BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

ELEKTRONİK HABERLEŞME HİZMETİ İÇİNDE GÜVENLİ SES/VERİ HABERLEŞMESİ AÇISINDAN KRİPTOLU HABERLEŞMENİN İNCELENMESİ, DÜZENLEMELER, ÖNERİLER VE TÜRKİYE ANALİZİ

Mustafa TEFON

Teknik Uzmanlık Tezi

Haziran 2013

Ankara

BTK
BİLGİ TEKNOLOJİLERİ
VE İLETİŞİM KURUMU

Bu yayında öne sürülen fikirler eserin yazarına aittir;

Bilgi Teknolojileri ve İletişim Kurumunun görüşlerini yansıtmaz.

BTK ISBN 978-605-345-050-4

BTK Yayın No T 0162

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

ELEKTRONİK HABERLEŞME HİZMETİ İÇİNDE GÜVENLİ SES/VERİ HABERLEŞMESİ AÇISINDAN KRİPTOLU HABERLEŞMENİN İNCELENMESİ, DÜZENLEMELER, ÖNERİLER VE TÜRKİYE ANALİZİ

Mustafa TEFON

Teknik Uzmanlık Tezi

Haziran 2013

Ankara

Mustafa TEFON tarafından hazırlanan " Haberleşme Hizmeti İçinde Güvenli Ses/Veri Haberleşmesi Açısından Kriptolu Haberleşmenin İncelenmesi, Düzenlemeler, Öneriler Ve Türkiye Analizi" adlı bu tezin Bilgi Teknolojileri ve İletişim Kurumunda Teknik Uzmanlık Tezi olarak uygun olduğunu onaylarım.

Prof. Dr. A.Bülent EKİN
Tez Yöneticisi

Bu çalışma, jürimiz tarafından Teknik Uzmanlık Tezi olarak kabul edilmiştir.

Başkan: N. Deniz YANIK

Üye : Prof.Dr. A.Bülent EKİN

Üye : Atilla Arslan

Üye : İlhan ELİEYİOĞLU

Üye : M. Salim KETENCİOĞLU

Bu tez, Bilgi Teknolojileri ve İletişim Kurumu tez yazım kurallarına uygundur.

İÇİNDEKİLER

ÖZET

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU	
Tezin Adı	Haberleşme Hizmeti İçinde Güvenli Ses/Veri Haberleşmesi Açısından Kriptolu Haberleşmenin İncelenmesi, Düzenlemeler, Öneriler Ve Türkiye Analizi
Türü	Teknik Uzmanlık Tezi
Yazar	Mustafa TEFON
Teslim Tarihi	20.06.2013
Anahtar kelimeler	Kriptografi, Gizli Anahtar Kripto Sistemler, Açık Anahtar Kripto Sistemler, Güvenli Haberleşme, Kripto Algoritmaları, Kanun , Yönetmelik
Tez Danışmanı	Prof. Dr. A. Bülent EKİN
Sayfa adedi	vii + 103

Özet

5809 sayılı Haberleşme Kanunu'na istinaden yayımlanan Yönetmelik çerçevesinde kamu kurum ve kuruşları ile gerçek ve tüzel kişilere de elektronik haberleşme cihazlarında kod ve kripto sistemi kullanılarak güvenli haberleşeme yapabilmelerine imkân tanınmıştır.

Geçmişte güvenli haberleşmeye askeri ve yönetim alanında ihtiyaç duyulmakta iken, içerisinde bulunduğumuz bilgi çağında iletişimdeki güvenlik birçok alanda karşımıza çıkmaktadır.

Bu tez çalışmasında, kripto sistemlerine ilişkin terminoloji, klasik ve modern kripto sistemleri, ülke uygulamaları incelenmiş, ülkemizdeki mevcut durum değerlendirilmesi yapılarak, kullanılacak kripto sistemlerinde BTK'yı ilgilendiren hususlar ve uygulamaya yönelik öneriler getirilmiştir.

ABSTRACT

INFORMATION AND COMMUNICATIONS TECHNOLOGIES AUTHORITY	
Thesis	Analysis Of Cryptographic Communications In Terms Of Secure Voice/Data Communications In Electronic Communications Services, Regulations, Proposals And Turkey Analysis
Type	Technical Expert Thesis
Author	Mustafa TEFON
Submission Date	20.06.2013
Key Words	Cryptography, Secret Key Cryptosystems, Public Key Cryptosystems, Secure Communications, Cryptography Algorithms, Electronic Communications Law, Regulation
Advisor	Assoc. Prof. Dr. A.Bülent EKİN
Total Page	vii + 103

Abstract

With the recently published By-Law based on Electronic Communications Law numbered 5809, natural and legal persons as well as public institutions have been allowed to use code and crypto systems in their electronic communication devices.

While needing the secured communication in the military and public in the past, the information security in the information era is faced in the most views nowadays.

In this thesis study, some proposals on the issues regarding classic and modern crypto systems which interest ICTA and on practical aspects by assessing mathematical methods of crypto systems, other countries' practices and current situation in Turkey.

TEŞEKKÜR

Bu tez çalışmamda bana yol gösteren teşvik eden ve yardımlarını esirgemeyen değerli öğretim görevlisi hocam Prof. Dr. A.Bülent EKİN ve Doç. Dr. Gültekin KAVUŞAN'a, kıymetli tecrübelerinden faydalandığım Daire Başkanlarım Müberra OĞUZ, Abdullah KARAKAŞ, ve Atilla ARSLAN'a, olumlu eleştirileri ve katkılarından dolayı dostlarım Binnur TUĞLUOĞLU, Osman ATEŞ, Yusuf YILDIRIM, Yunus Şuayip ÇETİN ve diğer çalışma arkadaşlarıma, manevi desteğini her zaman arkamda hissettiğim sevgili eşim Jale TEFON'a en derin saygı ve sevgilerimle teşekkürlerimi sunarım.

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

KISALTMALARIN LİSTESİ

AB	:	Avrupa Birliği
AÇMA FONKSİYONU	:	Kapalı mesajın açık hale getirilmesi
BSI	:	Enformasyon Teknolojileri Güvenlik Kurumu (Bundesamt für Sickerheit in der Informationstechnik-Almanya)
DPL	:	Dikrete Logaritma Problemi
DSA	:	Dijtal İmza Algoritması (Digital Signature Algorithm)
DÜZMETİN	:	Açık metin
EEK	:	Eliptik Eğri Kriptolaması
GCHQ	:	Kamu Haberleşme Koordinasyonu (Government Communications Headquarters-İngiltere)
KANUN	:	5809 sayılı Elektronik Haberleşme Kanunu
KAPAMA FONKSİYONU	:	Bir mesajın kapalı hale (okunamaması) getirilmesi
KODLAMA	:	Bilgiyi değişik sembol veya harflerle ifade etmeye denir.
KRİPTOANALİZ	:	Bir kripto sisteminin kırılma işlemleri.
KRİPTOGRAF	:	Kriptografi ile ilgilenen bilim adamları
KRİPTOGRAFİ	:	Gizli ve yazılı metin anlamına gelen yazma sanatı veya bilimi.
KRİPTOLOJİ	:	Kriptografi biliminin bilimsel çalışmasına
KRİPTO METNİ	:	Kapalı metin.
KRİPTO SİSTEM	:	Güvenliği haberleşme için oluşturulan sistemi.
KURUM, BTK	:	Bilgi Teknolojileri ve İletişim Kurumu
NIST	:	ABD'nin ulusal standartlar ve teknoloji enstitüsü (National Institute of Standards and Technology)
NSA	:	Ulusal Güvenlik Teşkilatı (National Security Agency-ABD)
OECD	:	Organization for Economic Co-operatting and Development (Ekonomik İşbirliği ve Kalkınma Teşkilatı)

