	5	2	2	0	0	1	9
8	2	9	9	7	2	6	5	7	1
6	7	6	8	6	6	9	9	5	5
1	1	0	6	2	1	0	5	8	2
9	9	6	5	7	1	6	7	0	7

0 4 6 6 6 7 0 6 6 9

3.6. SIS’de Anahtar Kullanılarak Şifreleme

Anahtar, şifrelemenin güvenliğini sağlayan ve şifreli metnin üçüncü şahıs tarafından çözülmemesi için kullanılan bir araçtır. İki kişi arasındaki iletişimde şifreleme algoritması tek başına anahtar görevini üstlenebilir. Ancak alıcıların sayısı arttıkça algoritmanın gizli tutulması giderek zorlaşacak bazı durumlarda ise ilan edilmesi gerekecektir. İşte bu durumda güvenliğini sağlamak için anahtar kullanmak gerekli olur. Örneğin A ve B isimli şahıslar kendi aralarında bir şifreleme geliştirmişler ve bu şifrelemeyi kullanarak birbirlerine mesaj gönderiyorlar. Bu durumda üçüncü kişilerin, mesajların nasıl şifrelendiğini bilmediklerinden, şifreli metinleri kırmak için çaba göstermesi gerekecektir. Bir X kurumu ise kendisine bağlı yüzlerce temsilcilikle şifreli olarak haberleşmek istiyor. Bu durumda kullanacağı algoritmanın gizliliğini sağlaması oldukça güç olacak, ayrıca herhangi bir temsilciliğine göndereceği mesajın diğer temsilcilikler tarafından çözülmesini istemiyorsa, her temsilcilik için farklı algoritma kullanması gerekecektir. X kurumu için önerilecek yol, mesajlarını bilinmesinde sakınca olmayan bir metotla şifrelemek ve her temsilcisi için bir anahtar belirleyerek gizliliği ve güvenliğini bu anahtarlarla sağlamak olacaktır.

SIS, anahtar kullanımında son derece esnek bir algoritmadır. Diğer algoritmalarda anahtar genellikle matematiksel bir fonksiyonun bir parametresi olarak kullanılır. SIS’de ise anahtar parametre olabileceği gibi yer değiştirmenin kurallarını belirtebilir veya rasgele seçilmiş bir başka anahtarı şifreli metin içerisinde gizleyen bir yer belirleyici olabilir. Ayrıca anahtar tek bir sayı olabileceği gibi bir haneli rakamlardan oluşan bir sayı dizisi olarak da kullanılabilir. SIS’in bu konuda sağladığı en büyük avantaj ise anahtar sayısının veya anahtarın uzunluğunun sınırlanmamış olmasıdır.

3.6.1. Tek Anahtarlı Modeller

Tek anahtar kullanarak yapılacak şifrelemede anahtarın kullanılma şekline göre farklı algoritmalar geliştirilebilir.

1- Anahtara ait sayı dizisindeki rakamlar şifrelenecek metne ait sayı dizisi (Örnek Algoritma 4) veya matristeki rakamlara(Örnek Algoritma 5) sıra ile eklenir.

2- Anahtara ait sayı dizisindeki rakamlar şifrelenecek metne ait sayı dizisindeki rakamların (Örnek Algoritma 6) veya matristeki satır ve sütunların (Örnek Algoritma 7) yer değiştirme kurallarını oluşturur.

3- Anahtara ait sayı dizisindeki rakamlar şifrelenecek metne ait matristeki satır ve sütunların kaydırılması kurallarını oluşturur (Örnek Algoritma 8).

Örnek Algoritma 4 (Encryption):

Şifrelenecek Metin: "E-mail: sinan@x.com Hesap: 817342 Şifre: 173gd23f5"

Anahtar: "DA14" = 36-32-65-68 = 36326568

Adım 1: Karakterlerin iki basamaklı sayılarla ifade edilmesi

37-87-15-00-11-14-82-99-22-11-16-00-16-78-29-80-02-17-15-99-41-05-22-00-19-82-99-72-65-71-67-68-66-99-55-11-06-21-05-82-99-65-71-67-07-04-66-67-06-69

Adım 2: İki basamaklı sayıların birleştirilmesi

3787150011148299221116001678298002171599410522001982997265716768669955110621058299657167070466670669

Adım 3: Birinci rakam anahtarın birinci rakamı ile, ikinci rakam anahtarın ikinci rakamı ile, vb toplanır. Anahtardaki rakamlar bitince yeniden başlanacak ve toplama işlemi (mod 10)'a göre yapılacaktır.

	3	7	8	7	1	5	0	0	1	1	1	4	8	2	9	9	2	2	1	1
+	3	6	3	2	6	5	6	8	3	6	3	2	6	5	6	8	3	6	3	2
=	6	3	1	9	7	0	6	8	4	7	4	6	4	7	5	7	5	8	4	3

	1	6	0	0	1	6	7	8	2	9	8	0	0	2	1	7	1	5	9	9
+	6	5	6	8	3	6	3	2	6	5	6	8	3	6	3	2	6	5	6	8
=	7	1	6	8	4	2	0	0	8	4	4	8	3	8	4	9	7	0	5	7

	4	1	0	5	2	2	0	0	1	9	8	2	9	9	7	2	6	5	7	1
+	3	6	3	2	6	5	6	8	3	6	3	2	6	5	6	8	3	6	3	2
=	7	7	3	7	8	7	6	8	4	5	1	4	5	4	3	0	9	1	0	3

	6	7	6	8	6	6	9	9	5	5	1	1	0	6	2	1	0	5	8	2
+	6	5	6	8	3	6	3	2	6	5	6	8	3	6	3	2	6	5	6	8

$$\begin{array}{r}
= \quad 2 \quad 2 \quad 2 \quad 6 \quad 9 \quad 2 \quad 2 \quad 1 \quad 1 \quad 0 \quad 7 \quad 9 \quad 3 \quad 2 \quad 5 \quad 3 \quad 6 \quad 0 \quad 4 \quad 0 \\
\\
\quad 9 \quad 9 \quad 6 \quad 5 \quad 7 \quad 1 \quad 6 \quad 7 \quad 0 \quad 7 \quad 0 \quad 4 \quad 6 \quad 6 \quad 6 \quad 7 \quad 0 \quad 6 \quad 6 \quad 9 \\
+ \quad 3 \quad 6 \quad 3 \quad 2 \quad 6 \quad 5 \quad 6 \quad 8 \quad 3 \quad 6 \quad 3 \quad 2 \quad 6 \quad 5 \quad 6 \quad 8 \quad 3 \quad 6 \quad 3 \quad 2 \\
= \quad 2 \quad 5 \quad 9 \quad 7 \quad 3 \quad 6 \quad 2 \quad 5 \quad 3 \quad 3 \quad 3 \quad 6 \quad 2 \quad 1 \quad 2 \quad 5 \quad 3 \quad 2 \quad 9 \quad 1
\end{array}$$

Adım 4: Rakamların tekrar iki basamaklı sayılar şeklinde gruplandırılması

6319706847464757584371684200844838497057773787684514543091032226922110
793253604025973625333621253291

63-19-70-68-47-46-47-57-58-43-71-68-42-00-84-48-38-49-70-57-77-37-87-68-45-14-
54-30-91-03-22-26-92-21-10-79-32-53-60-40-25-97-36-25-33-36-21-25-32-91

Adım 5: Elde edilen sayıların karakterlere çevrilmesi

Şifreli Metin: Zp64MLMUÜİ74Ia!NFO6U&E-4KlSy^çsü=rı€ARWĞu(DuBDruA^

Örnek Algoritma 4 (Decryption):

Şifreli metni çözmek için uygulanacak adımlar ise şunlardır:

Adım 1: Karakterlerin iki basamaklı sayılarla ifade edilmesi

63-19-70-68-47-46-47-57-58-43-71-68-42-00-84-48-38-49-70-57-77-37-87-68-45-14-
54-30-91-03-22-26-92-21-10-79-32-53-60-40-25-97-36-25-33-36-21-25-32-91

Adım 2: İki basamaklı sayıların birleştirilmesi

6319706847464757584371684200844838497057773787684514543091032226922110
793253604025973625333621253291

Adım 3: Birinci rakam anahtarın birinci rakamından, ikinci rakam anahtarın ikinci rakamından, vb çıkarılır. Anahtardaki rakamlar bitince yeniden başlanacak ve çıkarma işlemi (mod 10)'a göre yapılacaktır.

$$\begin{array}{r}
\quad 6 \quad 3 \quad 1 \quad 9 \quad 7 \quad 0 \quad 6 \quad 8 \quad 4 \quad 7 \quad 4 \quad 6 \quad 4 \quad 7 \quad 5 \quad 7 \quad 5 \quad 8 \quad 4 \quad 3 \\
- \quad 3 \quad 6 \quad 3 \quad 2 \quad 6 \quad 5 \quad 6 \quad 8 \quad 3 \quad 6 \quad 3 \quad 2 \quad 6 \quad 5 \quad 6 \quad 8 \quad 3 \quad 6 \quad 3 \quad 2 \\
= \quad 3 \quad 7 \quad 8 \quad 7 \quad 1 \quad 5 \quad 0 \quad 0 \quad 1 \quad 1 \quad 1 \quad 4 \quad 8 \quad 2 \quad 9 \quad 9 \quad 2 \quad 2 \quad 1 \quad 1 \\
\\
\quad 7 \quad 1 \quad 6 \quad 8 \quad 4 \quad 2 \quad 0 \quad 0 \quad 8 \quad 4 \quad 4 \quad 8 \quad 3 \quad 8 \quad 4 \quad 9 \quad 7 \quad 0 \quad 5 \quad 7 \\
- \quad 6 \quad 5 \quad 6 \quad 8 \quad 3 \quad 6 \quad 3 \quad 2 \quad 6 \quad 5 \quad 6 \quad 8 \quad 3 \quad 6 \quad 3 \quad 2 \quad 6 \quad 5 \quad 6 \quad 8 \\
= \quad 1 \quad 6 \quad 0 \quad 0 \quad 1 \quad 6 \quad 7 \quad 8 \quad 2 \quad 9 \quad 8 \quad 0 \quad 0 \quad 2 \quad 1 \quad 7 \quad 1 \quad 5 \quad 9 \quad 9
\end{array}$$

	7	7	3	7	8	7	6	8	4	5	1	4	5	4	3	0	9	1	0	3
-	3	6	3	2	6	5	6	8	3	6	3	2	6	5	6	8	3	6	3	2
=	4	1	0	5	2	2	0	0	1	9	8	2	9	9	7	2	6	5	7	1

	2	2	2	6	9	2	2	1	1	0	7	9	3	2	5	3	6	0	4	0
-	6	5	6	8	3	6	3	2	6	5	6	8	3	6	3	2	6	5	6	8
=	6	7	6	8	6	6	9	9	5	5	1	1	0	6	2	1	0	5	8	2

	2	5	9	7	3	6	2	5	3	3	3	6	2	1	2	5	3	2	9	1
-	3	6	3	2	6	5	6	8	3	6	3	2	6	5	6	8	3	6	3	2
=	9	9	6	5	7	1	6	7	0	7	0	4	6	6	6	7	0	6	6	9

Adım 4: Rakamların tekrar iki basamaklı sayılar şeklinde gruplandırılması

3787150011148299221116001678298002171599410522001982997265716768669955
110621058299657167070466670669

37-87-15-00-11-14-82-99-22-11-16-00-16-78-29-80-02-17-15-99-41-05-22-00-19-82-
99-72-65-71-67-68-66-99-55-11-06-21-05-82-99-65-71-67-07-04-66-67-06-69

Adım 5: Elde edilen sayıların karakterlere çevrilmesi

Gerçek Metin: E-mail: sinan@x.com Hesap: 817342 Şifre: 173gd23f5

Örnek Algoritma 5 (Encryption):

Şifrelenecek Metin: E-mail: sinan@x.com Hesap: 817342 Şifre: 173gd23f5

Anahtar: DA14 = 36-32-65-68

Adım 1: Karakterlerin iki basamaklı sayılarla ifade edilmesi

37-87-15-00-11-14-82-99-22-11-16-00-16-78-29-80-02-17-15-99-41-05-22-00-19-82-
99-72-65-71-67-68-66-99-55-11-06-21-05-82-99-65-71-67-07-04-66-67-06-69

Adım 2: İki basamaklı sayıların birleştirilmesi

3787150011148299221116001678298002171599410522001982997265716768669955
110621058299657167070466670669

Adım 3: Sayı dizisinin nxn matris olarak yazılması n = 10

3	7	8	7	1	5	0	0	1	1
1	4	8	2	9	9	2	2	1	1
1	6	0	0	1	6	7	8	2	9
8	0	0	2	1	7	1	5	9	9
4	1	0	5	2	2	0	0	1	9
8	2	9	9	7	2	6	5	7	1
6	7	6	8	6	6	9	9	5	5
1	1	0	6	2	1	0	5	8	2
9	9	6	5	7	1	6	7	0	7
0	4	6	6	6	7	0	6	6	9

Adım 4:

1- Anahtar önce sütun değeri olarak, daha sonra kaldığı yerden satır değeri olarak yazılır. Anahtardaki rakamlar bitince yeniden başlanacaktır.

Değerler:	3	6	3	2	6	5	6	8	3	6
3	3	7	8	7	1	5	0	0	1	1
2	1	4	8	2	9	9	2	2	1	1
6	1	6	0	0	1	6	7	8	2	9
5	8	0	0	2	1	7	1	5	9	9
6	4	1	0	5	2	2	0	0	1	9
8	8	2	9	9	7	2	6	5	7	1
3	6	7	6	8	6	6	9	9	5	5
6	1	1	0	6	2	1	0	5	8	2
3	9	9	6	5	7	1	6	7	0	7
2	0	4	6	6	6	7	0	6	6	9

2- Matrisin her değeri ait olduğu satır ve sütunun değerleri ile toplanır. Toplama işlemi (mod 10)'a göre yapılacaktır.

9	6	4	2	0	3	9	1	7	0
6	2	3	6	7	6	0	2	6	9
0	8	9	8	3	7	9	2	1	1
6	1	8	9	2	7	2	8	7	0
0	0	6	0	1	0	9	1	7	8
9	6	0	9	1	5	0	1	8	5
2	6	2	3	5	4	8	0	1	4
0	3	9	4	4	2	2	9	7	4
5	8	2	0	6	9	5	8	6	6
5	2	1	0	4	4	8	6	1	7

Adım 5: Rakamların tekrar iki basamaklı sayılar şeklinde gruplandırılması

9642039170623676026908983792116189272870006010917896091501852623548014
039442297458206958665210448617

96-42-03-91-70-62-36-76-02-69-08-98-37-92-11-61-89-27-28-70-00-60-10-91-78-96-
09-15-01-85-26-23-54-80-14-03-94-42-29-74-58-20-69-58-66-52-10-44-86-17

Adım 6: Elde edilen sayıların karakterlere çevrilmesi

Şifreli Metin: 'Iç^6YD%c5ğ)E=iX/vw6aWı^@'hmb?üşS.lç>Ix#Üq5Ü2QıJ+o

Örnek Algoritma 5 (Decryption):

Şifreli metni çözmek için uygulanacak adımlar ise şunlardır:

Adım 1: Karakterlerin iki basamaklı sayılarla ifade edilmesi

96-42-03-91-70-62-36-76-02-69-08-98-37-92-11-61-89-27-28-70-00-60-10-91-78-96-
09-15-01-85-26-23-54-80-14-03-94-42-29-74-58-20-69-58-66-52-10-44-86-17

Adım 2: İki basamaklı sayıların birleştirilmesi

9642039170623676026908983792116189272870006010917896091501852623548014
039442297458206958665210448617

Adım 3: Sayı dizisinin $n \times n$ matris olarak yazılması $n = 10$

9	6	4	2	0	3	9	1	7	0
6	2	3	6	7	6	0	2	6	9
0	8	9	8	3	7	9	2	1	1
6	1	8	9	2	7	2	8	7	0
0	0	6	0	1	0	9	1	7	8
9	6	0	9	1	5	0	1	8	5
2	6	2	3	5	4	8	0	1	4
0	3	9	4	4	2	2	9	7	4
5	8	2	0	6	9	5	8	6	6
5	2	1	0	4	4	8	6	1	7

Adım 4:

1- Anahtar önce sütun değeri olarak, daha sonra kaldığı yerden satır değeri olarak yazılır. Anahtardaki rakamlar bitince yeniden başlanacaktır.

Değerler	3	6	3	2	6	5	6	8	3	6
3	9	6	4	2	0	3	9	1	7	0
2	6	2	3	6	7	6	0	2	6	9
6	0	8	9	8	3	7	9	2	1	1
5	6	1	8	9	2	7	2	8	7	0
3	0	0	6	0	1	0	9	1	7	8
8	9	6	0	9	1	5	0	1	8	5
3	2	6	2	3	5	4	8	0	1	4
6	0	3	9	4	4	2	2	9	7	4
3	5	8	2	0	6	9	5	8	6	6
2	5	2	1	0	4	4	8	6	1	7

2- Matrisin her değerinden ait olduğu satır ve sütunun değerleri çıkarılır. Çıkarma işlemi (mod 10)'a göre yapılacaktır.