PKI	:	Açık Anahtar Altyapısı (Public Key Infrastructure)
PROTOKOL	:	Sistemler arası iletişim biçimini belirleyen kural.
RFID	:	Radyo frekanslı tanımlama sistemleri (Radio-Frequency Identification)
TİB	:	Telekomünikasyon İletişim Başkanlığı
WASSENAAR DÜZENLEMESİ	:	Konvensiyonel silahlar ile çift kullanımlı malzeme ve teknolojilerin İhracat kontrollerini yapmayı amaçlayan bir silah kontrol rejimi.
WEP	:	Kablolu Eşdeğer Protokolü (Wired Equivalancy Protocol)
YÖNETMELİK	:	20.10.2010 tarih ve 27738 sayılı "Kamu Kurum ve Kuruluşları ile Gerçek ve Tüzel Kişilerin Haberleşme Hizmeti İçinde Kodlu veya Kriptolu Haberleşme Yapma Usul ve Esasları Hakkında Yönetmelik"
MÜLGA YÖNETMELİK	:	Kriptolu Telsiz Sistemleri Yönetmeliği

GİRİŞ

Toplumların en değerli hazinesi bilgidir. Bilgi çağı olarak adlandırılan 21. yüzyılda, ülkeler iki temel sınıflandırmaya tabi tutulmaktadır. " ***Bilgi toplumu olmuş ülkeler*** " ve " ***bilgi toplumu olamamış ülkeler*** ".

Tarih boyunca insanlar birbirleri ile haberleşmede yeni yöntemler geliştirmiş ve iletilerin başka insanlardan saklanması gerekliliği ortaya çıktığından beri gizlilik, haberleşmedeki en önemli kıstas olmuştur. Bilgilerin güvenliği, binlerce yıl önce devletlerin ve imparatorlukların gizli ve önemli bilgileri düşmanın eline geçmeden iletebilmesi ile ortaya çıkmıştır. Eski dönemlerde, uzak mesafelerdeki haberleşmede kod[1] kullanımında mesajın düşmanın eline geçmeden ulaştırılması esastır.

Genelde bilginin kodlanması ile bilginin kapatılması (kriptografi) karıştırılan kavramlar olmuştur. Kavram karmaşasının ortadan kaldırmak adına kod ve kripto ifadelerini şu şekilde açıklayabiliriz. Örneğin, evimizde kullandığımız televizyonları ele alalım. Ses ve görüntü iletiminde radyo sinyalleri kullanılmaktadır. Televizyon içerisinde bulunan kod çözücü sayesinde bu kodlar ses ve görüntü olarak bize ulaşmaktadır.

Yani her televizyon gelen sinyali ses ve görüntüye çevirme yeteneğine sahiptir. Diğer taraftan bir kripto sistemi kullanılarak kapatılan aynı sinyaller normal bir televizyon ile bu ses ve görüntüleri bize veremezler. Özel bir cihaz ile bu kapatılan sinyaller açılarak normal televizyonda sunulur. Bu sistem telefonlar için de geçerlidir. Sesler radyo sinyali olarak kodlanır. Bu sinyali alan telefonlarımız bu kodu çözerek bize ses sinyalini ulaştırırlar.

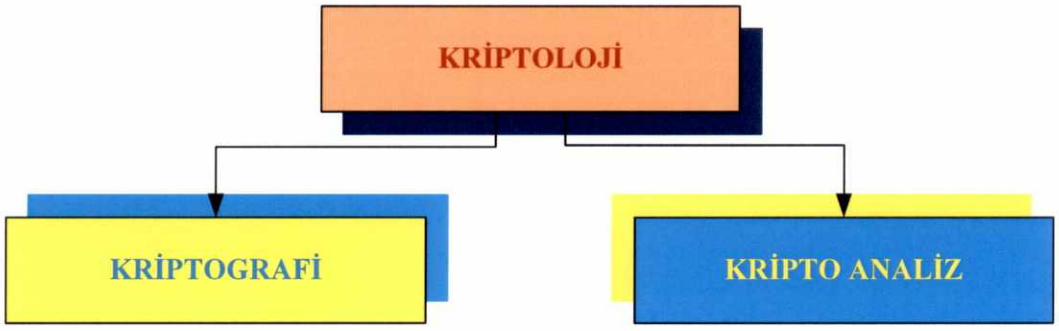
Kriptografi, kelime kökeni olarak Yunanca gizli/saklı anlamına gelen kryptós ve yazmak anlamına gelen gráphein kelimesinden türetilmiştir. Kriptografi, gizli yazı yazma bilimi ya da sanatıdır. Bu bilim çalışmasına da ***kriptoloji*** denir. Bu saha çift

---

[1] Bilgiyi değişik sembol veya harflerle ifade etmeye denir.

yönlüdür. Bir yandan gizli yazışma sistemlerini geliştirirken aynı anda oluşturulan bu sistemin kırılma çalışmaları da geliştirilmektedir. Bir kripto sisteminin kırılma işlemine de kripto analiz denir. (Şekil 1)

Şekil 1 Kriptoloji



Kaynak:Tübitak-Bilgem,2012

Geçmişte, kriptoloji bilgiyi yalnızca düşmandan gizlemek amacıyla kullanılmıştır. Günümüzde ise teknolojinin hayatımıza girmesiyle birlikte bilginin güvenliği çok daha önemli hale gelmiştir.

Bugün haberleşme teknolojisinde kullanılan (GSM Mobile telefonlar, sabit telefonlar, telsiz sistemleri, internet, e-mail, uydu v.b.) tekniklerin hepsi sıfır güvenlidir. Yani, güvenli bir haberleşme kanalı mevcut değildir.

Kriptografinin amacı, iki ya da daha fazla kişinin haberleşmesinde gizlilik, veri bütünlüğü, doğrulama ve inkar edememe esaslarını birleştirerek mesajın güvenli iletişimini sağlamaktır. Burada kişiler; insanlar olabileceği gibi, bilgisayar, telsiz, telefon v.b. cihazlar da olabilir.

Hayatın her alanında oldukça sık kullanımı olan haberleşme cihazları ile dünyanın en ücra köşesindeki bir bilgiye erişebilme kolay hale gelmiştir. Bilgilerin bu kadar kolay elde edilebilir olması, bilginin emniyeti, güvenirliği ve doğruluğunda çeşitli

zafiyetleri de beraberinde getirmiştir. Bu zafiyetlere; internet ortamındaki sanal alışverişlerde, şirketlerdeki firma casusluğunda, gereksiz e-postalardaki saldırı ve ataklarda rastlamak mümkündür. Bu konuda alınacak en önemli tedbir Kriptografi olmalıdır. Ticari faaliyetlerde, sabit ve mobil telefon ve telsiz haberleşmesinde, uydu haberleşmesinde, kamu kurum ve kuruluşlarda, özel sektörün iş faaliyetlerinde ve özellikle internet kullanımı ile ilgili konularında güvenli haberleşmede kripto büyük önem arz etmektedir (Çinem C, vd., 2007, s.7).

Bu değerlendirmeler ışığı altında tezde, elektronik haberleşme sistemlerinde güvenli haberleşmenin sağlanması amacıyla kullanılan kripto sistemlerinin tanımı, klasik kripto sistemleri, modern kripto sistemleri, ülke uygulamaları, ülkemizdeki mevcut durum değerlendirilmesi ve kullanılacak kripto sistemlerinde BTK'yı ilgilendiren hususlar ve uygulamaya yönelik öneriler getirilmiştir.

1. KLASİK KRİPTO SİSTEMLERİ

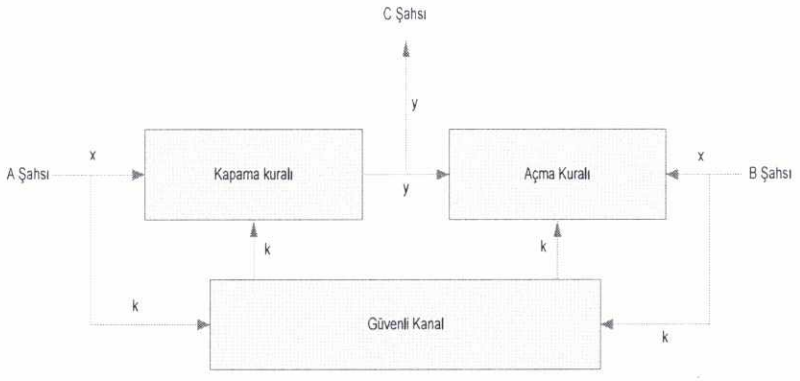
1.1. Klasik Kripto Sistemi Tanımı

Günümüzde, kriptografi metotları "***klâsik***" ve "***modern***" olmak üzere ikiye ayrılmaktadır. 1976 yılı kriptografi için bir milattır. Bu tarihten önce kullanılan kripto teknikleri ***klasik sistemler***, bu tarihten sonra kullanılan sistemler de ***modern sistemler*** olarak adlandırılmaktadır.

Zira 1976 yılında bilgisayarlar PC (Kişisel bilgisayarlar- Personel computer) olarak hayatımıza girmeye başlamışlardır. PC'ler sayesinde klasik kripto sistemlerinin kripto analiz çözümleri son derece kolay olmuştur.

Kısaca, bir klasik kripto sisteminin çalışma prensibi Şekil 1.1'den faydalanarak anlatalım:

Şekil 1.1. Klasik Kipto Sistemi



Kaynak: Şahin M,2007 (C şahsı düşman)

Aralarında haberleşme yapacak A ve B şahısları verinin güvenli iletilmesi için belirli bir kripto sistemi kullanmak için aşağıdaki protokole uyarlar. İlk olarak güvenli bir

kanal üzerinden rastgele bir $k \in \mathbf{K}$ anahtarı belirlenir (**K** anahtar uzayı, olası anahtarların bir kümesi).

Bu sistemde, açma ve kapama fonksiyonunda güvenli iletişim çözümü için tek bir gizli anahtar kullanmaktadır. Bu durum verilerin güvenliği için matematiksel açıdan daha az problem çıkaran bir yaklaşımdır ve çok kullanılan bir yöntemdir. Gönderilecek metin ile beraber alıcıya gizli anahtarın gönderilmesi gerekmektedir.

Zira dışarıdan gelen saldırılara karşı korumanın en etkili metodudur. Anahtarın her veri iletiminde değiştirilmesi ve saklanması bu sistemde en önemli sorundur. İşte bu gizli anahtar kripto sistemine kriptoloji de ***simetrik kripto sistem*** olarak adlandırılmaktadır. Simetrik kripto sistemi algoritmalarında çok hızlı bir şekilde kripto sistemi ve kripto çözme işlemlerini gerçekleştirebilmektedir.

Kabul edelim ki açık yazı,

$\boldsymbol{n \geq 1, n \in Z, x_i \in P}$ olmak üzere;

$\boldsymbol{x = x_1 x_2 x_3 \ldots\ldots x_n}$ olsun.

Önceden belirlenmiş $\mathbf{k} \in \mathbf{K}$ anahtarı ile tanımlanan $\boldsymbol{E_k}$ kapama fonksiyonu kullanarak her bir $\mathbf{x_i}$ hesaplanır.

A şahsı, $\boldsymbol{1 \leq i \leq n}$ için $\boldsymbol{y_i = E_k(x_i)}$ leri hesaplayarak,

$$\boldsymbol{y = y_1 y_2 y_3, \ldots\ldots y_n} \qquad (1.1)$$

kapalı yazısını kanal üzerinden B şahsına gönderir.

B şahsı $\boldsymbol{D_k}$ açma fonksiyonu kullanarak **y** kapalı yazısından

$$\boldsymbol{x = x_1 x_2 x_3 \ldots\ldots x_n} \qquad (1.2)$$

açık yazısını elde eder (Şahin M., 2007, s.4).

Bir kripto sisteminden beklenilen hususları daha iyi anlayabilmek ve bunlara çözüm getirmek için klasik kripto sistemlerinden birkaçını incelemek gerekmektedir.

1.1.1. Caesar kripto sistemi

Latin alfabesi kullanılarak yapılan en eski yerine koyma tekniklerinden biridir. Roma İmparatoru Julius Caesar tarafından, generalleri ile gizli haberleşme yapmak için kullanılmıştır. Modüler aritmetik (bkz. Ek-2) sistemi üzerine inşa edilmiştir.

Açık yazı ve kapalı yazı için türk alfabesini kullanalım.

$$P = C = K = Z_{29} \text{ olsun.}$$

Verilen bir $k \in K$ anahtarı için kapama ve açma fonksiyonları sırasıyla,

$$x, y \in Z_{29} \text{ için;}$$

$$E_k(x) := x + k \,(mod\ 29) \quad \text{(kapama fonksiyonu) ve} \qquad (1.3)$$

$$D_k(y) := y - k \,(mod\ 29) \quad \text{(açma fonksiyonu) olarak tanımlanır.} \qquad (1.4)$$

Buradan açma ve kapama fonksiyonlarının (Eş.1.1) özelliğini kolayca sağladığı gözükmektedir.