3	7	8	7	1	5	0	0	1	1
1	4	8	2	9	9	2	2	1	1
1	6	0	0	1	6	7	8	2	9
8	0	0	2	1	7	1	5	9	9
4	1	0	5	2	2	0	0	1	9
8	2	9	9	7	2	6	5	7	1
6	7	6	8	6	6	9	9	5	5
1	1	0	6	2	1	0	5	8	2
9	9	6	5	7	1	6	7	0	7
0	4	6	6	6	7	0	6	6	9

Adım 5: Rakamların tekrar iki basamaklı sayılar şeklinde gruplandırılması

3787150011148299221116001678298002171599410522001982997265716768669955
110621058299657167070466670669

37-87-15-00-11-14-82-99-22-11-16-00-16-78-29-80-02-17-15-99-41-05-22-00-19-82-
99-72-65-71-67-68-66-99-55-11-06-21-05-82-99-65-71-67-07-04-66-67-06-69

Adım 6: Elde edilen sayıların karakterlere çevrilmesi

Gerçek Metin: E-mail: sinan@x.com Hesap: 817342 Şifre: 173gd23f5

Örnek Algoritma 6 (Encryption):

Şifrelenecek Metin: E-mail: sinan@x.com Hesap: 817342 Şifre: 173gd23f5

Anahtar: DA14 = 36-32-65-68

Adım 1: Karakterlerin iki basamaklı sayılarla ifade edilmesi

37-87-15-00-11-14-82-99-22-11-16-00-16-78-29-80-02-17-15-99-41-05-22-00-19-82-99-72-65-71-67-68-66-99-55-11-06-21-05-82-99-65-71-67-07-04-66-67-06-69

Adım 2: İki basamaklı sayıların birleştirilmesi

3787150011148299221116001678298002171599410522001982997265716768669955
110621058299657167070466670669

Adım 3: Anahtara ait sayı dizisinde sıfır varsa bir olarak değiştirilir. Şifrelenecek metne ait sayı dizisinden sırası ile ve her seferinde yeniden saymak şartıyla sıra numarası anahtardaki rakama eşit olan sayılar yeni bir dizi oluşturacak şekilde diziden çıkarılır.

Sayı Dizisi:

3787150011148299221116001678298002171599410522001982997265716768669955
110621058299657167070466670669

Çıkarılacak sayı: 3.

Yeni Dizi: 8

Sayı Dizisi:

3771500111482992211160016782980021715994105220019829972657167686699551
10621058299657167070466670669

Çıkarılacak sayı: 6.

Yeni Dizi: 80

Sayı Dizisi:

3771501114829922111600167829800217159941052200198299726571676866995511
0621058299657167070466670669

Çıkarılacak sayı: 3.

Yeni Dizi: 807

Sayı Dizisi:

3715011148299221116001678298002171599410522001982997265716768669955110
621058299657167070466670669

Çıkarılacak sayı: 2.

Yeni Dizi: 8077

Sayı Dizisi:

3150111482992211160016782980021715994105220019829972657167686699551106
21058299657167070466670669

Çıkarılacak sayı: 6.

Yeni Dizi: 80771

Sayı Dizisi:

3150114829922111600167829800217159941052200198299726571676866995511062
1058299657167070466670669

Çıkarılacak sayı: 5.

Yeni Dizi: 807711

Sayı Dizisi:

3150148299221116001678298002171599410522001982997265716768669955110621
058299657167070466670669

Çıkarılacak sayı: 6.

Yeni Dizi: 8077114

Sayı Dizisi:

3150182992211160016782980021715994105220019829972657167686699551106210
58299657167070466670669

Çıkarılacak sayı: 8.

Yeni Dizi: 80771149

Bu işlemler dizideki tüm sayılar yeni diziye aktarılana kadar sürdürülürse:

8077114952012210869161881901207925071450129191272900561691286691658760
185519995601227046767660967630

Adım 4: Rakamların tekrar iki basamaklı sayılar şeklinde gruplandırılması

80-77-11-49-52-01-22-10-86-91-61-88-19-01-20-79-25-07-14-50-12-91-91-27-29-00-
56-16-91-28-66-91-65-87-60-18-55-19-99-56-01-22-70-46-76-76-60-96-76-30

Adım 5: Elde edilen sayıların karakterlere çevrilmesi

Şifreli Metin: .7iOIbsı+^X*pbq€uglÖj^^vxaTn^1-WöŞp~Tbs6L%%W'%y

Örnek Algoritma 6 (Decryption):

Şifreli metni çözmek için uygulanacak adımlar ise şunlardır:

Adım 1: Karakterlerin iki basamaklı sayılarla ifade edilmesi

80-77-11-49-52-01-22-10-86-91-61-88-19-01-20-79-25-07-14-50-12-91-91-27-29-00-
56-16-91-28-66-91-65-87-60-18-55-19-99-56-01-22-70-46-76-76-60-96-76-30

Adım 2: İki basamaklı sayıların birleştirilmesi

8077114952012210869161881901207925071450129191272900561691286691658760
185519995601227046767660967630

Adım 3: Anahtara ait sayı dizisinde sıfır varsa bir olarak değiştirilir. Şifreli metne ait sayı dizisindeki rakamlar yeni bir diziye anahtarda kendisine karşılık gelen rakam sayısınınca boşluk bırakılarak yerleştirilir.

Sayı Dizisi:

8077114952012210869161881901207925071450129191272900561691286691658760
185519995601227046767660967630

Çıkarılacak sayı: 8

Sıra Numarası: 3

Yeni Dizi:

1	2	3	4	5	6	7	8
							8

Sayı Dizisi:

0771149520122108691618819012079250714501291912729005616912866916587601
85519995601227046767660967630

Çıkarılacak sayı: 0

Sıra Numarası: 6

Yeni Dizi:

1	2		3	4	5	6	7	8
		8				0		

Sayı Dizisi:

771149520122108691618819012079250714501291912729005616912866

91658760185519995601227046767660967630

Çıkarılacak sayı: 7

Sıra Numarası: 3

Yeni Dizi:

1	2		3	4	5		6	7	8
		8	7			0			

Sayı Dizisi:

7114952012210869161881901207925071450129191272900561691286691658760185

519995601227046767660967630

Çıkarılacak sayı: 7

Sıra Numarası: 2

Yeni Dizi:

1	2			3	4		5	6	7	8
	7	8	7			0				

Sayı Dizisi:

1149520122108691618819012079250714501291912729005616912866916587601855

19995601227046767660967630

Çıkarılacak sayı: 1

Sıra Numarası: 6

Yeni Dizi:

1				2	3		4	5	6	7	8
	7	8	7			0			1		

Sayı Dizisi:

1495201221086916188190120792507145012919127290056169128669165876018551
9995601227046767660967630

Çıkarılacak sayı: 1

Sıra Numarası: 5

Yeni Dizi:

1				2	3		4	5		6	7	8
	7	8	7			0		1	1			

Sayı Dizisi:

4952012210869161881901207925071450129191272900561691286691658760185519
995601227046767660967630

Çıkarılacak sayı: 4

Sıra Numarası: 6

Yeni Dizi:

1				2	3		4		5	6	7	8
	7	8	7			0		1	1	4		

Sayı Dizisi:

9520122108691618819012079250714501291912729005616912866916587601855199
95601227046767660967630

Çıkarılacak sayı: 9

Sıra Numarası: 8

Yeni Dizi:

1				2	3		4		5		6	7	8
	7	8	7			0		1	1	4			9

Bu işlemler dizideki tüm sayılar yeni diziye aktarılanaya kadar sürdürülürse:

3787150011148299221116001678298002171599410522001982997265716768669955
110621058299657167070466670669

Adım 4: Rakamların tekrar iki basamaklı sayılar şeklinde gruplandırılması

3787150011148299221116001678298002171599410522001982997265716768669955
110621058299657167070466670669

37-87-15-00-11-14-82-99-22-11-16-00-16-78-29-80-02-17-15-99-41-05-22-00-19-82-
99-72-65-71-67-68-66-99-55-11-06-21-05-82-99-65-71-67-07-04-66-67-06-69

Adım 5: Elde edilen sayıların karakterlere çevrilmesi

Gerçek Metin: E-mail: sinan@x.com Hesap: 817342 Şifre: 173gd23f5

Örnek Algoritma 7 (Encryption):

Şifrelenecek Metin:

E-mail: sinan@x.com Hesap: 817342 Şifre: 173gd23f5

Anahtar: DA14 = 36-32-65-68

Adım 1: Karakterlerin iki basamaklı sayılarla ifade edilmesi

37-87-15-00-11-14-82-99-22-11-16-00-16-78-29-80-02-17-15-99-41-05-22-00-19-82-
99-72-65-71-67-68-66-99-55-11-06-21-05-82-99-65-71-67-07-04-66-67-06-69

Adım 2: İki basamaklı sayıların birleştirilmesi

3787150011148299221116001678298002171599410522001982997265716768669955
110621058299657167070466670669

Adım 3: Sayı dizisinin $n \times n$ matris olarak yazılması $n = 10$

3	7	8	7	1	5	0	0	1	1
1	4	8	2	9	9	2	2	1	1
1	6	0	0	1	6	7	8	2	9
8	0	0	2	1	7	1	5	9	9
4	1	0	5	2	2	0	0	1	9
8	2	9	9	7	2	6	5	7	1
6	7	6	8	6	6	9	9	5	5
1	1	0	6	2	1	0	5	8	2
9	9	6	5	7	1	6	7	0	7
0	4	6	6	6	7	0	6	6	9

Adım 4:

1- Anahtara ait sayı dizisinde sıfır varsa bir olarak değiştirilir.

2- Sırası ile ve her seferinde yeniden saymak şartıyla sıra numarası anahtardaki rakama eşit olan sütunlar yeni bir matris oluşturacak şekilde matrsten çıkarılır.

Çıkarılacak Sütun: 3.

1	2	3	4	5	6	7	8	9	10	Yeni Matris:
3	7	8	7	1	5	0	0	1	1	8
1	4	8	2	9	9	2	2	1	1	8
1	6	0	0	1	6	7	8	2	9	0
8	0	0	2	1	7	1	5	9	9	0
4	1	0	5	2	2	0	0	1	9	0
8	2	9	9	7	2	6	5	7	1	9
6	7	6	8	6	6	9	9	5	5	6
1	1	0	6	2	1	0	5	8	2	0
9	9	6	5	7	1	6	7	0	7	6
0	4	6	6	6	7	0	6	6	9	6

Çıkarılacak Sütun: 6.

1	2	3	4	5	6	7	8	9	Yeni Matris:
3	7	7	1	5	0	0	1	1	8 0
1	4	2	9	9	2	2	1	1	8 2
1	6	0	1	6	7	8	2	9	0 7
8	0	2	1	7	1	5	9	9	0 1
4	1	5	2	2	0	0	1	9	0 0
8	2	9	7	2	6	5	7	1	9 6
6	7	8	6	6	9	9	5	5	6 9
1	1	6	2	1	0	5	8	2	0 0
9	9	5	7	1	6	7	0	7	6 6
0	4	6	6	7	0	6	6	9	6 0

Çıkarılacak Sütun: 3.

1	2	3	4	5	6	7	8	Yeni Matris:
3	7	7	1	5	0	1	1	8 0 7
1	4	2	9	9	2	1	1	8 2 2
1	6	0	1	6	8	2	9	0 7 0
8	0	2	1	7	5	9	9	0 1 2
4	1	5	2	2	0	1	9	0 0 5
8	2	9	7	2	5	7	1	9 6 9
6	7	8	6	6	9	5	5	6 9 8
1	1	6	2	1	5	8	2	0 0 6
9	9	5	7	1	7	0	7	6 6 5

0 4 6 6 7 6 6 9

6 0 6

Çıkarılacak Sütun: 2.

1	2	3	4	5	6	7
3	7	1	5	0	1	1
1	4	9	9	2	1	1
1	6	1	6	8	2	9
8	0	1	7	5	9	9
4	1	2	2	0	1	9
8	2	7	2	5	7	1
6	7	6	6	9	5	5
1	1	2	1	5	8	2
9	9	7	1	7	0	7
0	4	6	7	6	6	9

Yeni Matris:

8	0	7	7
8	2	2	4
0	7	0	6
0	1	2	0
0	0	5	1
9	6	9	2
6	9	8	7
0	0	6	1
6	6	5	9
6	0	6	4

Çıkarılacak Sütun: 6.

1	2	3	4	5	6
3	1	5	0	1	1
1	9	9	2	1	1
1	1	6	8	2	9
8	1	7	5	9	9
4	2	2	0	1	9
8	7	2	5	7	1
6	6	6	9	5	5
1	2	1	5	8	2
9	7	1	7	0	7
0	6	7	6	6	9

Yeni Matris:

8	0	7	7	1
8	2	2	4	1
0	7	0	6	9
0	1	2	0	9
0	0	5	1	9
9	6	9	2	1
6	9	8	7	5
0	0	6	1	2
6	6	5	9	7
6	0	6	4	9

Çıkarılacak Sütun: 5.

1	2	3	4	5
3	1	5	0	1
1	9	9	2	1
1	1	6	8	2
8	1	7	5	9
4	2	2	0	1
8	7	2	5	7
6	6	6	9	5
1	2	1	5	8
9	7	1	7	0
0	6	7	6	6

Yeni Matris:

8	0	7	7	1	1
8	2	2	4	1	1
0	7	0	6	9	2
0	1	2	0	9	9
0	0	5	1	9	1
9	6	9	2	1	7
6	9	8	7	5	5
0	0	6	1	2	8
6	6	5	9	7	0
6	0	6	4	9	6

Çıkarılacak Sütun: 2. “ $6 \equiv 2 \pmod{4}$ (4 Sütun kaldığı için)”

1	2	3	4
3	1	5	0
1	9	9	2
1	1	6	8
8	1	7	5
4	2	2	0
8	7	2	5
6	6	6	9
1	2	1	5
9	7	1	7
0	6	7	6

Yeni Matris:

8	0	7	7	1	1	1
8	2	2	4	1	1	9
0	7	0	6	9	2	1
0	1	2	0	9	9	1
0	0	5	1	9	1	2
9	6	9	2	1	7	7
6	9	8	7	5	5	6
0	0	6	1	2	8	2
6	6	5	9	7	0	7
6	0	6	4	9	6	6

Çıkarılacak Sütun: 2. “ $8 \equiv 2 \pmod{3}$ (3 Sütun kaldığı için)”

1	2	3
3	5	0
1	9	2
1	6	8
8	7	5
4	2	0
8	2	5
6	6	9
1	1	5
9	1	7
0	7	6

Yeni Matris:

8	0	7	7	1	1	1	5
8	2	2	4	1	1	9	9
0	7	0	6	9	2	1	6
0	1	2	0	9	9	1	7
0	0	5	1	9	1	2	2
9	6	9	2	1	7	7	2
6	9	8	7	5	5	6	6
0	0	6	1	2	8	2	1
6	6	5	9	7	0	7	1
6	0	6	4	9	6	6	7

Çıkarılacak Sütun: 1. “ $3 \equiv 1 \pmod{2}$ (2 Sütun kaldığı için)”

1	2
3	0
1	2
1	8
8	5
4	0
8	5
6	9
1	5
9	7
0	6

Yeni Matris:

8	0	7	7	1	1	1	5	3
8	2	2	4	1	1	9	9	1
0	7	0	6	9	2	1	6	1
0	1	2	0	9	9	1	7	8
0	0	5	1	9	1	2	2	4
9	6	9	2	1	7	7	2	8
6	9	8	7	5	5	6	6	6
0	0	6	1	2	8	2	1	1
6	6	5	9	7	0	7	1	9
6	0	6	4	9	6	6	7	0

Kalan tek sütun en sona alınarak işlem tamamlanır.

Yeni Matris:

8	0	7	7	1	1	1	5	3	0
8	2	2	4	1	1	9	9	1	2
0	7	0	6	9	2	1	6	1	8
0	1	2	0	9	9	1	7	8	5
0	0	5	1	9	1	2	2	4	0
9	6	9	2	1	7	7	2	8	5
6	9	8	7	5	5	6	6	6	9
0	0	6	1	2	8	2	1	1	5
6	6	5	9	7	0	7	1	9	7
6	0	6	4	9	6	6	7	0	6

Aynı işlemler satırlar için de yapılırsa:

Yeni Matris:

0	7	0	6	9	2	1	6	1	8
6	9	8	7	5	5	6	6	6	9
0	1	2	0	9	9	1	7	8	5
8	2	2	4	1	1	9	9	1	2
6	0	6	4	9	6	6	7	0	6
6	6	5	9	7	0	7	1	9	7
0	0	5	1	9	1	2	2	4	0
9	6	9	2	1	7	7	2	8	5
8	0	7	7	1	1	1	5	3	0
0	0	6	1	2	8	2	1	1	5

Adım 5: Rakamların tekrar iki basamaklı sayılar şeklinde gruplandırılması

0706921618698755666901209917858224119912606496670666597071970051912240
969217728580771115300061282115

07-06-92-16-18-69-87-55-66-69-01-20-99-17-85-82-24-11-99-12-60-64-96-67-06-66-
59-70-71-97-00-51-91-22-40-96-92-17-72-85-80-77-11-15-30-00-61-28-21-15

Adım 6: Elde edilen sayıların karakterlere çevrilmesi

Şifreli Metin: gf=nö5-Ş25bq~o?:ti~jW0'3f2V67(aP^sĞ'=o8?.&imyaXwrm

Örnek Algoritma 7 (Decryption):

Şifreli metni çözmek için uygulanacak adımlar ise şunlardır:

Adım 1: Karakterlerin iki basamaklı sayılarla ifade edilmesi

07-06-92-16-18-69-87-55-66-69-01-20-99-17-85-82-24-11-99-12-60-64-96-67-06-66-59-70-71-97-00-51-91-22-40-96-92-17-72-85-80-77-11-15-30-00-61-28-21-15

Adım 2: İki basamaklı sayıların birleştirilmesi

0706921618698755666901209917858224119912606496670666597071970051912240969217728580771115300061282115

Adım 3: Sayı dizisinin $n \times n$ matris olarak yazılması $n = 10$

0	7	0	6	9	2	1	6	1	8
6	9	8	7	5	5	6	6	6	9
0	1	2	0	9	9	1	7	8	5
8	2	2	4	1	1	9	9	1	2
6	0	6	4	9	6	6	7	0	6
6	6	5	9	7	0	7	1	9	7
0	0	5	1	9	1	2	2	4	0
9	6	9	2	1	7	7	2	8	5
8	0	7	7	1	1	1	5	3	0
0	0	6	1	2	8	2	1	1	5

Adım 4:

1- Anahtara ait sayı dizisinde sıfır varsa bir olarak değiştirilir.

2- Şifreli metne ait matristeki satırlar yeni bir matrise anahtarda kendisine karşılık gelen rakam sayısınca boş satır bırakılarak yerleştirilir

Satırın Yerleşeceği Sıra: 3.