Örnek

" **BU GECE BULUŞALIM** " açık mesajını türk alfabesinde bir kodlama olan Tablo 1.1.'i kullanarak kapatmaya çalışalım. Kullanacağımız anahtarımız $k = 11$ olsun. Söz konusu açık mesajın kapama fonksiyonu;

$$E_k(x) = (x + 11)(mod\ 29) \text{ fonksiyonundan} \qquad (Eş.1.3)$$

Tablo 1.1. Türk alfabesinde bir kodlama

A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	
15	16	17	18	19	20	21	22	23	24	25	26	27	28	

Kaynak:Ekin A.Bülent,sunum

Tablo 1.1'den faydalanarak her harfi 11 harf sağa ötelediğimizde, " **BU GECE BULUŞALIM"** ifadesi,

B	U	G	E	C	E	B	U	L	U	Ş	A	L	I	M
1	24	7	5	2	5	1	24	14	24	22	0	14	10	15
11	11	11	11	11	11	11	11	11	11	11	11	11	11	11
12	35	18	16	13	16	12	35	25	35	33	11	25	21	26
J	F	Ö	N	K	N	J	F	Ü	F	D	İ	Ü	S	V

1. Satır: Açık mesaj
2. Satır: Kodlama
3. Satır: Kapama
4. Satır: Kapalı mesaj

kapama fonksiyonunu açık yazımıza uyguladığımızda , **"JFÖNKNJFÜFDİÜSV"** gibi anlamsız bir kapalı yazısını elde ederiz.

Caesar kripto sisteminde alfabeyi kaydırma işleminin temeli modüler aritmetiği (bkz. Ek-2) kullanarak sağlanmaktadır. Bir kapalı mesajı açık mesaj haline getirmek için ise algoritmanın tersi kullanılır, yani,

$$\mathbf{D_k\,(y)\ =\ (y-11)\ (mod\ 29)} \qquad \text{(Eş.2.4)}$$

açma fonksiyonu (her harfi 11 harf sola ötelemek) veya,

$$\mathbf{D_k\,(y) = (y+18)\ (mod\ 29)} \qquad \text{(Eş.2.4)}$$

(her harfe 18 eklemek) fonksiyonlarından birini kullanarak elde edilen anlamsız "**JF ÖNKNJFÜFDİÜSV**" kapalı yazısını kripto analiz ile açmaya çalışırsak (mod 29'a göre);

J	F	Ö	N	K	N	J	F	Ü	F	D	İ	Ü	S	V
12	35	18	16	13	16	12	35	25	35	33	11	25	21	26
18	18	18	18	18	18	18	18	18	18	18	18	18	18	18
30	53	36	34	31	34	30	53	43	53	51	29	43	39	44
B	U	G	E	C	E	B	U	L	U	Ş	A	L	I	M

BU GECE BULUŞALIM" açık yazısı elde edilecektir.

Kullanılan kripto sistemini gizlemek bize gizlilik sağlamayacaktır.

Güvenlik için anahtar sayısının büyük olması gereklidir, fakat yeterli değildir.)

1.1.2. Permütasyon kripto sistemi

Klasik kriptolama sisteminin bir diğeri de Permütasyon kripto sistemi yöntemidir. Permütasyon; **n** tane elemanın farklı sıralanışıdır. Dolayısıyla, **n** tane elemanın bütün permütasyonları sayısı **n!**'dir. Bu kripto sistemi bu haliyle yüzlerce yıl kullanılmıştır.

$$P = C = \{a, b, c, ç, \ldots\ldots y, z\}$$

$\{0, 1, 2, \ldots\ldots 28\}$ kümesinin bütün permütasyonlarını S_{29} ile gösterelim.

$$K = S_{29}$$

$\pi \in K$ için kapama ve açma fonksiyonları olmak üzere;

$$E_\pi(x) = \pi(x) \text{ kapama fonksiyonu} \quad (2.5)$$

$$D\pi(y) = \pi^{-1}(y) \text{ açma fonksiyonu} \quad (2.6)$$

olarak tanımlanır.

Örnek

"KORKMA HEDEFE ULAŞMAKTAN" açık mesajı Tablo 1.2.'de belirtilen permütasyon ile kapatıldığında **"YIVYEÇ DRLRTR YZÇNEÇYİÇG" kapalı** mesajı haline gelir.

Permütasyon yöntemi kullanılarak oluşturulan anahtar sayısı, mesajlaşılan dilin alfabesindeki harf sayısına bağlıdır.

Tablo 1.2. Permütasyon Tablosu

A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L
ç	f	h	j	l	r	t	ü	a	d	k	b	c	y	z
M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	
e	g	ı	m	ş	v	ğ	n	i	ö	o	p	u	s	

Kaynak: Ekin A.Bülent, 2009

Bu şekilde oluşan permütasyon sayısı 29!'dir.

$$29\ ! = 8\ 841\ 761\ 993\ 739\ 701\ 954\ 543\ 616\ 000\ 000\ (\ 31 \text{ basamaklı }\ )$$

8 nonilyon 841 oktilyon 761 septilyon 993 seksilyon 739 kentilyon 701 katrilyon 954 trilyon 543 milyar 616 milyon tane farklı anahtar bulunmaktadır. Kapalı metni ele geçiren bir kişi, hangi kripto alfabesi ile oluşturulduğunu ve kuralı bilmiyorsa düz metne ulaşabilmesi için olası tüm kripto alfabelerini denemesi gerekmektir. Bu kripto sisteminin kullanıldığı o dönemlerde bu işlemin çözümü imkânsız derecesinde ***zor***'dur. Çözümünde kullanılacak denemelerde insan ömrü yetmez. Bu nedenle o dönemlerde bu tür kullanım güvenli olmuştur. Fakat günümüzde bilgisayar teknolojileri sayesinde bu kripto alfabelerini çözmek oldukça kolaydır (Ekin, 2009, sunum).

Anahtarların tek tek denenerek metni açmak imkânsızdır. Öte yandan bu sistem Türkçe alfabenin frekans analizi kullanılarak kolayca çözülmektedir. Anahtar sayısı büyük olması güvenlik için yeterli olmadığı bu örnek ile görmüş olduk.

1.1.3. Afin kripto sistemi

$\boldsymbol{a, b} \in \boldsymbol{Z_{26}}$ olmak üzere;

$$\mathbf{E\,(x)\ =\ ax\ +\ b\ (mod\ 26)} \qquad (2.7)$$

ile tanımlanan fonksiyonlara ***"afin fonksiyonları"*** denir (Z_{26}: İngiliz alfabesi kullanılmıştır).
(**Not** : a = 1 alırsak Caesar kripto sistemi elde edilir.)