Yeni Matris:

0	7	0	6	9	2	1	6	1	8	1										
6	9	8	7	5	5	6	6	6	9	2										
0	1	2	0	9	9	1	7	8	5	3	0	7	0	6	9	2	1	6	1	8
8	2	2	4	1	1	9	9	1	2	4										
6	0	6	4	9	6	6	7	0	6	5										
6	6	5	9	7	0	7	1	9	7	6										
0	0	5	1	9	1	2	2	4	0	7										
9	6	9	2	1	7	7	2	8	5	8										
8	0	7	7	1	1	1	5	3	0	9										
0	0	6	1	2	8	2	1	1	5	10										

Satırın Yerleşeceği Sıra: 6.

Yeni Matris:

6	9	8	7	5	5	6	6	6	9	1
---	---	---	---	---	---	---	---	---	---	---

0	1	2	0	9	9	1	7	8	5	2	8	2	2	4	1	1	9	9	1	2
		0	7	0	6	9	2	1	6	1	8									
6	0	6	4	9	6	6	7	0	6	3										
6	6	5	9	7	0	7	1	9	7	4										
0	0	5	1	9	1	2	2	4	0	5										
9	6	9	2	1	7	7	2	8	5	6	6	9	8	7	5	5	6	6	6	9
8	0	7	7	1	1	1	5	3	0	7										
0	0	6	1	2	8	2	1	1	5	8										

Satırın Yerleşeceği Sıra: 3.

Yeni Matris:

0	1	2	0	9	9	1	7	8	5	1										
8	2	2	4	1	1	9	9	1	2	2	6	0	6	4	9	6	6	7	0	6
		0	7	0	6	9	2	1	6	1	8									
6	6	5	9	7	0	7	1	9	7	3	0	1	2	0	9	9	1	7	8	5
0	0	5	1	9	1	2	2	4	0	4										
9	6	9	2	1	7	7	2	8	5	5	8	0	7	7	1	1	1	5	3	0
		6	9	8	7	5	5	6	6	6	9									
0	0	6	1	2	8	2	1	1	5	6										

Satırın Yerleşeceği Sıra: 2.

Yeni Matris:

8	2	2	4	1	1	9	9	1	2	1										
6	0	6	4	9	6	6	7	0	6	2	8	2	2	4	1	1	9	9	1	2
6	6	5	9	7	0	7	1	9	7	0	7	0	6	9	2	1	6	1	8	
0	0	5	1	9	1	2	2	4	0	0	1	2	0	9	9	1	7	8	5	
9	6	9	2	1	7	7	2	8	5	3										
8	0	7	7	1	1	1	5	3	0	4										
0	0	6	1	2	8	2	1	1	5	6	9	8	7	5	5	6	6	6	9	

Satırın Yerleşeceği Sıra: 6.

Yeni Matris:

6	0	6	4	9	6	6	7	0	6	1										
6	6	5	9	7	0	7	1	9	7	8	2	2	4	1	1	9	9	1	2	
0	0	5	1	9	1	2	2	4	0	0	7	0	6	9	2	1	6	1	8	
9	6	9	2	1	7	7	2	8	5	0	1	2	0	9	9	1	7	8	5	
8	0	7	7	1	1	1	5	3	0	2										
0	0	6	1	2	8	2	1	1	5	3										
										6	9	8	7	5	5	6	6	6	9	
										4										
										5										
										6	6	0	6	4	9	6	6	7	0	6

Satırın Yerleşeceği Sıra: 5.

Yeni Matris:

6	6	5	9	7	0	7	1	9	7	1										
0	0	5	1	9	1	2	2	4	0		8	2	2	4	1	1	9	9	1	2
9	6	9	2	1	7	7	2	8	5		0	7	0	6	9	2	1	6	1	8
8	0	7	7	1	1	1	5	3	0		0	1	2	0	9	9	1	7	8	5
0	0	6	1	2	8	2	1	1	5	2										
										3										
											6	9	8	7	5	5	6	6	6	9
										4										
										5	6	6	5	9	7	0	7	1	9	7
											6	0	6	4	9	6	6	7	0	6

Satırın Yerleşeceği Sıra: 2. " $6 \equiv 2 \pmod{4}$ (4 Satır kaldığı için)"

Yeni Matris:

0	0	5	1	9	1	2	2	4	0	1										
9	6	9	2	1	7	7	2	8	5		8	2	2	4	1	1	9	9	1	2
8	0	7	7	1	1	1	5	3	0		0	7	0	6	9	2	1	6	1	8
0	0	6	1	2	8	2	1	1	5		0	1	2	0	9	9	1	7	8	5
										2	0	0	5	1	9	1	2	2	4	0
										3										
											6	9	8	7	5	5	6	6	6	9
										4										
											6	6	5	9	7	0	7	1	9	7
											6	0	6	4	9	6	6	7	0	6

Satırın Yerleşeceği Sıra: 2. " $8 \equiv 2 \pmod{3}$ (3 Satır kaldığı için)"

Yeni Matris:

9	6	9	2	1	7	7	2	8	5	1										
8	0	7	7	1	1	1	5	3	0		8	2	2	4	1	1	9	9	1	2
0	0	6	1	2	8	2	1	1	5		0	7	0	6	9	2	1	6	1	8
											0	1	2	0	9	9	1	7	8	5
											0	0	5	1	9	1	2	2	4	0
										2	9	6	9	2	1	7	7	2	8	5
											6	9	8	7	5	5	6	6	6	9
										3										
											6	6	5	9	7	0	7	1	9	7
											6	0	6	4	9	6	6	7	0	6

Satırın Yerleşeceği Sıra: 1. " $3 \equiv 1 \pmod{2}$ (2 Satır kaldığı için)"

Yeni Matris:

8	0	7	7	1	1	1	5	3	0	1	8	0	7	7	1	1	1	5	3	0
0	0	6	1	2	8	2	1	1	5	8	2	2	4	1	1	9	9	1	2	
										0	7	0	6	9	2	1	6	1	8	

0	1	2	0	9	9	1	7	8	5
0	0	5	1	9	1	2	2	4	0
9	6	9	2	1	7	7	2	8	5
6	9	8	7	5	5	6	6	6	9

2

6	6	5	9	7	0	7	1	9	7
6	0	6	4	9	6	6	7	0	6

Kalan tek satır boş satıra alınarak işlem tamamlanır.

Yeni Matris:

8	0	7	7	1	1	1	5	3	0
8	2	2	4	1	1	9	9	1	2
0	7	0	6	9	2	1	6	1	8
0	1	2	0	9	9	1	7	8	5
0	0	5	1	9	1	2	2	4	0
9	6	9	2	1	7	7	2	8	5
6	9	8	7	5	5	6	6	6	9
0	0	6	1	2	8	2	1	1	5
6	6	5	9	7	0	7	1	9	7
6	0	6	4	9	6	6	7	0	6

Aynı işlemler sütunlar için de yapılırsa:

Yeni Matris:

3	7	8	7	1	5	0	0	1	1
1	4	8	2	9	9	2	2	1	1
1	6	0	0	1	6	7	8	2	9
8	0	0	2	1	7	1	5	9	9
4	1	0	5	2	2	0	0	1	9
8	2	9	9	7	2	6	5	7	1
6	7	6	8	6	6	9	9	5	5
1	1	0	6	2	1	0	5	8	2
9	9	6	5	7	1	6	7	0	7
0	4	6	6	6	7	0	6	6	9

Adım 5: Rakamların tekrar iki basamaklı sayılar şeklinde gruplandırılması

3787150011148299221116001678298002171599410522001982997265716768669955
110621058299657167070466670669

37-87-15-00-11-14-82-99-22-11-16-00-16-78-29-80-02-17-15-99-41-05-22-00-19-82-99-72-65-71-67-68-66-99-55-11-06-21-05-82-99-65-71-67-07-04-66-67-06-69

Adım 6: Elde edilen sayıların karakterlere çevrilmesi

Gerçek Metin: E-mail: sinan@x.com Hesap: 817342 Şifre: 173gd23f5

Örnek Algoritma 8 (Encryption):

Şifrelenecek Metin: E-mail: sinan@x.com Hesap: 817342 Şifre: 173gd23f5

Anahtar: DA14 = 36-32-65-68

Adım 1: Karakterlerin iki basamaklı sayılarla ifade edilmesi

37-87-15-00-11-14-82-99-22-11-16-00-16-78-29-80-02-17-15-99-41-05-22-00-19-82-99-72-65-71-67-68-66-99-55-11-06-21-05-82-99-65-71-67-07-04-66-67-06-69

Adım 2: İki basamaklı sayıların birleştirilmesi

3787150011148299221116001678298002171599410522001982997265716768669955
110621058299657167070466670669

Adım 3: Sayı dizisinin nxn matris olarak yazılması n = 10

3	7	8	7	1	5	0	0	1	1
1	4	8	2	9	9	2	2	1	1
1	6	0	0	1	6	7	8	2	9
8	0	0	2	1	7	1	5	9	9
4	1	0	5	2	2	0	0	1	9
8	2	9	9	7	2	6	5	7	1
6	7	6	8	6	6	9	9	5	5
1	1	0	6	2	1	0	5	8	2
9	9	6	5	7	1	6	7	0	7
0	4	6	6	6	7	0	6	6	9

Adım 4:

1- Anahtar önce sütun değeri olarak, daha sonra kaldığı yerden satır değeri olarak yazılır. Anahtardaki rakamlar bitince yeniden başlanacaktır.

Değerler	3	6	3	2	6	5	6	8	3	6
3	3	7	8	7	1	5	0	0	1	1
2	1	4	8	2	9	9	2	2	1	1
6	1	6	0	0	1	6	7	8	2	9

5	8	0	0	2	1	7	1	5	9	9
6	4	1	0	5	2	2	0	0	1	9
8	8	2	9	9	7	2	6	5	7	1
3	6	7	6	8	6	6	9	9	5	5
6	1	1	0	6	2	1	0	5	8	2
3	9	9	6	5	7	1	6	7	0	7
2	0	4	6	6	6	7	0	6	6	9

2- Anahtarın ilk rakamı tek sayı ise önce sütunlar, çift sayı ise önce satırlar kaydırılacaktır. (3) tek sayı olduğundan her sütun kendisine karşılık gelen anahtar değeri kadar aşağıya dairesel olarak kaydırılır.

Değerler	3	6	3	2	6	5	6	8	3	6
3	1	1	0	5	2	2	0	8	8	9
2	9	2	6	6	7	6	6	5	0	1
6	0	7	6	7	6	1	9	0	6	5
5	3	1	8	2	2	1	0	5	1	2
6	1	9	8	0	7	7	6	9	1	7
8	1	4	0	2	6	5	0	5	2	9
3	8	7	0	5	1	9	0	7	9	1
6	4	4	0	9	9	6	2	6	1	1
3	8	6	9	8	1	7	7	0	7	9
2	6	0	6	6	1	2	1	2	5	9

3- Her satır kendisine karşılık gelen anahtar değeri kadar sağa dairesel olarak kaydırılır.

8	8	9	1	1	0	5	2	2	0
0	1	9	2	6	6	7	6	6	5
6	1	9	0	6	5	0	7	6	7
1	0	5	1	2	3	1	8	2	2
7	7	6	9	1	7	1	9	8	0
0	2	6	5	0	5	2	9	1	4
7	9	1	8	7	0	5	1	9	0
9	6	2	6	1	1	4	4	0	9
0	7	9	8	6	9	8	1	7	7
5	9	6	0	6	6	1	2	1	2

Adım 5: Rakamların tekrar iki basamaklı sayılar şeklinde gruplandırılması

8891105220019266766561906507671051231822776917198002650529147918705190
962611440907986981775960661212

88-91-10-52-20-01-92-66-76-65-61-90-65-07-67-10-51-23-18-22-77-69-17-19-80-02-
65-05-29-14-79-18-70-51-90-96-26-11-44-09-07-98-69-81-77-59-60-66-12-12

Adım 6: Elde edilen sayıların karakterlere çevrilmesi

Şifreli Metin: *^ıQqb=2%1X\lg3ıPşös&5op.c1exl€ö6P\üiJhg)5,&VW2jj

Örnek Algoritma 8 (Decryption):

Şifreli metni çözmek için uygulanacak adımlar ise şunlardır:

Adım 1: Karakterlerin iki basamaklı sayılarla ifade edilmesi

88-91-10-52-20-01-92-66-76-65-61-90-65-07-67-10-51-23-18-22-77-69-17-19-80-02-
65-05-29-14-79-18-70-51-90-96-26-11-44-09-07-98-69-81-77-59-60-66-12-12

Adım 2: İki basamaklı sayıların birleştirilmesi

8891105220019266766561906507671051231822776917198002650529147918705190
962611440907986981775960661212

Adım 3: Sayı dizisinin $n \times n$ matris olarak yazılması $n = 10$

8	8	9	1	1	0	5	2	2	0
0	1	9	2	6	6	7	6	6	5
6	1	9	0	6	5	0	7	6	7
1	0	5	1	2	3	1	8	2	2
7	7	6	9	1	7	1	9	8	0
0	2	6	5	0	5	2	9	1	4
7	9	1	8	7	0	5	1	9	0
9	6	2	6	1	1	4	4	0	9
0	7	9	8	6	9	8	1	7	7
5	9	6	0	6	6	1	2	1	2

Adım 4:

1- Anahtardaki rakamlar satır ve sütun sayısından çıkarılır.

10	10	10	10	10	10	10	10	10	10
-	3	6	3	2	6	5	6	8	
=	7	4	7	8	4	5	4	2	

2- Anahtar önce sütun değeri olarak, daha sonra kaldığı yerden satır değeri olarak yazılır. Anahtardaki rakamlar bitince yeniden başlanacaktır.

Değerler	7	4	7	8	4	5	4	2	7	4
7	8	8	9	1	1	0	5	2	2	0
8	0	1	9	2	6	6	7	6	6	5
4	6	1	9	0	6	5	0	7	6	7
5	1	0	5	1	2	3	1	8	2	2
4	7	7	6	9	1	7	1	9	8	0
2	0	2	6	5	0	5	2	9	1	4
7	7	9	1	8	7	0	5	1	9	0
4	9	6	2	6	1	1	4	4	0	9
7	0	7	9	8	6	9	8	1	7	7
8	5	9	6	0	6	6	1	2	1	2

3- Anahtarın ilk rakamı (3) tek olduğu için şifreleme sütunlardan başlamıştı. Şifre çözerken ise önce satırlardan başlanacaktır. Her satır kendisine karşılık gelen anahtar değeri kadar sağa dairesel olarak kaydırılır.

Değerler	7	4	7	8	4	5	4	2	7	4
7	1	1	0	5	2	2	0	8	8	9
8	9	2	6	6	7	6	6	5	0	1
4	0	7	6	7	6	1	9	0	6	5
5	3	1	8	2	2	1	0	5	1	2
4	1	9	8	0	7	7	6	9	1	7
2	1	4	0	2	6	5	0	5	2	9
7	8	7	0	5	1	9	0	7	9	1
4	4	4	0	9	9	6	2	6	1	1
7	8	6	9	8	1	7	7	0	7	9
8	6	0	6	6	1	2	1	2	5	9

4- Her sütun kendisine karşılık gelen anahtar değeri kadar aşağıya dairesel olarak kaydırılır.

3	7	8	7	1	5	0	0	1	1
1	4	8	2	9	9	2	2	1	1
1	6	0	0	1	6	7	8	2	9
8	0	0	2	1	7	1	5	9	9
4	1	0	5	2	2	0	0	1	9
8	2	9	9	7	2	6	5	7	1
6	7	6	8	6	6	9	9	5	5
1	1	0	6	2	1	0	5	8	2
9	9	6	5	7	1	6	7	0	7
0	4	6	6	6	7	0	6	6	9

Adım 5: Rakamların tekrar iki basamaklı sayılar şeklinde gruplandırılması

3787150011148299221116001678298002171599410522001982997265716768669955
110621058299657167070466670669

37-87-15-00-11-14-82-99-22-11-16-00-16-78-29-80-02-17-15-99-41-05-22-00-19-82-
99-72-65-71-67-68-66-99-55-11-06-21-05-82-99-65-71-67-07-04-66-67-06-69

Adım 6: Elde edilen sayıların karakterlere çevrilmesi

Gerçek Metin: E-mail: sinan@x.com Hesap: 817342 Şifre: 173gd23f5

3.6.2. Çok Anahtarlı Modeller

SIS kullanılacak anahtar sayısı konusunda oldukça esnek bir tekniktir. Ancak, çok fazla anahtar kullanmak işlem kalabalığı dolayısıyla zaman kaybı, anahtarların unutulma riskinin artması, kullanışlılığın azalması gibi etkilerin ortaya çıkmasına neden olabilir. Ayrıca, örneğin “1476” ve “2543” gibi iki anahtarın algoritma içerisinde farklı işlemlere sahip olsalar bile “14762543” şeklinde yazılması ve şifrelemede işlevlerin iki blok halinde tanımlanması halinde yine bir anahtar sayılabileceği de göz önünde bulundurulmalıdır. Bu yüzden bir algoritmanın çok anahtarlı olabilmesi için, zaman kaybı ve risk artışına yol açmaması, kullanışlı olması gibi şartların yanı sıra, anahtarların işlevlerinin veya kullanılma şartlarının birbirlerinden kesin olarak ayrı olması şartını da aramak uygun olacaktır. Birden fazla anahtarın kullanılması aşağıdaki şekillerde olabilir.

- 1- Birden fazla anahtar kullanılması bazen şifrelemenin kullanılacağı iletişimin yapısına bağlı olarak zorunlu hale gelebilir. Bu tür durumlarda şifreleme algoritması tek anahtarlı olabilir. Bu tek anahtar birden fazla anahtarın belirli bir sistemle birleştirilmesi sonucu elde edilir.
- 2- Metin rasgele seçilmiş bir anahtarla şifrelenir. İkinci bir anahtar rasgele anahtarın şifreli metin içerisine yerleştirilmesi için kullanılır.
- 3- Bir anahtar değişik şekillerde kullanılabiliyorsa ikinci bir anahtar ile alternatif şekillerden bir veya birkaçı seçilebilir.

3.6.2.1. Çok Parçalı Anahtar

Şifrelemenin kullanılacağı iletişimin türü birden fazla anahtar kullanılmasını gerektiriyorsa tek bir anahtar sistematik olarak parçalara ayrılıp kullanılabilir. Aşağıda bu amaçla uygulanabilecek metotlardan birkaçı örnek olarak verilmiştir.

Örnek 1: Anahtar parçaların arka arkaya birleştirilmesi ile elde edilir.

1. Parça: 25687

2. Parça: 41952

Anahtar: 2568741952

Örnek 2: Parçalardan sırası ile birer karakter alınarak anahtar bulunur.

1. Parça: 2 5 6 8 7

2. Parça: 4 1 9 5 2

Anahtar: 2451698572

Örnek 3: Parçalardaki karakterler toplanarak anahtar elde edilir.

1. Parça: 2568752413

2. Parça: 4195239611

$$2 + 4 \equiv 6 \pmod{10}, \quad 5 + 1 \equiv 6 \pmod{10}, \quad 6 + 9 \equiv 5 \pmod{10}, \quad 8 + 5 \equiv 3 \pmod{10},$$

$$7 + 2 \equiv 9 \pmod{10}$$

$$5 + 3 \equiv 8 \pmod{10}, \quad 2 + 9 \equiv 1 \pmod{10}, \quad 4 + 6 \equiv 0 \pmod{10}, \quad 1 + 1 \equiv 2 \pmod{10},$$

$$3 + 1 \equiv 4 \pmod{10}$$

Anahtar: 6653981024

3.6.2.2. Rasgele Anahtar

Aynı metin aynı anahtarla birkaç kez şifrelendiğinde elde edilecek şifreli metin hep aynı olacaktır. Bu durumun ortadan kalkması için rasgele seçilen ve her şifrelemede değişecek bir anahtar kullanılabilir. Kullanılacak rasgele anahtarın şifreli metinle birlikte gönderilmesi durumunda güvenlik açısından şifreli metin içerisine gizlenmesi gerekir. Bu gizleme işi sabit bir anahtar kullanılarak yapılırsa iki anahtarlı bir model kurulmuş olur.

Şifrelenecek Metin:

E-mail: sinan@x.com Hesap: 817342 Şifre: 173gd23f5

Anahtar: DA14 = 36-32-65-68 = 36326568

Bu metni (Örnek Algoritma 8)'i kullanarak iki kere şifreleyelim. Şifrelemelerde kullanılacak rasgele anahtarların uzunluğu sabit anahtarın uzunluğuna eşit olarak belirlenebilir.

1. Şifreleme:

Rasgele Anahtar: 65982145

Şifreleme sonucu elde edilen sayı dizisi:

0696166967261000176860095270721617206009965901091468982111137257481174
895715765828615101299079262592

Rasgele anahtar şifreli metne yerleştirilirken izlenecek metot:

Karakter	Sıra
6	3
5	3+6=9
9	9+3=12
8	12+2=14
2	14+6=20
1	20+5=25
4	25+6=31
5	31+8=39

Yeni Sayı Dizisi:

0669616659697826100201761860094527072156172060099659010914689821111372
57481174895715765828615101299079262592

Şifreli Metin:

f5X2V5@üıcb%öWhKvgrToqWh'Vbhl4)rik8UNi#/Um%ÜwXPbx€üu=

2. Şifreleme:

Rasgele Anahtar: 42562327

Şifreleme sonucu elde edilen sayı dizisi:

9621769167875669020610151978516971131862590001117899060026812921002470
571255187919966764069248072625

Rasgele anahtar şifreli metne yerleştirilirken izlenecek metot:

Karakter	Sıra
4	3
2	3+6=9
5	9+3=12
6	12+2=14
2	14+6=20
3	20+5=25
2	25+6=31
7	31+8=39

Yeni Sayı Dizisi:

9642176921657687566290203610152197851679711318625900011178990600268129
21002470571255187919966764069248072625

Şifreli Metin:

'To5r1%-TY\qDımr(?n€7köYVabi@~faü,xrat6UjŞöep'30f=Ngüu

Örnekte görüldüğü gibi sabit anahtar yalnızca şifreli metne ait sayı dizisi içerisinde şifrelemede kullanılan anahtarın yerini belirlemekte ve şifrelemede kullanılan anahtar her seferinde değiştiğinden aynı metin her şifrelendiğinde farklı şifreli metinler ortaya çıkmaktadır.

3.6.2.3. Seçici Anahtar

Bir şifreleme algoritmasında anahtarın kullanımı için farklı alternatif şekiller varsa, bu alternatiflerden hangisinin veya hangilerinin seçildiğini belirlemek gerekir. Bunun için izlenebilecek iki yol vardır:

1- Bir metot sabit tutulur ve her zaman o seçilir.

2- Seçilecek metot ikinci bir anahtarla belirlenir.

(Örnek Algoritma 6)'yı ele alalım: Anahtar satır ve sütun değeri olarak yerleştirilirken şu seçenekler söz konusudur:

Şifrelenecek Metin:

E-mail: sinan@x.com Hesap: 817342 Şifre: 173gd23f5

Anahtar: DA14 = 36-32-65-68 = 36326568

1- Anahtar yerleştirilirken sütundan veya satırdan başlanabilir.

Önce Sütun

	3	6	3	2	6	5	6	8	3	6
3	3	7	8	7	1	5	0	0	1	1
2	1	4	8	2	9	9	2	2	1	1
6	1	6	0	0	1	6	7	8	2	9
5	8	0	0	2	1	7	1	5	9	9
6	4	1	0	5	2	2	0	0	1	9
8	8	2	9	9	7	2	6	5	7	1
3	6	7	6	8	6	6	9	9	5	5
6	1	1	0	6	2	1	0	5	8	2
3	9	9	6	5	7	1	6	7	0	7
2	0	4	6	6	6	7	0	6	6	9

Önce Satır

	3	2	6	5	6	8	3	6	3	2
3	3	7	8	7	1	5	0	0	1	1
6	1	4	8	2	9	9	2	2	1	1
3	1	6	0	0	1	6	7	8	2	9
2	8	0	0	2	1	7	1	5	9	9
6	4	1	0	5	2	2	0	0	1	9
5	8	2	9	9	7	2	6	5	7	1
6	6	7	6	8	6	6	9	9	5	5
8	1	1	0	6	2	1	0	5	8	2
3	9	9	6	5	7	1	6	7	0	7
6	0	4	6	6	6	7	0	6	6	9

2- İkinci olarak yerleştirilecek alan işlem ilk alanda kaldığı yerden devam ederek veya baştan başlayarak yapılabilir.

Satırlar kaldığı yerden devam

	3	6	3	2	6	5	6	8	3	6
3	3	7	8	7	1	5	0	0	1	1
2	1	4	8	2	9	9	2	2	1	1
6	1	6	0	0	1	6	7	8	2	9
5	8	0	0	2	1	7	1	5	9	9

6	4	1	0	5	2	2	0	0	1	9
8	8	2	9	9	7	2	6	5	7	1
3	6	7	6	8	6	6	9	9	5	5
6	1	1	0	6	2	1	0	5	8	2
3	9	9	6	5	7	1	6	7	0	7
2	0	4	6	6	6	7	0	6	6	9

Satır yeniden başlar

	3	6	3	2	6	5	6	8	3	6
3	3	7	8	7	1	5	0	0	1	1
6	1	4	8	2	9	9	2	2	1	1
3	1	6	0	0	1	6	7	8	2	9
2	8	0	0	2	1	7	1	5	9	9
6	4	1	0	5	2	2	0	0	1	9
5	8	2	9	9	7	2	6	5	7	1
6	6	7	6	8	6	6	9	9	5	5
8	1	1	0	6	2	1	0	5	8	2
3	9	9	6	5	7	1	6	7	0	7
6	0	4	6	6	6	7	0	6	6	9

3- Yerleştirmeye anahtarın herhangi bir yerinden başlanabilir.

Birinci sayıdan başlar

	3	6	3	2	6	5	6	8	3	6
3	3	7	8	7	1	5	0	0	1	1
2	1	4	8	2	9	9	2	2	1	1
6	1	6	0	0	1	6	7	8	2	9
5	8	0	0	2	1	7	1	5	9	9
6	4	1	0	5	2	2	0	0	1	9
8	8	2	9	9	7	2	6	5	7	1
3	6	7	6	8	6	6	9	9	5	5
6	1	1	0	6	2	1	0	5	8	2
3	9	9	6	5	7	1	6	7	0	7
2	0	4	6	6	6	7	0	6	6	9

Dördüncü sayıdan başlar

	2	6	5	6	8	3	6	3	2	6
5	3	7	8	7	1	5	0	0	1	1
6	1	4	8	2	9	9	2	2	1	1
8	1	6	0	0	1	6	7	8	2	9
3	8	0	0	2	1	7	1	5	9	9

6	4	1	0	5	2	2	0	0	1	9
3	8	2	9	9	7	2	6	5	7	1
2	6	7	6	8	6	6	9	9	5	5
6	1	1	0	6	2	1	0	5	8	2
5	9	9	6	5	7	1	6	7	0	7
6	0	4	6	6	6	7	0	6	6	9

Alternatif şekilleri çoğaltmak mümkündür. Satır ve sütunun ayrı ayrı ve anahtarın herhangi bir noktasından başlayarak yerleştirildiği durumu göz önüne alalım. Satırlar 4.'den sütunlar 2.den başlayarak yerleştirilirse ikinci anahtar 42 olacak ve matris şu şekilde değerlendirilecektir:

1. Anahtar: 36326568

2. Anahtar: 42

	6	3	2	6	5	6	8	3	6	3
2	3	7	8	7	1	5	0	0	1	1
6	1	4	8	2	9	9	2	2	1	1
5	1	6	0	0	1	6	7	8	2	9
6	8	0	0	2	1	7	1	5	9	9
8	4	1	0	5	2	2	0	0	1	9
3	8	2	9	9	7	2	6	5	7	1
6	6	7	6	8	6	6	9	9	5	5
3	1	1	0	6	2	1	0	5	8	2
2	9	9	6	5	7	1	6	7	0	7
6	0	4	6	6	6	7	0	6	6	9

Satır ve sütunlar birbirini takip ederek değerlendirilecekse, örneğin 39 olarak belirlenecek ikinci anahtar şu şekilde kullanılabilir. İlk rakam tek ise sütundan, çift ise satırdan başlanır. $3+9 \equiv 4 \pmod{8}$ (Birinci anahtar sekiz karakter uzunluğunda) olduğundan değerlendirme dördüncü rakamdan başlayarak yapılır.

	2	6	5	6	8	3	6	3	2	6
5	3	7	8	7	1	5	0	0	1	1
6	1	4	8	2	9	9	2	2	1	1
8	1	6	0	0	1	6	7	8	2	9
3	8	0	0	2	1	7	1	5	9	9
6	4	1	0	5	2	2	0	0	1	9
3	8	2	9	9	7	2	6	5	7	1
2	6	7	6	8	6	6	9	9	5	5

6	1	1	0	6	2	1	0	5	8	2
5	9	9	6	5	7	1	6	7	0	7
6	0	4	6	6	6	7	0	6	6	9

3.7. SIS Kullanılarak Tasarlanmış Bir Elektronik Ödeme Sistemi

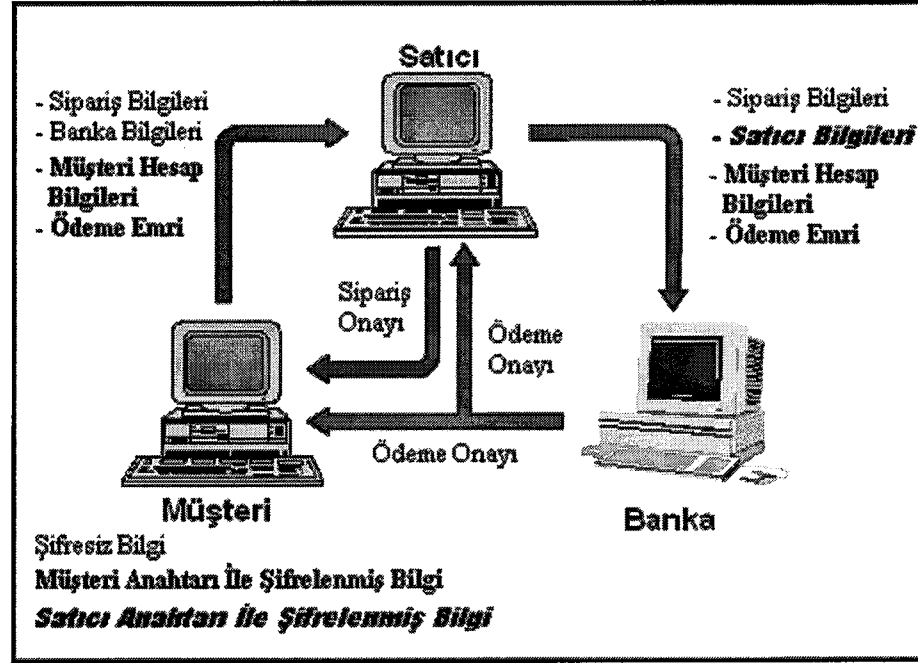
Bu bölümde mevcut ödeme sistemlerine göre daha basit bir ödeme sistemi sunulacaktır. Bu ödeme sisteminin gücü algoritmanın rasgele anahtarlı oluşundan kaynaklanmakta güvenilirliği ise banka sisteminin güvenilirliği ile doğru orantılı olarak artmaktadır. Sistem, banka dışında dışarıdan müdahalelere açık ama banka içerisinde güçlü bir doğrulama mekanizması ile bu müdahaleleri fark edebilecek bir yapıya sahiptir. Ayrıca işlemleri karmaşıktırmayacak şekilde mevcut sistemlerde kullanılan güvenlik unsurları bu sisteme de monte edilebilir.

3.7.1. Sistemin İşleyişi

Sistemin işleyişi basit olarak Şekil 3.17’de görülmektedir. Müşteri satıcıya sipariş bilgileri ile ödemeyi yapacak banka hakkındaki bilgileri şifresiz olarak, Kendi hesap bilgileri ile ödeme emrini ise kendi anahtarı ile şifreleyerek gönderir. Satıcı, müşterinin anahtarını bilmediği için yalnızca şifrelenmemiş bilgileri okuyabilecektir. Satıcı bu bilgilere ek olarak kendi hesap bilgilerini kendi anahtarı ile şifreler ve bankaya gönderir. Banka hem satıcının hem de müşterinin anahtarlarını bilen tek taraftır. Müşterinin ve satıcının şifreli bilgilerini çözen banka bilgiler tutarlı ise işleme onay verir ve bunu taraflara bildirir. Böylece alış veriş ve ödeme işlemleri tamamlanır. Sistemin işleyişi, örnek olaylarla daha ayrıntılı olarak açıklanmaya çalışılacaktır.

Örnek Olay 1.

Ahmet Kar, E-Ticaret Bankası’nda bir vadesiz mevduat hesabı vardır ve bankaya internet yolu ile işlem yapmak istediğini bildirir. Banka, Ahmet Kar’dan en az iki karakterden oluşan bir şifre belirlemesini, banka tarafından belirlenecek ve gerektiğinde değiştirilecek şifre için en az iki karakter olmak üzere bir uzunluk seçmesini ve dört rakamlı bir güvenlik şifresi değiştirme kodu ister. Ahmet Kar kendisinden istenen bilgileri şu şekilde doldurur.



Şekil 3.17. SIS Kullanılarak Tasarlanmış Bir Elektronik Ödeme Sistemi

Adı Soyadı: Ahmet Kar

Banka Hesap Numarası: 1356236589884580

Hesap Türü: Vadesiz Mevduat

Şifre: a0cd

Güvenlik Şifresi Uzunluğu:2

Güvenlik Şifresi Değiştirme Kodu:2587

E-mail: ahmetkar@ahmetkar.com

Banka Ahmet Kar'a şifre bilgilerinin e-posta adresine yine şifreli olarak gönderileceğini ve postanın eline ulaştığı andan itibaren internet yolu ile işlem yapabileceğini bildirir. Ahmet Kar'a e-posta yolu ile şu bilgiler gönderilir:

SIS Tanıtım Numarası: We2a

Güvenlik Şifresi:A3

Şifre: A3a0cd

Örnek Algoritma 9 (Encryption):

Şifrelenecek Mesaj:

SIS Tanıtım Numarası: We2a Güvenlik Şifresi:A3 Şifre: A3a0cd

Mesaj metninin uzunluğu: $n = 58$

Şifrelenecek serinin uzunluğu: $N = 58 \times 2 = 116$

Matris boyutu: $M = 11$ (11×11)

Şifrelenecek Mesaj Kodları:

54-42-54-99-56-00-16-10-24-10-15-99-48-25-15-00-21-00-22-10-82-60-05-66-00-99-39-26-27-05-16-14-11-13-99-55-11-06-21-05-22-11-82-32-67-99-55-11-06-21-05-82-32-67-00-64-02-04

$x = \{x_1, x_2, x_3, \dots, x_N\} = \{5, 4, 4, 2, 5, 4, 9, 9, 5, 6, 0, 0, 1, 6, 1, 0, 2, 4, 1, 0, 1, 5, 9, 9, 4, 8, 2, 5, 1, 5, 0, 0, 2, 1, 0, 0, 2, 2, 1, 0, 8, 2, 6, 0, 0, 5, 6, 6, 0, 0, 9, 9, 3, 9, 2, 6, 2, 7, 0, 5, 1, 6, 1, 4, 1, 1, 1, 3, 9, 9, 5, 5, 1, 1, 0, 6, 2, 1, 0, 5, 2, 2, 1, 1, 8, 2, 3, 2, 6, 7, 9, 9, 5, 5, 1, 1, 0, 6, 2, 1, 0, 5, 8, 2, 3, 2, 6, 7, 0, 0, 6, 4, 0, 2, 0, 4\}$