Kapama fonksiyonu 1-1 fonksiyon olmalıdır. Bu yüzden kapama fonksiyonu 1-1 afin fonksiyonları kullanacağız.
Şimdi **E** fonksiyonunun hangi durumlarda 1-1 olacağını inceleyelim:

$\forall y \in Z_{26}$ için;

$$ax + b \equiv y \,(\mathbf{mod26}) \tag{2.8}$$

kongrüansı[2] hangi durumlarda bir tek **x** çözümüne sahip olur?

$$ax + b \equiv y \,(\mathbf{mod26}) \Longrightarrow ax \equiv y - b \,(\mathbf{mod\ 26}) \tag{2.9}$$

y, Z_{26} üzerinde değişirken **y – b** 'de Z_{26} üzerinden değişir. Dolayısıyla,

$\forall y \in Z_{26}$ için,

$$ax \equiv y \,(\mathbf{mod\ 26}) \tag{2.10}$$

olacak şekilde bir tek $x \in Z_{26}$ vardır.

$$\Longleftrightarrow \qquad \mathbf{ebob}\,(a, 26) = 1 \qquad \text{(Bkz. Ek-3)}$$

Sonuç olarak, a = 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25 sayılarından herhangi biri olabilir. **b,** Z_{26}'da herhangi bir sayı olabilir. Afin kripto sisteminde anahtarımız (a,b) ikilileri olmalıdır. Dolayısıyla afin kripto sisteminde 12 x 26 = 312 tane olası anahtar vardır. Bu sayı güvenlik için oldukça küçüktür.

$$\mathbf{P} = \mathbf{C} = Z_{26},$$

$$\mathbf{K} = \{(a, b) \in Z_{26} \times Z_{26} : \mathbf{ebob}\,(a, 26) = 1\}$$

$k = (a, b) \in K$ için kapama ve açma fonksiyonları sırasıyla,

$\forall x, y \in Z_{26}$ için;

---

[2] Uyma, uygunluk, ahenk

$$E_k(x) = ax + b \pmod{26} \qquad \text{(Eş.2.7)}$$

(kapama fonksiyonu) ve

$$D_k(y) = a^{-1}(y - b) \pmod{26} \qquad \text{(Eş.2.6)}$$

(açma fonksiyonu) olarak tanımlanır.

Örnek

Anahtarımızı $k = (7, 3)$ olarak seçelim.

O halde, kapama fonksiyonu;

$$E_k(x) \equiv 7x + 3 \pmod{26} \text{ olur.} \qquad \text{(Eş.2.7)}$$

(İngiliz alfabesinde kodlama ile)

$$7^{-1} \equiv 15 \pmod{26} \text{ ise açma fonksiyonu,} \qquad \text{(Eş.2.6)}$$

$$D_k(y) \equiv 15(y - 3) \equiv 15y - 19 \pmod{26} \text{ olur.} \qquad \text{(Eş.2.11)}$$

Şimdi **"K O T"** açık yazısını k anahtarı Tablo 1.3'ü kullanarak kapatalım:

Tablo 1.3. İngiliz alfabesinde kodlama

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

Kaynak: Ekin A.Bülent, 2009

Tablo 2.3.'den, K, O ve T harflerine karşılık gelen sayılarla kapama fonksiyonu denklemini kullanarak (Eş.2.8) kapatırsak,

x	=	**K**	**O**	**T**
		10	14	19
		7 . 10 + 3 (mod 26)	7 . 14 + 3 (mod 26)	7 . 19 + 3 (mod 26)
		21	23	6
y	=	**V**	**X**	**G**

x = "**K O T**" açık yazısı için y = "**V X G**" kapalı yazısı elde edilir.

$$\mathbf{D_k\,(y) \equiv 15y - 19\ (mod\ 26)} \qquad \text{(Eş.2.11)}$$

"**V X G**" kapalı yazısını (Eş.2.11)açma fonksiyonu kullanarak ***y kapalı*** yazısından, " **K O T**" ***x açık*** yazısını elde ederiz.

Afin kripto sisteminin permütasyon kripto sisteminin özel bir hali olduğu bu örnekte açıkça görülmektedir. Burada dikkat edecek olursak bir harf kapatıldığında alfabedeki diğer harfe dönüşmektedir. Örnekte afin kripto sisteminde kullanılan dilin frekans analiz yöntemi ile kolayca çözülmektedir

1.1.4. Kripto analiz

Kripto sisteminin kapama ve açma fonksiyonu hakkında herhangi bir bilgiye sahip olmadan, kapalı ve açık mesajları inceleyerek, bilmediğimiz bir kripto sistemindeki kapalı yazıdan anahtarı tespit etme çalışmalarına " ***Kripto Analiz*** " denir (Ekin B.A., 2009, sunum) .

Kripto analiz çalışması sırasında kripto analiz yapanın elinde çoğu zaman çok az bilgi vardır. Bu bilgiler,

- Kriptolanmış mesaj analizi
- Tam bir açık mesajın analizi

- Yarım olarak elde edilmiş açık mesajın analizi
- İstenen açık mesajın kriptolanmış halinin analizi
- Kriptolu mesajın kriptolanmış algoritması bilinerek analizi
    - Kaba kuvvet yöntemi
    - Diferansiyel kriptoanaliz

olabilir (TÜBİTAK-Uekae, 2008).

Yazıldığı dili bildiğimiz kriptolu bir mesajı çözmek en azından kolaydır. Aynı dilde yazılmış uzun bir metni bulup her bir harfin kullanım sıklığına göre hesaplanabilir. Buradaki mantık, metinde en sık kullanılan harf, kriptolamada en çok kullanılan harfe karşılık gelmektedir.

Aynı işlem sık kullanılan her harf içinde yapılır. İşlem sonucunda mesajdaki harfler ortaya çıkmış olur. Bu kriptoanaliz[3] yöntemine aynı zamanda frekans analizi adı verilmiştir. Zira bir dildeki her harfin bir kullanım sıklığı, yani frekansı vardır. Türkçe ve İngilizceyi karşılaştırdığımızda; Türkçe de frekans "A" İngilizce de "E" harfidir.

Dilin bu harf frekansları elde etmekle kripto sistemi çözmek uzun zaman almayacaktır. Ayrıca, kriptoanaliz de harflerin sesli, sessiz, ikili, üçlü gibi bulunuş karakteristiklerine de bakılarak çözüme ulaşmak mümkündür.

Çinem (2007, s 30-33) kripto analiz çözümünde farklı bir yaklaşım ile,

> Harflerin frekansları kısa metinler üzerinden hesaplanırsa, bulunan sonuçlar genelde frekans tablosundaki değerden büyük sapma gösterebilir veya tablodaki harflerin kullanım sıklıkları değişebilir, görüşündedir.

[3] Kriptoları çözme bilimi; kriptografik teknikleri alt etmek için yapılan matematiksel çalışmalar.

Kripto analizlerce İngiliz alfabesi üzerine yapılan araştırmalarda; dergiler, romanlar, gazeteler, makaleler ve raporlar kullanılarak ingiliz alfabesindeki 26 harfin istatistiksel olarak hangi sıklıkta (frekans analizi) gözüktüğü hesaplanmıştır. Bu 26 harfin bulunma olasılıkları listelemesinde;

1. E harfinin yaklaşık 0.120 olasılığa,
2. T, A, O, I, N, S, H, R harflerinin 0.06 ve 0.09 arasında olasılığa,
3. D, L harflerinin yaklaşık 0.04 olasılığa,
4. C, U, M, W, F, G, Y, P, B harflerinin 0.015 ve 0.028 arasında olasılığa,
5. V, K, J, X, Q, Z harflerinin 0.01'den daha az olasılığa,

sahip olduğu tespit edilmiştir.

İngiliz alfabesindeki 26 harften "TH" ve "TE" ikilileri (digrams) en çok sıklıkta görünen ikililerdir. "THE" üçlüsü (trigrams) en çok sıklıkta görünen üçlüdür (Stinson 1995).
(**Not** : Eğer yeterince uzun kapalı yazıya sahipsek afin kripto sistemini kırmak için de frekans analiz metodunu kullanabiliriz.)

Örnek

İngiliz alfabesinde 26 harfi kullanarak afin kripto sistemi ile kapatılmış **"FMRXVEDKAPHFERBNDKRXRSREFMORUDSDKDVSHVUFEDKAPRKDLYEVLRHHRH"**
kapalı yazısından açık yazıyı frekans analizi (kripto analiz) kullanarak açmak isteyelim.

Çözüm olarak;

Kapalı yazıda en sık görünen karakterleri listelendiğinde;

R: 8, D:7, E, H, K:5, F, S, V: 4 defa kapalı yazıda görülecektir.

E ve T harfleri bir ingilizce metinde en sık görülen harfler olup, tahmin yapıldığında;

R, E'nin ve D; T nin kapatılmış hali olsun.

Harflerin dijital karşılıklarını kullanırsak;

$$E_k(4) = 17 \quad \text{ve} \quad D_k(19) = 3$$

olarak tahmin yapabiliriz.

(Bkz. Tablo 2-3'den E'nin değeri 4, R'nin değeri 17, D'nin değeri 3 ve T'nin değeri de 19 olduğu görülecektir.)

Afin kripto sistemde kapama fonksiyonu;

$$\mathbf{E_k(x) = ax + b \ (mod\ 26)'dır.} \qquad \text{(Eş.2.7)}$$

Buradaki amaç bilinmeyen a ve b sayılarının bulunması yani anahtarı bulmaktadır. Tahminlerimizi kapama fonksiyonunda yerine yazarsak iki bilinmeyenli iki doğrusal denklem elde ederiz.

$$\mathbf{4a + b = 17}$$

$$\mathbf{19a + b = 3}$$

Bu sistem tek bir çözüme sahip;

$$\mathbf{a = 6 \quad ve \quad b = 19 \ (a, b \in Z_{26})}$$

$$\boldsymbol{ebob\ (a, 26) = 2 > 1} \text{ (bkz. Ek-3)}$$

olup tahminimiz yanlış çıkmıştır. Bu durumda frekans analizi kullanarak başka bir tahmin yapmak gerekmektedir. Bu durumda bu sefer;
R, E'nin ve K, T'nin kapatılmış hali olduğunu kabul edelim.

Yine kapama fonksiyonunda tahminlerimizi yerine yazarsak iki bilinmeyenli iki doğrusal denklem elde ederiz. Bu denklemlerin tek bir çözümü vardır;

$$\mathbf{a = 3 \text{ ve } b = 5}$$

$\mathbf{ebob\,(3,26) = 2 > 1}$ olduğundan,

$$\mathbf{D_k(y) = 9y - 19} \qquad \text{(Eş.2.11)}$$

açma fonksiyonu kullanarak açık yazıyı elde ederiz.

"algorithms/are/quite/genereal/definitions/of/arithmetic/processes"

Şahin (2007, s 11) kripto analiz çözümündeki ifadesinde,

> Eğer anlamlı bir metin elde edemediysek tahminlerimiz anlamlı bir metin buluncaya kadar devam edeceğini " söylemektedir.

1.1.5. Vigenere kripto sistemi

Vigenere kripto sistemi adını 16. yy da yaşamış Blaise de Vigenere'den almıştır. Şimdiye kadar gördüğümüz kripto sistemlerinde bir anahtar seçildikten sonra açık yazıdaki her bir harf kapalı yazıdaki tek bir harfe dönüştürülmüştür. Bu tür sistemler

"***mono alfabetik***" [4] kripto sistemleri olarak ifade edilir. Bütün bu sistemlerde kullanılan dilin frekans analizi ile çözüme ulaşmak kolaydır

Vigenere kripto sisteminde; **k** anahtarı ve **m** uzunlukta bir anahtar kelime kullanılır. Açık yazı **m** uzunluğunda bloklara ayrıldıktan sonra her bir defasında **m** tane harf kapatılır. Bu tip kripto sistemlere de "***poli alfabetik***"[5] kripto sistemleri denir. Zira, bir harf alfabede birden fazla harfe dönüşmektedir. Genel olarak poli alfabetik sistemin kripto analizi mono alfabetik sistem kripto analizinden zordur (Şahin M.,2007, s 11).

Yukarıda anlatılan diğer kripto sistemlerine nazaran daha zor kırılabilen Vigenere kripto sistemini;

$$\mathbf{m} \in \mathbf{Z}\ \textbf{olsun.}\ \mathbf{P} = \mathbf{C} = \mathbf{K} = (\mathbf{Z_{26}})^{\mathbf{m}} \text{ olmak üzere,}$$

$$\mathbf{Z_{26}}\ \mathbf{x},\ \mathbf{Z_{26}}\ \mathbf{x},\ldots\ldots\ldots,\ \mathbf{Z_{26}}\ \mathbf{x}$$

$$\mathbf{k} = (\mathbf{k_1}, \mathbf{k_2}, \ldots\ldots\ldots, \mathbf{k_m}) \in \mathbf{K} \text{ için,}$$

kapama ve açma fonksiyonları sırasıyla,

$$\mathbf{E_k}(\mathbf{x_1}, \mathbf{x_2}, \ldots\ldots \mathbf{x_m}) \coloneqq (\mathbf{x_1} + \mathbf{k_1}, \mathbf{x_2} + \mathbf{k_2}, \ldots\ldots \mathbf{x_m} + \mathbf{k_m})\ \textbf{(mod 26)} \qquad (2.12)$$

(kapama fonksiyonu) **ve**

$$\mathbf{D_k}(\mathbf{y_1}, \mathbf{y_2}, \ldots\ldots \mathbf{y_m}) \coloneqq (\mathbf{y_1} - \mathbf{k_1}, \mathbf{y_2} - \mathbf{k_2}, \ldots\ldots \mathbf{y_m} - \mathbf{k_m}) \qquad (2.13)$$

(açma fonksiyonu)

olarak tanımlanırlar.

---

[4] Bir anahtar seçildikten sonra açık yazıdaki her bir harf kapalı yazıdaki tek bir harfe dönüştüren kripto sistemi

[5] Bir açık yazının m uzunluğundaki bloklara ayrıldıktan sonra her defasında m tane harf ile kapatılmasına denir.

Bu kriptografide düz metin deki her bir harf ayrı bir kripto alfabesi ile kapatılır. Hangi alfabenin seçileceğine anahtar sözcüğe bakılıp karar verilir. Böylece düz metindeki aynı sözcükler için farklı metinleri oluşur ve bu da frekans analizinin basit tek başına uygulanmasına engel olur. Uzun yıllar güvenilirliğini korumuştur (Çinem vd.,2007, s.34-35)" . (**Not:** Vigenere kripto sistemi mono alfabetik bir kripto sistemi değildir.)

Örnek

k: SEVGİLİM (21, 5, 26, 7, 11, 14, 11, 15) ve blok sayısını **m = 8** açık mesajı **"LALE BENİM KARIM DİĞER YARIM"** olan bir kelime seçelim.