Sayı dizisinin matris olarak yazılması:

$$X(i,j) = x_{(M(i-1)+j)}$$

5	4	4	2	5	4	9	9	5	6	0
0	1	6	1	0	2	4	1	0	1	5
9	9	4	8	2	5	1	5	0	0	2
1	0	0	2	2	1	0	8	2	6	0
0	5	6	6	0	0	9	9	3	9	2
6	2	7	0	5	1	6	1	4	1	1
1	3	9	9	5	5	1	1	0	6	2
1	0	5	2	2	1	1	8	2	3	2
6	7	9	9	5	5	1	1	0	6	2
1	0	5	8	2	3	2	6	7	0	0
6	4	0	2	0	4	9	9	9	9	9

Anahtar:

1- Banka Hesap Numarası: $h = 16$ için $H = \{H_1, H_2, H_3, \dots, H_h\} = \{1, 3, 5, 6, 2, 3, 6, 5, 8, 9, 8, 8, 4, 5, 8, 0\}$

2- Güvenlik Değiştirme Kodu: $G = \{g_1, g_2, g_3, g_4\} = \{2, 5, 8, 7\}$

3- Rasgele Anahtar: M adet rastgele seçilmiş rakamdan oluşur. $R = \{R_1, R_2, R_3, \dots, R_M\} = \{1, 9, 7, 4, 1, 3, 0, 2, 8, 4, 2\}$

Birinci anahtar herhangi bir rakamındaki değişikliğin diğer tüm rakamları etkilemesi için yeniden düzenlenir.

$$H=\{7,7,1,5,5,1,1,7,3,3,0,8,1,9,7,2\}$$

Birinci anahtar için satır ve sütun değerleri sütundan başlayarak yerleştirilir:

$$K_i = H_{(h(i-1)+i)}$$

$$K = \{K_1, K_2, K_3, \dots, K_M\} = \{7,7,1,5,5,1,1,7,3,3,0\}$$

$$K_M = H_e \text{ iken}$$

$$L_i = H_{(e+h(i-1)+i)}$$

$$L = \{L_1, L_2, L_3, \dots, L_M\} = \{8,1,9,7,2, 7,7,1,5,5,1\}$$

Değerler	7	7	1	5	5	1	1	7	3	3	0
8	5	4	4	2	5	4	9	9	5	6	0
1	0	1	6	1	0	2	4	1	0	1	5
9	9	9	4	8	2	5	1	5	0	0	2
7	1	0	0	2	2	1	0	8	2	6	0
2	0	5	6	6	0	0	9	9	3	9	2
7	6	2	7	0	5	1	6	1	4	1	1
7	1	3	9	9	5	5	1	1	0	6	2
1	1	0	5	2	2	1	1	8	2	3	2
5	6	7	9	9	5	5	1	1	0	6	2
5	1	0	5	8	2	3	2	6	7	0	0
1	6	4	0	2	0	4	9	9	9	9	9

Matristeki her değer kendi satır ve sütun değerleri ile toplanır:

$$X1_{(i,j)} = (X_{(i,j)} + L_i + K_j) \pmod{10}$$

Değerler	7	7	1	5	5	1	1	7	3	3	0
8	0	9	3	5	8	3	8	4	6	7	8
1	8	9	8	7	6	4	6	9	4	5	6
9	5	5	4	2	6	5	1	1	2	2	1
7	5	4	8	4	4	9	8	2	2	9	6
2	5	9	3	2	3	9	3	9	4	4	5
7	3	6	4	4	9	8	3	5	6	1	1
7	5	5	9	5	1	7	3	9	1	1	7
1	4	0	3	6	1	4	4	9	5	2	3
5	5	4	2	7	9	5	1	7	9	9	5

5	8	4	7	0	5	4	8	1	7	1	7
1	4	5	2	6	2	6	2	0	4	8	0

Rasgele anahtar için satır ve sütun değerleri sütundan başlayarak yerleştirilir:

$$K_i = R_i$$

$$K = \{K_1, K_2, K_3, \dots, K_M\} = \{1, 9, 7, 4, 1, 3, 0, 2, 8, 4, 2\}$$

$$L_i = R_i$$

$$L = \{L_1, L_2, L_3, \dots, L_M\} = \{1, 9, 7, 4, 1, 3, 0, 2, 8, 4, 2\}$$

Değerler	1	9	7	4	1	3	0	2	8	4	2
1	0	9	3	5	8	3	8	4	6	7	8
9	8	9	8	7	6	4	6	9	4	5	6
7	5	5	4	2	6	5	1	1	2	2	1
4	5	4	8	4	4	9	8	2	2	9	6
1	5	9	3	2	3	9	3	9	4	4	5
3	3	6	4	4	9	8	3	5	6	1	1
0	5	5	9	5	1	7	3	9	1	1	7
2	4	0	3	6	1	4	4	9	5	2	3
8	5	4	2	7	9	5	1	7	9	9	5
4	8	4	7	0	5	4	8	1	7	1	7
2	4	5	2	6	2	6	2	0	4	8	0

Sütun Kaydırma

Sütunlar aşağıya doğru sütun değerleri kadar dairesel olarak kaydırılır.

Değerler	1	9	7	4	1	3	0	2	8	4	2
1	4	5	3	6	2	5	8	1	2	2	7
9	0	4	4	7	8	4	6	0	4	9	0
7	8	9	9	0	6	6	1	4	6	1	8
4	5	6	3	6	6	3	8	9	1	8	6
1	5	5	2	5	4	4	3	1	5	7	1
3	5	0	7	7	3	5	3	2	9	5	6
0	3	4	2	2	9	9	3	9	7	2	5
2	5	4	3	4	1	9	4	5	4	9	1
8	4	5	8	2	1	8	1	9	6	4	7
4	5	9	4	4	9	7	8	9	4	1	3
2	8	9	8	5	5	4	2	7	2	1	5

Satır Kaydırma

Satırlar sağa doğru satır değerleri kadar dairesel olarak kaydırılır.

Değerler	1	9	7	4	1	3	0	2	8	4	2
1	7	4	5	3	6	2	5	8	1	2	2
9	4	7	8	4	6	0	4	9	0	0	4
7	6	6	1	4	6	1	8	8	9	9	0
4	9	1	8	6	5	6	3	6	6	3	8
1	1	5	5	2	5	4	4	3	1	5	7
3	9	5	6	5	0	7	7	3	5	3	2
0	3	4	2	2	9	9	3	9	7	2	5
2	9	1	5	4	3	4	1	9	4	5	4
8	2	1	8	1	9	6	4	7	4	5	8
4	9	4	1	3	5	9	4	4	9	7	8
2	1	5	8	9	8	5	5	4	2	7	2

Elde edilen matris Y matrisidir. Matristeki rakamlar seri haline getirilir:

$$y_i = Y_{([i/M], i \bmod M)}$$

$$y = \{y_1, y_2, y_3, \dots, y_{M \times M}\} = \{7, 4, 5, 3, 6, 2, 5, 8, 1, 2, 2, 4, 7, 8, 4, 6, 0, 4, 9, 0, 0, 4, 6, 6, 1, 4, 6, 1, 8, 8, 9, 9, 0, 9, 1, 8, 6, 5, 6, 3, 6, 6, 3, 8, 1, 5, 5, 2, 5, 4, 4, 3, 1, 5, 7, 9, 5, 6, 5, 0, 7, 7, 3, 5, 3, 2, 3, 4, 2, 2, 9, 9, 3, 9, 7, 2, 5, 9, 1, 5, 4, 3, 4, 1, 9, 4, 5, 4, 2, 1, 8, 1, 9, 6, 4, 7, 4, 5, 8, 9, 4, 1, 3, 5, 9, 4, 4, 9, 7, 8, 1, 5, 8, 9, 8, 5, 5, 4, 2, 7, 2\}$$

İkinci anahtar kullanılarak rasgele anahtar seri içerisine yerleştirilir. İki anahtarın uzunlukları farklı ise kısa olan uzun olana tamamlanıncaya kadar ilk rakamdan başlayarak yeniden yazılır.

Karakter	Sıra
1	2
9	$2 + 5 = 7$
7	$7 + 8 = 15$
4	$15 + 7 = 22$
1	$22 + 2 = 24$
3	$24 + 5 = 29$
0	$29 + 8 = 37$
2	$37 + 7 = 44$
8	$44 + 2 = 46$
4	$46 + 5 = 51$
2	$51 + 8 = 59$

7145369258122477846044910046361461880990918268563646381552254431579565
07735323422993972591543419454218196474589413594497815898554272

Sayı dizisi ikiyeşerli gruplandırılır:

71-45-36-92-58-12-24-77-84-60-44-91-00-46-36-14-61-88-09-90-91-82-68-56-36-46-
38-15-52-25-44-31-57-95-65-07-73-53-23-42-29-93-97-25-91-54-34-19-45-42-18-19-
64-74-58-94-13-59-44-97-81-58-98-55-42-72

Tablo değerleri bulunarak şifreli metin elde edilir:

7KD=Üjt&!WJ^aLDIX*h\^:4TDLFmQuJzU_1g9RşIx<(u^SCpKIöp0#Ü>kVJ(,Ü)Şİ8

Ahmet Kar işlem yaparken tek bir uygulama dosyasından ibaret olan bir şifreleme programı kullanacak ve bu programı bankanın ilgili sayfalarından veya aynı ödeme sistemini kullanan sitelerden istediği zaman bilgisayarına indirebilecektir. Kendisine posta ile gelen şifreleri çözmek için, anahtar olarak banka hesap numarasını ve güvenlik değiştirme kodunu, yapacağı diğer işlemlerde hesap numarasını ve şifresini kullanacaktır. Güvenlik değiştirme kodunun ikinci bir işlevi de şifrenin ilk iki karakterini oluşturan güvenlik şifresini değiştirmek veya korumaktır. Ahmet Kar'a yapacağı her işlemde güvenlik değiştirme kodu sorulacaktır. Eğer doğru kodu girerse güvenlik şifresi korunur. Başka herhangi dört rakam (0000, 2588, 1234, v.b.) girerse güvenlik şifresi değiştirilecek ve yeni şifre e-posta yolu ile yine şifreli olarak kendisine gönderilecektir.

Ahmet Kar'a gelen şifreli metnin çözülmesi ise aşağıdaki gibi yapılacaktır.

Örnek Algoritma 9 (Decryption):

Çözülecek Mesaj:

7KD=Üjt&!WJ^aLDIX*h\^:4TDLFmQuJzU_1g9RşIx<(u^SCpKIöp0#Ü>kVJ(,Ü)Şİ8

Mesaj metninin uzunluğu: $n = 66$

Çözülecek serinin uzunluğu: $N = 66 \times 2 = 132$

Matris boyutu:

$$M^2 + g = N \quad (M < g \text{ iken})$$

$$M^2 + M = N \quad (M > g \text{ iken}) \quad M=11$$

Çözülecek Mesaj Kodları:

71-45-36-92-58-12-24-77-84-60-44-91-00-46-36-14-61-88-09-90-91-82-68-56-36-46-38-15-52-25-44-31-57-95-65-07-73-53-23-42-29-93-97-25-91-54-34-19-45-42-18-19-64-74-58-94-13-59-44-97-81-58-98-55-42-72

Anahtar:

1- Banka Hesap Numarası: $h=16$ için

$H=\{H_1, H_2, H_3, \dots, H_h\}=\{1, 3, 5, 6, 2, 3, 6, 5, 8, 9, 8, 8, 4, 5, 8, 0\}$

Dönüştürülürse: $H=\{7, 7, 1, 5, 5, 1, 1, 7, 3, 3, 0, 8, 1, 9, 7, 2\}$

2- Güvenlik Değiştirme Kodu: $G = \{g_1, g_2, g_3, g_4\} = \{2, 5, 8, 7\}$

3- Rasgele Anahtar: M adet rasgele seçilmiş rakamdan oluşur.

İkinci anahtar kullanılarak rasgele anahtar seri içerisinde bulunur.

Karakter	Sıra
1	2
9	$2 + 5 = 7$
7	$7 + 8 = 15$
4	$15 + 7 = 22$
1	$22 + 2 = 24$
3	$24 + 5 = 29$
0	$29 + 8 = 37$
2	$37 + 7 = 44$
8	$44 + 2 = 46$
4	$46 + 5 = 51$
2	$51 + 8 = 59$

7145369258122477846044910046361461880990918268563646381552254431579565
07735323422993972591543419454218196474589413594497815898554272

$S = \{S_1, S_2, S_3, \dots, S_M\} = \{1, 9, 7, 4, 1, 3, 0, 2, 8, 4, 2\}$

$y = \{y_1, y_2, y_3, \dots, y_N\} = \{7, 4, 5, 3, 6, 2, 5, 8, 1, 2, 2, 4, 7, 8, 4, 6, 0, 4, 9, 0, 0, 4, 6, 6, 1, 4, 6, 1, 8, 8, 9, 9, 0, 9, 1, 8, 6, 5, 6, 3, 6, 6, 3, 8, 1, 5, 5, 2, 5, 4, 4, 3, 1, 5, 7, 9, 5, 6, 5, 0, 7, 7, 3, 5, 3, 2, 3, 4, 2, 2, 9, 9, 3, 9, 7, 2, 5, 9, 1, 5, 4, 3, 4, 1, 9, 4, 5, 4, 2, 1, 8, 1, 9, 6, 4, 7, 4, 5, 8, 9, 4, 1, 3, 5, 9, 4, 4, 9, 7, 8, 1, 5, 8, 9, 8, 5, 5, 4, 2, 7, 2\}$

Sayı dizisinin matris olarak yazılması:

$$Y(i,j) = y_{(M.(i-1)+j)}$$

7	4	5	3	6	2	5	8	1	2	2
4	7	8	4	6	0	4	9	0	0	4
6	6	1	4	6	1	8	8	9	9	0
9	1	8	6	5	6	3	6	6	3	8
1	5	5	2	5	4	4	3	1	5	7
9	5	6	5	0	7	7	3	5	3	2
3	4	2	2	9	9	3	9	7	2	5
9	1	5	4	3	4	1	9	4	5	4
2	1	8	1	9	6	4	7	4	5	8
9	4	1	3	5	9	4	4	9	7	8
1	5	8	9	8	5	5	4	2	7	2

Rasgele anahtarın tüm değerleri $M=11$ 'den çıkarılır

$$R_i = M - S_i$$

$$R = \{R_1, R_2, R_3, \dots, R_M\} = \{1, 9, 7, 4, 1, 3, 0, 2, 8, 4, 2\}$$

Rasgele anahtar için satır ve sütun değerleri sütundan başlayarak yerleştirilir:

$$K_i = R_i$$

$$K = \{K_1, K_2, K_3, \dots, K_M\} = \{1, 9, 7, 4, 1, 3, 0, 2, 8, 4, 2\}$$

$$L_i = R_i$$

$$L = \{L_1, L_2, L_3, \dots, L_M\} = \{1, 9, 7, 4, 1, 3, 0, 2, 8, 4, 2\}$$

Değerler	10	2	4	7	10	8	0	9	3	7	9
10	7	4	5	3	6	2	5	8	1	2	2
2	4	7	8	4	6	0	4	9	0	0	4
4	6	6	1	4	6	1	8	8	9	9	0
7	9	1	8	6	5	6	3	6	6	3	8
10	1	5	5	2	5	4	4	3	1	5	7
8	9	5	6	5	0	7	7	3	5	3	2
0	3	4	2	2	9	9	3	9	7	2	5
9	9	1	5	4	3	4	1	9	4	5	4
3	2	1	8	1	9	6	4	7	4	5	8
7	9	4	1	3	5	9	4	4	9	7	8
9	1	5	8	9	8	5	5	4	2	7	2

Satır Kaydırma

Satırlar sağa doğru satır değerleri kadar dairesel olarak kaydırılır.

Değerler	1	9	7	4	1	3	0	2	8	4	2
----------	---	---	---	---	---	---	---	---	---	---	---

1	4	5	3	6	2	5	8	1	2	2	7
9	0	4	4	7	8	4	6	0	4	9	0
7	8	9	9	0	6	6	1	4	6	1	8
4	5	6	3	6	6	3	8	9	1	8	6
1	5	5	2	5	4	4	3	1	5	7	1
3	5	0	7	7	3	5	3	2	9	5	6
0	3	4	2	2	9	9	3	9	7	2	5
2	5	4	3	4	1	9	4	5	4	9	1
8	4	5	8	2	1	8	1	9	6	4	7
4	5	9	4	4	9	7	8	9	4	1	3
2	8	9	8	5	5	4	2	7	2	1	5

Sütun Kaydırma

Sütunlar aşağıya doğru sütun değerleri kadar dairesel olarak kaydırılır.

Değerler	1	9	7	4	1	3	0	2	8	4	2
1	0	9	3	5	8	3	8	4	6	7	8
9	8	9	8	7	6	4	6	9	4	5	6
7	5	5	4	2	6	5	1	1	2	2	1
4	5	4	8	4	4	9	8	2	2	9	6
1	5	9	3	2	3	9	3	9	4	4	5
3	3	6	4	4	9	8	3	5	6	1	1
0	5	5	9	5	1	7	3	9	1	1	7
2	4	0	3	6	1	4	4	9	5	2	3
8	5	4	2	7	9	5	1	7	9	9	5
4	8	4	7	0	5	4	8	1	7	1	7
2	4	5	2	6	2	6	2	0	4	8	0

Birinci anahtar için satır ve sütun değerleri sütundan başlayarak yerleştirilir:

$$K_i = R_{(h.(i-1)+i)}$$

$$K = \{K_1, K_2, K_3, \dots, K_M\} = \{7, 7, 1, 5, 5, 1, 1, 7, 3, 3, 0\}$$

$$K_M = H_e \text{ iken}$$

$$L_i = H_{(e+h.(i-1)+i)}$$

$$L = \{L_1, L_2, L_3, \dots, L_M\} = \{8, 1, 9, 7, 2, 7, 7, 1, 5, 5, 1\}$$

Değerler	7	7	1	5	5	1	1	7	3	3	0
8	0	9	3	5	8	3	8	4	6	7	8
1	8	9	8	7	6	4	6	9	4	5	6
9	5	5	4	2	6	5	1	1	2	2	1
7	5	4	8	4	4	9	8	2	2	9	6
2	5	9	3	2	3	9	3	9	4	4	5

7	3	6	4	4	9	8	3	5	6	1	1
7	5	5	9	5	1	7	3	9	1	1	7
1	4	0	3	6	1	4	4	9	5	2	3
5	5	4	2	7	9	5	1	7	9	9	5
5	8	4	7	0	5	4	8	1	7	1	7
1	4	5	2	6	2	6	2	0	4	8	0

Matristeki her değerdan kendi satır ve sütun değerdleri çıkarılır:

$$Y1_{(i,j)} = (Y_{(i,j)} - L_i - K_j) \pmod{10}$$

Değerler	7	7	1	5	5	1	1	7	3	3	0
8	5	4	4	2	5	4	9	9	5	6	0
1	0	1	6	1	0	2	4	1	0	1	5
9	9	9	4	8	2	5	1	5	0	0	2
7	1	0	0	2	2	1	0	8	2	6	0
2	0	5	6	6	0	0	9	9	3	9	2
7	6	2	7	0	5	1	6	1	4	1	1
7	1	3	9	9	5	5	1	1	0	6	2
1	1	0	5	2	2	1	1	8	2	3	2
5	6	7	9	9	5	5	1	1	0	6	2
5	1	0	5	8	2	3	2	6	7	0	0
1	6	4	0	2	0	4	9	9	9	9	9

Elde edilen matris X matrisidir. Matristeki rakamlar seri haline getirilir:

$$X_i = X_{([i/M], i \bmod M)}$$

Şifrelenecek Mesaj Kodları:

$x = \{x_1, x_2, x_3, \dots, x_{M \times M}\} = \{5, 4, 4, 2, 5, 4, 9, 9, 5, 6, 0, 0, 1, 6, 1, 0, 2, 4, 1, 0, 1, 5, 9, 9, 4, 8, 2, 5, 1, 5, 0, 0, 2, 1, 0, 0, 2, 2, 1, 0, 8, 2, 6, 0, 0, 5, 6, 6, 0, 0, 9, 9, 3, 9, 2, 6, 2, 7, 0, 5, 1, 6, 1, 4, 1, 1, 1, 3, 9, 9, 5, 5, 1, 1, 0, 6, 2, 1, 0, 5, 2, 2, 1, 1, 8, 2, 3, 2, 6, 7, 9, 9, 5, 5, 1, 1, 0, 6, 2, 1, 0, 5, 8, 2, 3, 2, 6, 7, 0, 0, 6, 4, 0, 2, 0, 4\}$

Sayı dizisi ikişerli gruplandırılır:

54-42-54-99-56-00-16-10-24-10-15-99-48-25-15-00-21-00-22-10-82-60-05-66-00-99-39-26-27-05-16-14-11-13-99-55-11-06-21-05-22-11-82-32-67-99-55-11-06-21-05-82-32-67-00-64-02-04

Tablo değerdleri bulunarak orjinal metin elde edilir:

SIS Tanıtım Numarası: We2a Güvenlik Şifresi:A3 Şifre: A3a0cd

Örnek Olay 2.

Ahmet Kar ev kirası olarak ev sahibinin hesabına havale yapmak istiyor. Bunun için havale işlemleri yapılan sayfada aşağıdaki bilgileri giriyor:

Adı Soyadı: Ahmet Kar

Banka Hesap Numarası: 1356236589884580

SIS Tanıtım Numarası: We2a

İşlem Türü: 01 - Hesaba Havale

Havale Yapılacak Kişi: Orhan Genç

Havale Yapılacak Hesap: 1356654876541321

Havale Miktarı: 150000000

Para Birimi: 01-TL

Açıklama: Ocak 2003 Kira Bedeli

Şifre: A3a0cd

Güvenlik Şifresi Değiştirme Kodu:2587

Ahmet kar bu işlemleri evinden yaptığı ve kendisini güvende hissettiği için güvenlik şifresinin değişmesine ihtiyaç duymamaktadır. Bu yüzden güvenlik değiştirme kodunu doğru girmiştir ve bundan sonra yapacağı işlemlerde aynı güvenlik şifresini kullanacaktır. Ahmet Kar gerekli bilgileri girdikten sonra mesaj bankaya gönderilmek üzere şifrelenir. Şifrelemede kullanılan rastgele anahtar “12723178493408” olarak belirlenmiş olsun.

Şifrelenecek Mesaj: Ahmet Kar&1356236589884580&01&150000000&01&Orhan Genç&1356654876541321&Ocak 2003 Kira Bedeli&2587

Şifrelenecek Mesaj Kodları:

3209150524994500217765676970666770697273727268697264776465776569646464
6464646477646577492109001699390516037765676970706968727170696865676665
774902001399666464679945112100993305040514117766697271

Anahtar: $H = \{1,3,5,6,2,3,6,5,8,9,8,8,4,5,8,0\}$

$G = \{3,2,6,7,0,0,6,4,0,2,0,4\}$

$R = \{1,2,7,2,3,1,7,8,4,9,3,4,0,8\}$

Karakter Sayısı:97

Rakam Sayısı $97 \times 2 = 194$

Matris Boyutları: $14 \times 14 = 196$

Şifrelenmiş Mesaj Kodları:

3617224452717540223107769708384893108402078315351964190441098838498267
4881009473027834600971919492271485383638058467728696842713911959689903
2445467414741290817467653827846074913686126727812704312466682189740284

Şifrelenmiş Mesaj:

DosJQ7\$Ğszg%(ğFN<ı!cg;mÇp0pdHh*FO:3N,a>9c@CWh7^>=vl?FDFe!38+!vk^pV
4 çtKL#l#j\,#31Fv!W#^D+j3v,vdzt24r/#c!

Şifrelenmiş Mesaj Özeti:

40NaĞ

Ahmet Kar mesajı şifreledikten sonra bankaya gönderir. Bankaya gönderilen bilgiler şunlardır:

Adı Soyadı: Ahmet Kar

SIS Tanıtım Numarası: We2a

İşlem:DosJQ7\$Ğszg%(ğFN<ı!cg;mÇp0pdHh*FO:3N,a>9c@CWh7^>=vl?FDFe!38+!vk^pV4 çtKL#l#j\,#31Fv!W#^D+j3v,vdzt24r/#c!

Özet: 040NaĞ

Banka SIS tanıtım numarasına ait hesap numarası ve şifre bilgilerini kullanarak şifreli mesajı çözer ve havale işlemini gerçekleştirir.

Örnek Olay 3.

Ahmet Kar, bir internet kafeden E-Market A.Ş. nin internet alışveriş sitesine giriyor ve ürün kodu 21345 olan üründen bir adet, 36423 olan üründen iki adet, 74563

olan üründen bir adet, 14632 olan üründen üç adet sipariş veriyor. Ahmet Kar ödeme şekli olarak SIS'i seçiyor. E-Market A.Ş.'nin sis tanıtım numarası "Eq21"dir Ahmet Kar işlemleri internet kafeden yaptığı için şifresinin ve hesap numarasının kötü niyetli kişiler tarafından ele geçirilmesinden endişe etmektedir. Bu yüzden "Güvenlik Değiştirme Kodu" alanına gerçek kod yerine "4567" yazıyor. Ahmet Kar'ın girdiği sipariş bilgileri şunlardır:

Adı Soyadı: Ahmet Kar

Adresi: Irmak Sokak No:12

Posta Kodu:06999

Semt/İlçe: Kızılay

İl: Ankara

Ülke:Türkiye

Satıcı Firma:E-Market A.Ş.

Ürün Kodu:21345;36423(2);74563;14632(3)

Toplam Fiyat:1235863000

Para Birimi:01-TL

Teslimat:Kargo

Teslimat Ücreti:25000000

Toplam Ödenecek:12608630000

Ödeme Şekli: SIS

Banka: E-Ticaret Bankası

SIS Tanıtım Numarası:Ae2a

Hesap Türü:01-Vadesiz Mevduat

Hesap Numarası:1356236589884580

Şifre:A30cda

Güvenlik Değiştirme Kodu:4567

Ahmet Kar gerekli bilgileri girdikten sonra mesaj satıcı firmaya gönderilmek üzere şifrelenir. Şifrelemede kullanılan rasgele anahtar “720462097813” olarak belirlenmiş olsun.

Şifrelenecek Mesaj: Ahmet Kar&1356236589884580&01&12608630000&01&E-Market A.Ş.&Eq21&4567

Şifrelenecek Mesaj Kodları:

3209150524994500217765676970666770697273727268697264776465776566706472
706764646464776465773787470021131124993280558077372066657768697071

Anahtar: $H = \{1,3,5,6,2,3,6,5,8,9,8,8,4,5,8,0\}$

$G = \{3,2,6,7,0,0,6,4,0,2,0,4\}$

$R = \{7,2,0,4,6,2,0,9,7,8,1,3\}$

Karakter Sayısı:68

Rakam Sayısı $68 \times 2 = 136$

Matris Boyutları: $12 \times 12 = 144$

Şifrelenmiş Mesaj Kodları:

7271275660082120846244067077897081280352174868540538210311024912841345
2444014415470116827588924906895698219266388950586843037746060806280999
3104372105597716

Şifrelenmiş Mesaj:

87vTWğrq!YJf6&/6,wçQoN4SeFrçicOj!kKtJbJmMbn:\$*=Of/T)r=2F/ÖÜ4İç&Lfğfwh
zdEreV&n

Şifrelenmiş Mesaj Özeti:

m*U8İ

Ahmet Kar mesajı şifreledikten sonra E-Market A.Ş.’ne gönderir. E-Market A.Ş.’ne gönderilen bilgiler şunlardır:

Adı Soyadı: Ahmet Kar

Adresi: Irmak Sokak No:12

Posta Kodu:06999

Semt/İlçe: Kızılay

İl: Ankara

Ülke:Türkiye

Satıcı Firma:E-Market A.Ş.

Ürün Kodu:21345;36423(2);74563;14632(3)

Toplam Fiyat:1235863000

Para Birimi:01-TL

Teslimat:Kargo

Teslimat Ücreti:25000000

Toplam Ödenecek:12608630000

Ödeme Şekli: SIS

Banka: E-Ticaret Bankası

SIS Tanıtım Numarası:Ae2a

İşlem:

87vTWğrq!YJf6&/6,wçQoN4SeFrçicOj!kKtJbJmMbn:\$*=Of/T)r=2F/ÖÜ4İç&Lfğfwh
zdEreV&n

Özet: m*U8İ

E-Market A.Ş. bu bilgiler içerisinde bankayı ilgilendiren kısımlar ile banka ile ilgili kendi bilgilerini bir araya getirir ve kendi bilgilerini ayrıca şifreler.

Satıcı Firma: E-Market A.Ş.

Hesap Numarası: 1847236584852014

Hesap Türü: 02-Ticari

SIS Tanıtım Numarası: Eq21

Şifre:Yey0312

Güvenlik Değiştirme Kodu:3519

Müşteri: Ahmet Kar

SIS Tanıtım Numarası: Ae2a

Toplam Tutar: 12608630000

Para Birimi: 01-TL

İşlem:

Ğ&:P.~hzA.LxU.\İ(?qsF^srBshCF?Ğ6xM1"H1ÜhD07@k~1!y4ox~@ıVn'#G\
R1öUÖ/###6~-81e

Özet: çHQ6V

Şifrelenecek Mesaj:

E-Market A.Ş.&1847236584852014&02&12608630000&01&Ahmet Kar&Ae2a&3519

Şifrelenecek Mesaj Kodları:

3787470021131124993280558077657268716667706972687269666465687764667765
667064727067646464647764657732091505249945002177320566007767696573

Anahtar: $H = \{1, 8, 4, 7, 2, 3, 6, 5, 8, 4, 8, 5, 2, 0, 1, 4\}$

$G = \{6, 2, 0, 5, 3, 0, 6, 4, 6, 7, 6, 5, 6, 6\}$

$R = \{1, 1, 8, 4, 2, 4, 9, 0, 5, 2, 7, 2\}$

Karakter Sayısı: 68

Rakam Sayısı $68 \times 2 = 136$

Matris Boyutları: $12 \times 12 = 144$

Şifrelenmiş Mesaj Kodları:

6096043155411852046949048284997052194198300004720522335944223390467189
6552743868095158928276333870508977471150363869134526994644978243383657
7308598372481121

Şifrelenmiş Mesaj:

W'dz\$HöQd5Od:!6QpH)yad8esBVJsB\L7/1Q#F4hPÜ=: %BF6Ö/&MiÖDF5kKülJ(:İF
DU9ğV;8Nir

Şifrelenmiş Mesaj Özeti:

dxğL)

Ahmet Kar mesajı şifreledikten sonra E-Market A.Ş.'ne gönderir. E-Market A.Ş.'ne gönderilen bilgiler şunlardır:

Satıcı Firma: E-Market A.Ş.

SIS Tanıtım Numarası: Eq21

İşlem: W'dz\$HöQd5Od:!6QpH)yad8esBVJsBL7/1Q#F4hPÜ=:%BF6Ö/&MiÖDF5kKü
LJ(:İFDU9ğV;8Nir

Özet: dxğL)

Müşteri: Ahmet Kar

SIS Tanıtım Numarası: Ae2a

İşlem

Ğ&:P.~hzA.LxU.\İ(?qsF^srBshCF?Ğ6xM1"H1ÜhD07@k~1!y4ox~@ıVn'#G\R1öUÖ/
##6~-8ie

Özet: çHQ6V

Banka SIS tanıtım numaralarına ait hesap numaraları ve şifre bilgilerini kullanarak şifreli mesajları çözer ve işlemleri gerçekleştirdikten sonra taraflara işlemin onaylandığını bildirir.

3.7.2. Sistemin Özellikleri

- 1- Kullanıcı veri iletişim kanallarına gönderdiği mesajlarda banka hesap numarasını açıkça yazmadığından hesap numarasının gizliliğini korumak için bir avantajı sahiptir.
- 2- Kullanıcıya ait parolanın şifrelemede anahtar olarak kullanılması ile sistemde dijital imza, parola koruması gibi diğer güvenlik unsurlarının görevleri de şifreleme algoritması tarafından yerine getirilmektedir.
- 3- Kullanıcı hesap ve şifre bilgilerinin kötü niyetli kişilerin eline geçmesi tehlikesine karşı gerekli donanıma sahiptir. Tüm bu bilgilerin kalıcı veya tek kullanımlık olması kullanıcının işlem yaptığı andaki isteğine bağlıdır.

4- Kullanıcı internette alış veriş, site aboneliği gibi üç taraflı işlemler (Kullanıcı, Satıcı, Banka) yaparken şifrelediği bilgiler ancak banka tarafından çözülebildiğinden banka dışındaki taraflara güvenme ihtiyacı hissetmemektedir.

5- Gönderilen mesaj birinci elden cevaplanmadığı için hızlı bir şekilde şifre deneme şansı yoktur. Yanlış şifre ile gönderilen mesaj önce satıcıya ulaşır ama satıcı tarafından denetlenmez. Satıcı mesajı bankaya gönderir ve şifrenin doğruluğu burada denetlenir. Bu durum ise deneme yanılma yolu ile anahtarın bulunmasını engelleyecektir.

3.7.3. Kullanılan SIS algoritmasının güvenlik analizi

Günümüze kadar kullanılan algoritmaların ilk ortaya çıkışlarına bakıldığında tümünün ortak iddiasının kriptanalize karşı direnci olduğu görülecektir. Zaten böyle bir iddia taşımayan bir algoritma kullanıma şansını bulamaz. Bu çerçevede, sunulan örnek algoritmanın hem parametreleri hakkında bilgi vermek hem de çözülmeye karşı direncini göstermek için bir tablo hazırlanmıştır.

Tablo 3.3'de birinci sütun şifrelenecek metnin uzunluğunu, ikinci sütun ise kullanılacak kare matrisin boyutlarını gösterir. Metinden elde edilecek rakamlar kare matrise yerleştirileceğinden belirli kare matris büyüklükleri için belirli metin uzunluğu aralıkları öngörülmüştür. Örneğin 4x4 kare matrise en çok 16 adet rakam sığacaktır. 16 rakam ise en çok $16/2 = 8$ karakter uzunluğunda bir metin anlamına gelir. 9 karakterlik metin ise 5x5 boyutlarındaki kare matrise yerleştirilecektir.

Tablodaki üçüncü sütun anahtar uzunluğu sütunudur. Anahtar uzunluğu matristeki satır (veya sütun) sayısının üç katı olarak bulunur. Yine 4x4 matris için örnek verirse; $2 \cdot 4 = 8$ rakamdan oluşan birinci anahtar ve 4 rakamdan oluşan bir rasgele anahtar kullanılacak ve toplam anahtar uzunluğu $8 + 4 = 12$ olacaktır.

Beşinci sütunda elde edilecek şifreli metnin uzunluğu karakter sayısı birimi ile hesaplanmıştır. 4x4 matris için şifreli metin uzunluğu şu şekilde hesaplanır: Kare matristen $4 \cdot 4 = 16$ rakam elde edilir. Bu 16 rakama 4 rakamdan oluşan rasgele anahtar eklenir. 20 rakamdan oluşan dizi ikişerli gruplanarak karakterlere çevrildiğinde 10 karakterden oluşan bir şifreli metin elde edilecektir.

Anahtar ihtimal sayısı ise 0-9 arası on rakamdan iadeli çekimle elde edilecek n uzunluğunda serinin adedi (10^n) olarak hesaplanır. Yine 4x4 matris için anahtar uzunluğu $n=12$ ve anahtar ihtimal sayısı 10^{12} olacaktır.

Tablodaki diğer sütunlar saniyede bir milyon anahtar deneyebilen bir sistemin olası tüm anahtarları denemesi için ihtiyaç duyulacak sürenin saniye, dakika, saat, gün ve yıl olarak hesaplanmış değerleridir. Saniye sütunu anahtar ihtimal sayısı bir milyona (10^6) bölünerek elde edilmiştir.