Bu ifadeyi, **8** uzunluğunda bloklara ayrılması ve her bir defasında **8** tane harf ile kapatılması gerekmektedir. Anahtar kelimeyi **8** uzunlukta böldüğümüzde

"LALEBENİ – MKARIMDİ - ĞERYARIM" anahtar kelimesi elde edilecektir. Bu da sekizli bloklar halinde

Tablo 1.4.'e göre kodlanırılırsa;

Tablo 1.4. Türk Alfabesinde bir kodlama

A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	
15	16	17	18	19	20	21	22	23	24	25	26	27	28	

Kaynak: Ekin A.Bülent,2009

L	A	L	E	B	E	N	İ
14	0	14	5	1	5	16	11
21	5	26	7	11	14	11	15
6	5	17	12	12	19	27	2
F	E	O	J	J	P	Y	B

M	K	A	R	I	M	D	İ
15	13	0	20	10	15	4	11
21	5	26	7	11	14	11	15
7	18	26	27	21	0	15	7
G	Ö	V	Y	S	A	M	G
Ğ	E	R	Y	A	R	I	M
8	5	20	27	0	20	10	15
21	5	26	7	11	14	11	15
0	10	17	5	11	5	21	1
A	I	O	E	İ	E	S	B

"FEOJJPYBGÖVYSAMGAIOEİESB" anlamsız bir kapalı metin elde edilir.

Buradaki m uzunluğundaki olası anahtar sayısı türk alfabesini kullandığımız için 29^{m}'dir. Örneğin m = 8 için K > 10^{7}' olacaktır ki bu rakam oldukça büyüktür. Bu mesajın çözümü de o zamanki koşullarda zordur. Fakat günümüzde bilgisayar istatistiki yöntemler ile sistem kolayca çözülmektedir. (Şahin M., 2007, s.12).

1.2. Gizli Haberleşmede Göz Önüne Alınması Gereken Hususlar

Klasik kripto sistemlerinde anahtar yönetimi en önemli sorunlardan biridir. Çünkü güvenli bir kanala ihtiyaç olacağından ama gerçek hayatta güvenli bir kanal olmayacağından anahtar alışverişlerinin yapılması mümkün değildir.

Bir Network çalışmasında bir grup insanın birbirleriyle güvenli iletişim yapmak istediklerinde, grupta bulunan her insan çifti için farklı bir anahtar belirlenmesi gerekmektedir. Örnek olarak, grupta 8 kullanıcı olduğu düşünürsek, $\binom{8}{2} = 28$ farklı anahtara ihtiyacımız olacaktır. Eğer 50 kullanıcı varsa $\binom{50}{2} = 1225$ anahtara ihtiyacımız olacaktır. Kullanıcı sayısının artmasına bağlı olarak bu kadar büyük sayıdaki anahtarın taşınması ve muhafazası anlamında sorunlar getirecektir.

Şahin M.,2007, s16) anahtar paylaşımı ile ilgili verdiği örnekle anahtarın önemini ortaya koymaktadır.

> "Klasik kripto sistemlerinde bir başka sorun karşılıklı güvendir. Örneğin, A ve B şahısları aynı anahtarı paylaşsınlar. Eğer C şahsı gizli anahtarı elde ederse, B şahsı gibi A şahsına mesaj gönderebilir. A şahsının bu mesajı B şahsından gelip gelmediğini bilme imkânı yoktur.
>
> Üstelik C şahsı mesajı değiştirip yeniden göndermiş olabilir. Bu durumda B şahsı gönderdiği mesajın değiştirildiğini fark etmesi zordur. İnternet üzerinden yapılan bankacılık,- e-ticaret ve e-imza durumlarda bunlar çok önemlidir. Bir banka müşterisi yaptığı bir işlemi yalanlayamazken, müşteri de bankanın kendisi adına bir işlem yapmadığından emin olabilmelidir" denilmektedir.

Bir kripto sistemin kripto analiz olarak güvenli olmasının yanında aşağıdaki hususları da dikkate almamız gerekir.

1. **Anahtar Yöntemi:** Haberleşecek taraflar arasında anahtar alışverişi,
2. **Kimlik Doğrulama:** Mesajı alan kişinin mesajın kimden geldiğini belirleyebilmesi,
3. **Mesaj Bütünlüğü:** Mesajı alan kişi mesajın kanal üzerinde değiştirilip değiştirilmediğinin belirlenmesi,

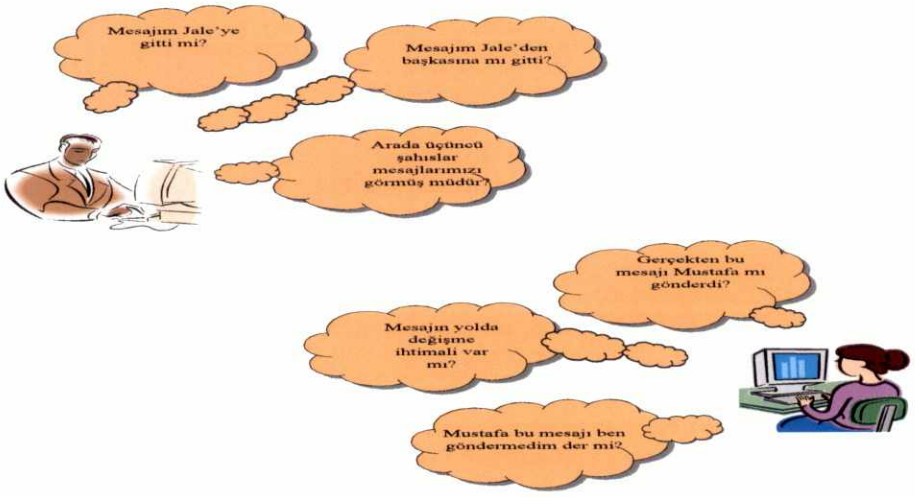
4. **Reddetme:** Mesajı gönderen kişinin gönderdiği mesajı kendisinin göndermediğini iddia etmesini,

olarak sıralayabiliriz.

Göz önüne alınması gereken hususları

Şekil 1.2 Göz önüne alınması gereken hususları gösterilmiştir.

Şekil 1.2 Göz önüne alınması gereken hususları



Kaynak:KARA O, Tübitak-Bilgem, 2012

İnkar edememeye ile bir örnek verecek olursak

Örnek

Mustafa ve Jale hafta sonu için; Jale sinemaya, Mustafa da futbol maçına birlikte gitmek istediklerini varsayalım. Telefonda herkes kendi isteklerinde ısrarlı ve diğerini ikna etmeye çalışmaktadır. Jale sinemaya, Mustafa futbol maçına gitmeye kararlı. Çözüm için yazı-tura atma fikri ortaya atılıyor. Jale bu fikri kabul ederken Mustafa'nın tereddütleri vardır. Mustafa'nın bu tereddütlerden kurtulmasında kriptografi devreye girmektedir.

Matematikte sihirli fonksiyonlar olarak adlandırılan fonksiyonlar vardır. Bu fonksiyonların değeri x verildiği zaman kolayca hesaplanabilir, fakat fonksiyonun değeri verildiği zaman x'in hesaplanması çok zordur. Şimdi kahramanlarımızın kullanacakları fonksiyonu; f (x) = x5 + x olsun.