Tablo 3.3. SIS Algoritmasının Güvenlik Analizi

Gerçek Metin Uzunluğu	Matris Büyüklüğü	Anahtar Uzunluğu	Şifreli Metin Uzunluğu	Anahtar İhtimal Sayısı	Saniye	Dakika	Saat	Gün	Yıl
1	2x2	6	3	$1,E+06$	$1,E+00$	$2,E-02$	$3,E-04$	$1,E-05$	$3,E-08$
2-4	3x3	9	6	$1,E+09$	$1,E+03$	$2,E+01$	$3,E-01$	$1,E-02$	$3,E-05$
5-8	4x4	12	10	$1,E+12$	$1,E+06$	$2,E+04$	$3,E+02$	$1,E+01$	$3,E-02$
9-12	5x5	15	15	$1,E+15$	$1,E+09$	$2,E+07$	$3,E+05$	$1,E+04$	$3,E+01$
13-18	6x6	18	21	$1,E+18$	$1,E+12$	$2,E+10$	$3,E+08$	$1,E+07$	$3,E+04$
19-24	7x7	21	28	$1,E+21$	$1,E+15$	$2,E+13$	$3,E+11$	$1,E+10$	$3,E+07$
25-32	8x8	24	36	$1,E+24$	$1,E+18$	$2,E+16$	$3,E+14$	$1,E+13$	$3,E+10$
33-40	9x9	27	45	$1,E+27$	$1,E+21$	$2,E+19$	$3,E+17$	$1,E+16$	$3,E+13$
41-50	10x10	30	55	$1,E+30$	$1,E+24$	$2,E+22$	$3,E+20$	$1,E+19$	$3,E+16$
51-60	11x11	33	66	$1,E+33$	$1,E+27$	$2,E+25$	$3,E+23$	$1,E+22$	$3,E+19$
61-72	12x12	36	78	$1,E+36$	$1,E+30$	$2,E+28$	$3,E+26$	$1,E+25$	$3,E+22$
73-84	13x13	39	91	$1,E+39$	$1,E+33$	$2,E+31$	$3,E+29$	$1,E+28$	$3,E+25$
85-98	14x14	42	105	$1,E+42$	$1,E+36$	$2,E+34$	$3,E+32$	$1,E+31$	$3,E+28$
99-112	15x15	45	120	$1,E+45$	$1,E+39$	$2,E+37$	$3,E+35$	$1,E+34$	$3,E+31$
113-128	16x16	48	136	$1,E+48$	$1,E+42$	$2,E+40$	$3,E+38$	$1,E+37$	$3,E+34$

Kullanılan örnek algoritmanın güvenlik özellikleri Tablo 3.3'deki değerlerden yararlanılarak maddeler halinde aşağıda sıralanmıştır:

- 1- Kullanılan algoritmada bir karakterin hangi karakterle değişeceğini belirleyen parametrelerin (metindeki diğer tüm karakterler, kullanılan anahtarlar, değişecek karakterin metin içindeki konumu) çokluğu nedeniyle kırılması için mutlaka anahtarın bilinmesi gerekir.
- 2- Algoritmada herhangi bir matematiksel fonksiyon kullanılmamıştır. Bu nedenle matematiksel yaklaşımlarla çözülemez
- 3- Anahtar uzunluğu şifrelenen metnin uzunluğu ile orantılı olarak artmaktadır. Bu durumda metin uzadıkça olası anahtar sayısı da artmaktadır. Tablo 3.3'de görüldüğü gibi kullanılan algoritma anahtarın tahmin edilme zorluğu bakımından 61 karakter uzunluğu için DES algoritmasını 85 karakter uzunluğu için AES algoritmasını geride bırakmaktadır.

4- Şekil 3.19. a göre algoritmada şifrelenmiş metin şifrelenecek metnin uzunluğuna göre değişen bazı sabit uzunluk değerlerine sahip olacaktır. Bu durumda örneğin 41-50 aralığında bir uzunluğa sahip olan metin 10x10 matrise yerleştirilecek ve beş karakter uzunluğundaki rasgele anahtarın da eklenmesi ile şifreli metin 55 karakter uzunluğunda olacaktır. Şifreli metnin 54 ya da 56 karakter uzunluğa sahip olma olasılığı yoktur. Bu durumda veri iletişim araçlarından geçerken meydana gelebilecek bozulmalardan biri olan eksik iletim bir ölçüde denetlenebilecektir.

5- Yine Şekil 3.19. da görüldüğü gibi 113-128 karakter uzunluğunda bir metin için anahtarı tahmin etme olasılığı $1/10^{48}$ dir ve tüm olasılıkları denemek saniyede 1.000.000 deneme yapabilen bir sistem için bile 3×10^{34} yıl sürecektir.

6- Bu tür karşılaştırmaların ötesinde SIS, tek bir metot ya da algoritma değil, bir yaklaşımdır ve üzerinde çalışılmaya, desteklenmeye, geliştirilmeye muhtaçtır. Bu yaklaşım için getirilebilecek en olumlu eleştiri gelişime açık olması olacaktır.

SONUÇ

Bilgisayar ve iletişim teknolojilerindeki gelişmelere paralel olarak özellikle son on beş yıl içerisinde diğer faaliyetler gibi ticari faaliyetlerde de önemli değişimler meydana gelmiştir. Ortaya çıkan yeni ticaret araçları geleneksel metotlardan çok daha hızlı alışveriş yapma imkanı sunmaktadır. Elektronik ticaret adı verilen bu yeni ticaret şekli yeni imkanların yanı sıra yeni sorunları ve engelleri de beraberinde getirmiştir. Bu sorunların önemli bir bölümü veri iletişimi güvenliği ile ilgili sorunlardır.

Elektronik ortamda alışverişin geleneksel yöntemlere tercih edilmesi için birçok sebep sayılabilir. Hızlı ve yaygın alışveriş imkanı bu sebepler içerisinde en önemlileridir. Hızlı ve yaygın iletişimin sunduğu dünyanın herhangi bir yerindeki müşteriye veya satıcıya ulaşabilme, birçok alternatif içerisinden seçim yapabilme, bilgisayar kullanarak ürünleri görebilme, kalite ve fiyat karşılaştırması yapabilme gibi imkanlar bu yeni alışveriş aracının tartışılmaz üstünlüğünü göstermektedir. Ancak bütün üstünlüklerine rağmen güvenlik konusundaki en küçük bir kuşku insanların elektronik ticareti tercih etmemesi için yeterli olabilmektedir. Bu durum elektronik ticaretin gelişimi ile paralel olarak güvenlik teknolojilerinin de hızla gelişmesinin en önemli sebebidir.

Elektronik ticarete güvenlik araçları üç temel amaç çerçevesinde incelenmektedir. Birinci amaç karşıdaki kişinin kimliğinin kesin ve doğru olarak tanınmasıdır. İkinci amaç tanımlanan bu kişinin söz konusu işlemi yapmaya yetkili olup olmadığının belirlenmesi ve yetkisiz kişilerin müdahalesinin engellenmesidir. Üçüncü amaç ise yapılan işlemin taraflar tarafından daha sonra inkar edilememesinin sağlanmasıdır.

Bu amaçlar doğrultusunda geliştirilen güvenlik araçları donanım denilen bir kısım fiziksel aygıt ile yazılım denilen programlardan oluşur. Güvenlik amacı ile geliştirilen bilgisayar programları veya program parçacıkları güvenlik araçlarının yazılım kısmını oluşturmaktadır. Bu araçlar içerisinde verilerin istenmeyen kişiler tarafından okunamayacak şekilde şifrelenmesi büyük önem arz eder. Çünkü şifrelemenin kullanılmadığı güvenlik sistemi ya çok azdır veya yaygın olarak kullanılmamaktadır.

Bu çalışmada şifreleme ile ilgili kavramlar tanımlandıktan ve şifreleme metotları kısaca tanıtıldıktan sonra şifrelemenin elektronik ticarete bir güvenlik aracı olarak nasıl kullanıldığı açıklanmış ve son olarak SIS adı verilen yeni bir yaklaşımla yeni şifreleme algoritmaları geliştirilmeye çalışılmıştır.

SIS, diğer algoritmalarından farklı olarak anahtar kullanılıp kullanılmaması, anahtarların sayısı, çeşidi veya uzunluğu konularında tam bir esnekliğe sahiptir. SIS onlu sayı sistemi ve on tabanlı modüler aritmetiğin bir arada kullanılmasının getirdiği avantajlar ile diğer algoritmalarından daha az karmaşık işlemler icra ederek onlar kadar güvenli yeni algoritmalar geliştirme imkanı sunmaktadır. SIS'in bir diğer önemli avantajı da şifrelenecek metnin uzunluğu, metnin parçalara ayrılarak veya bütün halinde şifrlenmesi konularında da esneklik sağlamasıdır. SIS'in benzer algoritmalara karşı en önemli eksikliği ise kullanılan karakter sayısının yüzün katları olması zorunluluğu olarak belirlenebilir.

Ortaya konulan yeni metodun yaklaşım olarak isimlendirilmesinin sebebi bu metot kullanılarak birçok yeni şifreleme algoritması geliştirme imkanının var olmasıdır. Bu yeni yaklaşım yapılacak katkılarla daha da geliştirilmeye elverişli olduğu gibi şifreleme konusunda yapılacak çalışmalar için de farklı bir bakış açısı sağlayabilir.

KAYNAKLAR

Makaleler

Alman, Stuart, "Encryption and security: the Advanced Encryption Standard", **EDN**, 31 Ekim 2002.

Asenjo, Juan C., "The Advanced Encryption Standard: Implementation and Transition to a New Cryptographic Benchmark", **Network Security**, 1 Temmuz 2002, Sayı 7.

Barcelo, Julia, "Towards a European Framework For Digital Signatures And Encryption", **Computer Law & Security Report**, 1998, Sayı 14, No 2.

Bigelow, Robert, "Encryption Controls are US Government Priority", **Information Security Technical Report**, 1997, Cilt 2, Sayı 1.

Birch, Dave, "The Certificate Business Public Key Infrastructure Will Be Big Business", **Computer Law & Security Report**, 1997, Sayı 13, No 6.

Borst Johan, Bart Preneel, Vincent Rijmen, "Cryptography on Smart Cards", **Computer Networks**, 2001, Sayı 36.

Chang, Chin-Chen, Shin-Jia Hwang, "A Simple Approach for Generating RSA Keys", **Information Processing Letters**, 1997, Sayı 63.

Coppersmith, Don, Chris Holloway, Stephen M Matyas, Nev Zunic, "Data Encryption Standart", **Information Security Technical Report**, 1997, Sayı 2, No 2.

Diffie, Whitfield, "The National Security Establishment and the Development of Public-Key Cryptography", **Designs Codes and Cryptography**, 1996, Sayı 7.

Ersoy, Zeynep, "Elektronik Ticaretin Ekonomik ve Sosyal Etkileri", **Gorus**, Mart 2000.

Fan, C. W Chen, Y. Yeh, "Date Attachable Electronic Cash", **Computer Communications**, 2000, Sayı 23.

Forte, Dario, "The Future of the Advanced Encryption Standart", **Network Security**, Haziran 1999.

Golic, J.Dj., "Stream Cipher Encryption of Random Access Files", **Information Processing Letters**, 1999, Sayı 69.

Heinlein, Edwin B., "The RSA Security Conference 1995", **Computers & Security**, 1995, Sayı 14.

- Hickson, Nigel, "Encryption Policy: A UK Perspective", **Computers & Security**, 1997, Sayı 16.
- Highland, Harold Joseph, "Data Encryption: A Non-Mathematical Approach", **Computers & Security**, 1997, Sayı 16.
- Hwang, Shin-Jia, Chin-Chen Chang, Wei-Pang Yang, "Authenticated Encryption Schemes with Message Linkage", **Information Processing Letters**, 1996, Sayı 58
- Jansen, Cees J. A., Piet van der Vlist, "Message Encryption With Minimal Expansion and Redundancy-Doing Better Than ISO-10126", **Computer & Security**, 1996, Cilt 10, Sayı 7.
- Kennedy, Gabriella, "Codemakers, Codebreakers Rulemakers Dilemmas in Current Encryption Policies", **Computer Law & Security Report**, 2000, Cilt 16, Sayı 4.
- Kocarev, Ljupco, Goce Jagirovski, "Logistic Map as a Block Encryption Algorithm", **Physics Letters A.**, 2001, Sayı 289.
- Koops, Bert-Jaap, "Crypto Regulation in Europe: Some Key Trends and Issues", **Computer Networks and ISDN Systems**, 1997, Sayı 29.
- Lee, Wei-Bin, Chin-Chen Chang, "Using RSA With Low Exponent in a Public Network", **Computer Communications**, 1998, Sayı 21.
- Mitchell, Chris, "Authentication Using Cryptography", **Information Security Technical Report**, 1997, Cilt 2, Sayı 2.
- Murphy, Sean, "The Advanced Encryption Standard", **Information Security Technical Report**, 1999, Sayı 4.
- Palmer, Chloe, "DES Replacement Announced", **Computer Fraud & Security**, Kasım 2000.
- Pays, Poul-Andree, "Fabrice de Comarmond. An intermediation And Payment System Technology", **Computer Networks and ISDN Systems**, 1996, Sayı 28.
- Peyravian, Mohammad, Allen Roginsky, Nev Zunic, "Hash-Based Encryption System", **Computers & Security**, 1999, Cilt 18, Sayı 4.
- Pounder, Chris, "Further Developments in the Field of Encryption and Digital Signatures", **Computers & Security**, 1998, Sayı 17.
- Read, R. C., "Graph Theory and the Amateur Cryptographer", **Computers Math. Application**, 1997, Cilt 34, Sayı 11.

- Rove Heather, "Securing Payments Through Effective Authentication: Evaluating Trusted Third Party Proposals for a Thrust Hierarchy in the UK", **Computer Law & Security Report**, 1998, Cilt 14, Sayı 3.
- Schudelaro, A.A.P., "Electronic Payments", **Computer Law & Security Report**, 2001, Cilt 17, Sayı 2.
- Shepherd, Simon J., "A High Speed Software Implementation of the Data Encryption Standart", **Computers & Security**, 1995, Sayı 14.
- Stirland, Mark, "Smartcards in Secure Electronic Commerce", **Information Security Technical Report**, 1998, Sayı 3, No 2.
- Syed, Furqan, "Children of DES: A Look at the Advanced Encryption Standard", **Network Security**, Eylül 2000.
- Varadharajan, Vijay, Khanh Quoc Nguyen, Yi Mu, "On the design of e_ficient RSA-based on-line electronic cash schemes", **Theoretical Computer Science**, 1999, Sayı 226.
- Wright, Marie A., "Encription Alternatives for Network Security", **Computer Farud & Security**, Mart 1996.
- Wright, Marie A., "The Advanced Encryption Standard", **Network Security**, Ekim 2001.
- Wright, Marie A., "The Evolution of the Advanced Encryption Standard", **Network Security**, Kasım 1999.
- Yeh, Wen-Hung, Jing-Jang Hwang, "Hiding Digital Information Using a Novel System Scheme", **Computers & Security**, 2001, Cilt 20, Sayı 8.
- Zheng, Yuliang, Hideki Imai, "How to Construct Efficient Signcryption Schemes on Elliptic Curves", **Information Processing Letters**, 1998, Sayı 68.

Kitap-Yayın

- Beckett, Brian, **Introduction to Cryptography and PC Security**, McGraw-Hill Int., 1997.
- ETKK, **Türkiye Elektronik Ticaret Koordinasyon Kurulu Elektronik Ticaret Raporu**, 1998.
- FIPS Pub 197, **Announcing the Advanced Encryption Standard (AES)**, Federal Information Processing Standards Publication, 26 Kasım 2001.

- FIPS Pub 46-3, **Data Encryption Standard (DES)**, Federal Information Processing Standards Publication, 25 Ekim 1999.
- FIPS Pub. 171, **Specifications for Key Management Using ANSI X9 17**, Federal Information Processing Standard Publication, 27 Nisan 1992.
- FIPS Pub. 180-1, **Announcing the Standard for SECURE HASH STANDARD**, Federal Information Processing Standards Publication, 17 Nisan 1995.
- Ford, Warwick, **Computer Communications Security**, Prentice Hall PTR, 1994.
- Guttman, Barbara, **Computer Security Considerations in Federal Procurements: A Guide for Procurment Initiators, Contracting Officers and Computer Security Officials**, NIST Special Publication 800-4, Mart 1992.
- Kalakota, Ravi, Andrew B. Whinston, **Electronic Commerce: A Managar's Guide**, Addison Wesley, 1997.
- Kienan, Brenda, **İşletmeler İçin Çözümler: E-Ticaret**, Arkadaş Yayınları. 2002.
- Mc. Daniel, George, **IBM dictionary of computing**, MCGraw Hill Inc., Ağustos 1993.
- Menezes, Alfred J., Paul C. van Oorschot, Scott A. Vanstone, **Handbook of Applied Cryptography**, CRC Pres, 3. Baskı, 2001.
- Nechvatal, James, **Public-Key Cryptography**, NIST Special Publication 800-2, Nisan 1991.
- NITSEC, **NATO Information Technology Security Evaluation Criteria**, NITSEC Publications AC/35, 1996.
- OECD, **Information Technology Outlook**, OECD Publications, Paris, 1997.
- Özen, Üstün, **Firma Müşteri Boyutuyla E-Ticaret: İnternet Kullanıcılarının Elektronik Alışveriş Davranışları**, Aktif Yayınevi, İstanbul, 1998.
- Parmar, S.K., **An Introduction To Security**, RCMP Publication.
- Petras, Richard T. **Mathematics Teacher**. Kasım 2001. Sayı 94/8.
- NIST, **SP-800-4**, NIST Special Publications.
- Stinson, Douglas R., **Cryptography: Theory and Practice**, CRC Press Inc., 1995.
- Turban, Efraim, Jae Lee, David King, H. Michael Chung, **Electronic Commerce: A Managerial Perspective**, Prentice-Hall Inc., 1999.

Ziya, Rüçhan, **A Study on the Internet as a Commerce Medium**, MSc Thesis 1997.

İnternet Kaynakları

GPO, Federal Register, Ocak 1997, Sayı 62, No 1, wais.access.gpo.gov.

<http://csrc.nist.gov>

<http://www.codesandciphers.org.uk/enigma/enigma1.htm>

<http://www.docs.sum.com>

<http://www.emmy.nmsu.edu/~crypto>

<http://www.eng.bahcesehir.edu.tr/css/bolum11>

<http://www.swimmer.org/morton/enigma.html>

<http://www.techdirections.com>

<http://www.ugrad.cs.jhu.edu/~russell/classes/enigma/history.html>

<http://www.ykb.com>

Office of Fair Trading. E-Commerce and Its Implications for Competition Policy. Discussion Paper. 2000, <http://www.oft.gov.uk>.

Senger, Matt, Providing Security through Secure Socket Layer, www.mrs.umn.edu

EKLER

EK 1. Visual Basic Kodları (Örnek Algoritma 9-Encryption)

'Şifrelenecek metnin değişken-e aktarılması

```
texte = Text1.Text
```

'Metnin uzunluğu

```
n1 = Len(texte)
```

'Sayı dizisinin uzunluğu

```
N = 2 * n1
```

```
ReDim X1(0 To n1 - 1) As String
```

```
ReDim X2(0 To N - 1) As Integer
```

'Metnin sayı dizisi olarak X2 değişkenine yazılması

```
x3 = 0
```

```
For i = 0 To n1 - 1
```

```
    x1(i) = tabloe(Mid(texte, i + 1, 1))
```

```
    x2(x3) = Int(Mid(X1(i), 1, 1))
```

```
    x3 = x3 + 1
```

```
    x2(x3) = Int(Mid(X1(i), 2, 1))
```

```
    x3 = x3 + 1
```

```
Next i
```

'Sayı dizisinin yerleştirileceği kare matrisin büyüklüğü

```
M = Int(Sqr(N)) + 1
```

'Sayı dizisinin kare matrise yazılması

```
x3 = 0
```

```
ReDim X(0 To M - 1, 0 To M - 1) As Integer
```

```
For i = 0 To M - 1
```

```
    For j = 0 To M - 1
```

```
        If x3 > N - 1 Then X(i, j) = 9 Else X(i, j) = X2(x3)
```

```
        x3 = x3 + 1
```

```
    Next j
```

```
Next i
```

'Birinci anahtarın sayı dizisi olarak yazılması

```
textH = Text4.Text
```

```
h1 = Len(textH)
```

```
ReDim H(0 To h1 - 1) As Integer
```

```
ReDim H2(0 To h1 - 1) As Integer
```

```
For i = 0 To h1 - 1
```

```
    H(i) = Int(Mid(textH, i + 1, 1))
```

Next i

'Birinci anahtarın düzenlenmesi

If $h1 > 6$ Then

For $i = 0$ To $h1 - 1$

$e1 = i - 2$

If $e1 < 0$ Then $e1 = e1 + 10$

If $e1 > h1 - 1$ Then $e1 = e1 - ((e1 \setminus h1) * h1)$

$e2 = i - 1$

If $e2 < 0$ Then $e2 = e2 + 10$

If $e2 > h1 - 1$ Then $e2 = e2 - ((e2 \setminus h1) * h1)$

$e3 = i + 1$

If $e3 > 9$ Then $e3 = e3 - 10$

If $e3 > h1 - 1$ Then $e3 = e3 - ((e3 \setminus h1) * h1)$

$e4 = i + 2$

If $e4 > 9$ Then $e4 = e4 - 10$

If $e4 > h1 - 1$ Then $e4 = e4 - ((e4 \setminus h1) * h1)$

$e5 = H(i) + H(e1) + H(e2) + H(e3) + H(e4)$

If $e5 > 9$ Then $e5 = e5 - ((e5 \setminus 10) * 10)$

$H2(i) = e5$

Next i

For $i = 0$ To $h1 - 1$

$e1 = i - 2$

If $e1 < 0$ Then $e1 = e1 + 10$

If $e1 > h1 - 1$ Then $e1 = e1 - ((e1 \setminus h1) * h1)$

$e2 = i - 1$

If $e2 < 0$ Then $e2 = e2 + 10$

If $e2 > h1 - 1$ Then $e2 = e2 - ((e2 \setminus h1) * h1)$

$e3 = i + 1$

If $e3 > 9$ Then $e3 = e3 - 10$

If $e3 > h1 - 1$ Then $e3 = e3 - ((e3 \setminus h1) * h1)$

$e4 = i + 2$

If $e4 > 9$ Then $e4 = e4 - 10$

If $e4 > h1 - 1$ Then $e4 = e4 - ((e4 \setminus h1) * h1)$

$e5 = 0$

For $j = 0$ To $h1 - 1$

If $j \diamond e1$ And $j \diamond e2$ And $j \diamond e3$ And $j \diamond e4$ And $j \diamond i$ Then

$e5 = e5 + H2(j)$

EndIf

Next j

```

        If e5 > 9 Then e5 = e5 - ((e5 \ 10) * 10)
        H(i) = e5
    Next i
End If

'Birinci anahtar kullanılarak sütun(K) ve satır(L) değerlerinin belirlenmesi
ReDim K(0 To M - 1) As Integer
ReDim L(0 To M - 1) As Integer
For i = 0 To M - 1
    If i > h1 - 1 Then x3 = i - ((i \ h1) * h1) Else x3 = i
    K(i) = H(x3)
Next i
E = x3 + 1
For i = 0 To M - 1
    If i + E > h1 - 1 Then x3 = i + E - (((i + E) \ h1) * h1) Else x3 = i + E
    L(i) = H(x3)
Next i

'Matris değerlerinin satır ve sütun değerleri ile toplanması
For i = 0 To M - 1
    For j = 0 To M - 1
        E = X(i, j) + K(j) + L(i)
        E = E - ((E \ 10) * 10)
        x(i, j) = E
    Next j
Next i

'Rasgele anahtarın üretilmesi
ReDim R(0 To M - 1) As Integer
For i = 0 To M - 1
    R(i) = (Rnd() * 9 + 1) - 1
Next i

'Rasgele anahtara göre sütunların dairesel olarak kaydırılması
ReDim Y(0 To M - 1, 0 To M - 1) As Integer
For j = 0 To M - 1
    For i = 0 To M - 1
        E = M - R(j) + i
        If E > M - 1 Then E = E - ((E \ M) * M)
        Y(i, j) = X(E, j)
    Next i
Next j

'Rasgele anahtara göre satırların dairesel olarak kaydırılması

```

```

For i = 0 To M - 1
    For j = 0 To M - 1
        E = M - R(i) + j
        If E > M - 1 Then E = E - ((E \ M) * M)
        X(i, j) = Y(i, E)
    Next j
Next i

'matrisin tekrar sayı dizisi olarak yazılması
ReDim Y1(0 To (M * M + M) - 1) As Integer
x3 = 0
For i = 0 To M - 1
    For j = 0 To M - 1
        Y1(x3) = X(i, j)
        x3 = x3 + 1
    Next j
Next i

'ikinci anahtarın sayı dizisi olarak yazılması
textG = Text3.Text
g1 = Len(textG)
g2 = 2 * g1
ReDim g3(0 To g1 - 1) As String
ReDim G(0 To g2 - 1) As Integer
x3 = 0
x4 = 0
For i = 0 To g1 - 1
    g3(i) = tabloe(Mid(textG, i + 1, 1))
    G(x3) = Int(Mid(g3(i), 1, 1))
    x3 = x3 + 1
    G(x3) = Int(Mid(g3(i), 2, 1))
    x3 = x3 + 1
Next i
If g2 > M Then
    For i = M To g2 - 1
        For j = 0 To M - 1
            G(j) = G(j) + G(i)
            If G(j) > 9 Then G(j) = G(j) - 10
        Next j
    Next i
End If

```

'İkinci anahtar kullanılarak rasgele anahtarın sayı dizisi içerisine yerleştirilmesi

ReDim Y2(0 To (M * M + M) - 1) As Integer

x3 = 0

x4 = 0

x5 = 0

x6 = 0

x7 = True

For i = 0 To (M * M + M) - 1

 If x4 = G(x5) - 1 And x7 = True Then

 Y2(i) = R(x6)

 If i = 24 Or i = 49 Or i = 74 Or i = 99 Or i = 124 Or i = 149 Or i = 174 Then

 EndIf

 x5 = x5 + 1

 If x5 = g2 Then x5 = 0

 If G(x5) = 0 Then x4 = -1 Else x4 = 0

 x6 = x6 + 1

 If x6 = M Then x7 = False

 Else

 Y2(i) = Y1(x3)

 Y2(i) & " ";

 If i = 24 Or i = 49 Or i = 74 Or i = 99 Or i = 124 Or i = 149 Or i = 174 Then

 EndIf

 x3 = x3 + 1

 x4 = x4 + 1

 End If

Next i

x3 = 0

'sayı dizisinin ikiyeşerli olarak gruplandırılması ve karakterlere çevrilmesi

ReDim Y3(0 To (M * M + M) \ 2 - 1) As String

For i = 0 To (M * M + M) \ 2 - 1

 Y3(i) = Y2(x3) & Y2(x3 + 1)

 x3 = x3 + 2

 Text2(0).Text = Text2(0).Text & tablod(Y3(i))

Next i

End

EK 2. Visual Basic Kodları (Örnek Algoritma 9-Decryption)

'Şifrelenecek metnin değişkene aktarılması

```
texted = Text2(0).Text
```

'metnin uzunluğu

```
n1 = Len(texted)
```

'Sayı dizisinin uzunluğu

```
N = 2 * n1
```

'Metnin sayı dizisi olarak Y2 değişkenine yazılması

```
x3 = 0
```

```
ReDim Y1(0 To n1 - 1) As String
```

```
ReDim Y2(0 To N - 1) As Integer
```

```
x3 = 0
```

```
For i = 0 To n1 - 1
```

```
    Y1(i) = tabloe(Mid(texted, i + 1, 1))
```

```
    Y2(x3) = Int(Mid(Y1(i), 1, 1))
```

```
    x3 = x3 + 1
```

```
    Y2(x3) = Int(Mid(Y1(i), 2, 1))
```

```
    x3 = x3 + 1
```

```
Next i
```

'Sayı dizisinin yerleştirileceği kare matrisin büyüklüğünün bulunması

```
x3 = 0
```

```
Do
```

```
    M = Int(Sqr(N)) - x3
```

```
    If M < 1 Then
```

```
        MsgBox "Bu metin SIS ile şifrlenmemiş"
```

```
    End
```

```
End If
```

```
    If N = M * M + M Then
```

```
        Exit Do
```

```
    Else
```

```
        x3 = x3 + 1
```

```
    End If
```

```
Loop
```

'İkinci anahtarın sayı dizisi olarak yazılması

```
textG = Text3.Text
```

```
g1 = Len(textG)
```

```
g2 = 2 * g1
```

```
ReDim g3(0 To g1 - 1) As String
```

```
ReDim G(0 To g2 - 1) As Integer
```

```
x3 = 0
```

```
x4 = 0
```

```
For i = 0 To g1 - 1
```

```
    g3(i) = tabloe(Mid(textG, i + 1, 1))
```

```
    G(x3) = Int(Mid(g3(i), 1, 1))
```

```
    x3 = x3 + 1
```

```
    G(x3) = Int(Mid(g3(i), 2, 1))
```

```
    x3 = x3 + 1
```

```
Next i
```

```
If g2 > M Then
```

```
    For i = M To g2 - 1
```

```
        For j = 0 To M - 1
```

```
            G(j) = G(j) + G(i)
```

```
            If G(j) > 9 Then G(j) = G(j) - 10
```

```
        Next j
```

```
    Next i
```

```
End If
```

```
N = M * M
```

```
n1 = N / 2
```

'İkinci anahtar kullanılarak rasgele anahtarın sayı dizisi içerisinde bulunması ve gerçek sayı dizisinin (Y3) elde edilmesi

```
ReDim Y3(0 To N - 1) As Integer
```

```
ReDim R(0 To M - 1) As Integer
```

```
x3 = 0
```

```
x4 = 0
```

```
x5 = 0
```

```
x6 = 0
```

```
x7 = True
```

```
For i = 0 To (M * M + M) - 1
```

```
    If x4 = G(x5) - 1 And x7 = True Then
```

```
        R(x6) = Y2(i)
```

```
        x5 = x5 + 1
```

```
        If x5 = g2 Then x5 = 0
```

```
        If G(x5) = 0 Then x4 = -1 Else x4 = 0
```

```
        x6 = x6 + 1
```

```
        If x6 = M Then x7 = False
```

```
    Else
```

```
        Y3(x3) = Y2(i)
```

```

        x3 = x3 + 1
        x4 = x4 + 1
    End If
Next i
'Sayı dizisinin kare matrise yazılması
ReDim Y(0 To M - 1, 0 To M - 1) As Integer
x3 = 0
For i = 0 To M - 1
    For j = 0 To M - 1
        Y(i, j) = Y3(x3)
        x3 = x3 + 1
    Next j
Next i
'Rasgele anahtara göre satırların dairesel olarak kaydırılması
ReDim X(0 To M - 1, 0 To M - 1) As String
For i = 0 To M - 1
    For j = 0 To M - 1
        E = R(i) + j
        If E > M - 1 Then E = E - ((E \ M) * M)
        X(i, j) = Y(i, E)
    Next j
Next i
'Rasgele anahtara göre sütunların dairesel olarak kaydırılması
For j = 0 To M - 1
    For i = 0 To M - 1
        E = R(j) + i
        If E > M - 1 Then E = E - ((E \ M) * M)
        Y(i, j) = X(E, j)
    Next i
Next j
'Birinci anahtarın sayı dizisi olarak yazılması
textH = Text4.Text
h1 = Len(textH)
ReDim H(0 To h1 - 1) As Integer
ReDim H2(0 To h1 - 1) As Integer
For i = 0 To h1 - 1
    H(i) = Int(Mid(textH, i + 1, 1))
Next i
'Birinci anahtarın düzenlenmesi

```

If $h1 > 6$ Then

For $i = 0$ To $h1 - 1$

$e1 = i - 2$

If $e1 < 0$ Then $e1 = e1 + 10$

If $e1 > h1 - 1$ Then $e1 = e1 - ((e1 \setminus h1) * h1)$

$e2 = i - 1$

If $e2 < 0$ Then $e2 = e2 + 10$

If $e2 > h1 - 1$ Then $e2 = e2 - ((e2 \setminus h1) * h1)$

$e3 = i + 1$

If $e3 > 9$ Then $e3 = e3 - 10$

If $e3 > h1 - 1$ Then $e3 = e3 - ((e3 \setminus h1) * h1)$

$e4 = i + 2$

If $e4 > 9$ Then $e4 = e4 - 10$

If $e4 > h1 - 1$ Then $e4 = e4 - ((e4 \setminus h1) * h1)$

$e5 = H(i) + H(e1) + H(e2) + H(e3) + H(e4)$

If $e5 > 9$ Then $e5 = e5 - ((e5 \setminus 10) * 10)$

$H2(i) = e5$

Next i

For $i = 0$ To $h1 - 1$

$e1 = i - 2$

If $e1 < 0$ Then $e1 = e1 + 10$

If $e1 > h1 - 1$ Then $e1 = e1 - ((e1 \setminus h1) * h1)$

$e2 = i - 1$

If $e2 < 0$ Then $e2 = e2 + 10$

If $e2 > h1 - 1$ Then $e2 = e2 - ((e2 \setminus h1) * h1)$

$e3 = i + 1$

If $e3 > 9$ Then $e3 = e3 - 10$

If $e3 > h1 - 1$ Then $e3 = e3 - ((e3 \setminus h1) * h1)$

$e4 = i + 2$

If $e4 > 9$ Then $e4 = e4 - 10$

If $e4 > h1 - 1$ Then $e4 = e4 - ((e4 \setminus h1) * h1)$

$e5 = 0$

For $j = 0$ To $h1 - 1$

If $j \diamond e1$ And $j \diamond e2$ And $j \diamond e3$ And $j \diamond e4$ And $j \diamond i$ Then

$e5 = e5 + H2(j)$

EndIf

Next j

If $e5 > 9$ Then $e5 = e5 - ((e5 \setminus 10) * 10)$

$H(i) = e5$

```

Next i
End If
'Birinci anahtar kullanılarak sütun(K) ve satır(L) değerlerinin belirlenmesi
ReDim K(0 To M - 1) As Integer
ReDim L(0 To M - 1) As Integer
For i = 0 To M - 1
    If i > h1 - 1 Then x3 = i - ((i \ h1) * h1) Else x3 = i
    K(i) = H(x3)
Next i
E = x3 + 1
For i = 0 To M - 1
    If i + E > h1 - 1 Then x3 = i + E - (((i + E) \ h1) * h1) Else x3 = i + E
    L(i) = H(x3)
Next i
'Satır ve sütun değerlerinin matris değerlerinden çıkarılması
For i = 0 To M - 1
    For j = 0 To M - 1
        E = Y(i, j) - K(j) - L(i)
        If E < 0 Then E = E + (((-1 * E) \ 10 + 1) * 10)
        If E > 9 Then E = E - ((E \ 10) * 10)
        Y(i, j) = E
    Next j
Next i
'matrisin tekrar sayı dizisi olarak yazılması
ReDim X1(0 To N - 1) As Integer
x3 = 0
For i = 0 To M - 1
    For j = 0 To M - 1
        x1(x3) = Y(i, j)
        x3 = x3 + 1
    Next j
Next i
'sayı dizisinin ikişerli olarak gruplandırılması ve karakterlere çevrilmesi
ReDim X2(0 To N \ 2 - 1) As String
x3 = 0
For i = 0 To N \ 2 - 1
    x2(i) = X1(x3) & X1(x3 + 1)
    x3 = x3 + 2
    Text1.Text = Text1.Text & tablod(X2(i))
Next i
End

```

ÖZGEÇMİŞ

1970 Erzurum Doğumluyum. İlk ve orta öğrenimimi Erzurum'da yaptım. 1996'da İstanbul Üniversitesi İktisat Fakültesinden mezun oldum. Yüksek Lisansımı 1999 yılında Erzurum Atatürk Üniversitesi Sosyal Bilimler Enstitüsünde tamamladım. 1998'den beri Erzurum Atatürk Üniversitesi İktisadi ve İdari Bilimler Fakültesi'nde Araştırma Görevlisi olarak görev yapmaktayım.