Matematikte ikinci, üçüncü ve dördüncü değerlerin denklemlerinden kökleri bulmak için formüller olduğu halde beşinci dereceden kök bulma formülü olmayacağı ispatlanmıştır. Burada x değerinin tek mi çift mi olduğunu tahmin etmek % 50'dir. Bu da yazı-tura atılmasında, yazı mı tura mı gelme olasılığı ile aynıdır.

Sorunun çözümünde, Mustafa ve Jale telefon sanal ortamında yazı tura oynamaya başlıyorlar. Jale ve Mustafa açık anahtar kripto sistemi kapsamında, yukarıdaki f (x) fonksiyonunu seçmiş olsunlar. Burada x'in tek sayıda tura, x'in çift sayıda yazı olması konusunda da anlaşmış olsunlar. Jale içinden x = 16 gibi bir sayı tutsun.

Bu tuttuğu sayıyı ortak bilinen formülde yerine koyduğunda; yani (16)'yı hesaplayıp bulduğu 1048592 sayısını Mustafa'ya telefonda söylesin. Bu arada Jale yazı tura atarak Mustafa'ya soruyor yazı mı tura mı? Denklemden (x5 + x – 1048592 = 0) Mustafa'nın x'i o anda hemen bulma şansı neredeyse yok gibi. Bu yüzden sayının tek mi çift mi olduğuna tahmin ederek karar vermeli. Bu tahmini yaparak Jale'ye söylüyor.

Mustafa verdiği tahmin sonucunun doğruluğunu test etmek için Jale'nin kullandığı x sayısını öğrenip, fonksiyonda x sayısın yerine koyduğunda, çıkan sonuçla Jale'nin gönderdiği sonucu karşılaştırmasını yapıyor. Bu noktada Jale, Mustafa'yı asla kandıramaz, zira x değerini sonradan değiştirme şansı yoktur. Bu herkes tarafından bilinen sihirli fonksiyon sayesinde Jale ve Mustafa güvenli bir şekilde yazı-tura oynaması sağlanmıştır.

Bunun bir anlamı da şudur, telefonda Jale ve Mustafa'yı dinleyenlerin; sayıları ve fonksiyonu bilmeleri sonucun yazı mı tura mı olduğunun anlamaları mümkün değildir. Zira, çift veya tek sayının ne anlama geldiğini hiçbir zaman bilemeyeceklerdir.

1.3. Gizli Haberleşmede Göz Önüne Alınması Gereken Hususların Çözümü

Bilgisayarın keşfi ile birlikte insanlar arasındaki iletişimin ortamının yeniden şekillenmesi, haberleşme alanında güvenlik kavramına yeni bir boyut kazandırmıştır.

Bir grup araştırmacı 1970 yılında IBM laboratuarında daha önce Demon adı verilen, daha sonra Lucifer diye adlandırılan ve 64 bitlik anahtar kullanılan kripto sistemini geliştirmişlerdir. Bu sistem ABD'de "***Bilgi İşleme Standardı***" olarak seçilmiştir. Bunu sağlayacak algoritmanın ismi de bu büro tarafından ***Veri Kriptolama Standardı (DES)*** olarak belirlenmiştir. DES yapısı itibarı ile blok şifreleme örneğidir.

Bilgisayarlarda harflerin "**bit**"[6]lerle ifadesi ve sonucunda kriptolamanın da bitlerle yapılması ***modern kriptografinin*** başlangıcı olmuştur. Genel bir ifadeyle DES, ikilik tabanda (bkz. Ek-5) olan düzmetin 64 bit'lik parçalar, yani bloklar halinde, 56 bit'lik anahtar kullanarak kripto işlemi yapmaktadır. Yayılma ve karıştırma özelliklerine sahip olan DES algoritmasında her bloğun her bit'i diğer bit'lere ve anahtarın her bit'ine bağımlıdır.

64 bit'lik bir düz metin bloğu üzerinde sadece bir bitin değeri değiştirilirse, tamamen farklı bir metin elde edilir. Bundan dolayı anahtar üzerindeki tahmin edilememezlik çok önemlidir ve kripto analizi zorlaştıran bir etkendir.

Karıştırma sayesinde her anahtarın açık ve kapalı yapıları arasında istatistiksel bağlantı olmamasını sağlanır. Bu durum, düşmanın eline geçen düz metin ve düz metinin kırılması ile ele geçecek metin arasında bir bağlantı kuramayacağından anahtar hakkında tahminde bulunması imkânsızdır. Bu özellikler, DES'in güvenliğini artıran önemli özelliklerinden biridir.

---

[6] İkili tabandaki sayı sistemindeki basamağa verilen addır.

Bilgisayarda yazdığımız yazılar harflerden oluşmaktadır, fakat kullanırken klavyede bastığımız her tuşun bilgisayar içinde temsil şekli başkadır. Bilgisayarlardaki bu karakterler ikilik sayı sisteminde 8 haneli bir sayı ile ifade edilir.

Bu sayının her bir basamağına bilgisayar dilinde daha önce de bahsettiğimiz gibi bit denir. Bit 0 ya da 1 değerini alabilir ve doğru/yanlış gibi düşünülebilecek karşıt iki durumu belirtmekte kullanılır. Örneğin, E harfinin bilgisayar içindeki temsili 01000101 şeklindedir. Bu ASCII tablosunda E'nin 69'a denk gelmesi ve ikilik tabanda ifadesidir. ASCII tablosunda toplam 256 karakter vardır; bu da 2^8 sayısında eşittir. Yani, sekiz haneli bitlerden oluşmuş sayıların olası bütün durumları için ASCII tablosunda bir karakteri vardır.

2. MODERN KRİPTO SİSTEMLERİ

Klasik kripto sistemlerinde anahtarın her veri iletiminde değişmesi probleminden bahsetmiştik. Bu konunun çözümünde milat olarak kabul edilen 1976 yılında Diffie ve Hellman anahtar alış-verişi protokolünü önermişlerdir.

Bu yeni sistem ile klasik kripto sistemi yerini modern kripto sistemine geçişin dönüm noktasıdır. Anahtar değişim algoritması ile, sayılar teorisinin uzun yıllardır bilinen ama kullanılmayan özellikleri ortaya çıkmıştır.

Diffie-Hellman, kriptografinin temel tabularından birini yıkarak, güvenli bir kanal üzerinden alıcı ve göndericinin gizli bir anahtar üzerinde anlaşmaları için bir araya gelmek zorunda olmadıklarını kanıtlamıştır.

Sayılar teorisini kullanarak anahtar değişimi işleminin herkese açık bir şekilde yapılabileceğini göstermiştir. Diffei-Hellman anahtar değişim algoritması, simetrik kripto sistemi (gizli anahtar) anahtar dağıtım sorununa güvenilir bir çözüm getirmekle birlikte, yeni bir tanımı da ortaya atmıştır. Asimetri kripto sistemi (açık anahtar).

Asimetri (açık anahtar) kripto sisteminin temelinde herkesin birbirlerini tanımadan bile gizli bir şekilde haberleşmesini sağlamaktadır. Klasik kripto sistemi o döneme kadar tasarlanan bütün sistemlerde kullanılan anahtarın taraflarca bilinmesini gerekirken, modern kripto sistemde kişilerin sadece kendilerinin bildiği özel anahtarı yeterlidir.

Modern kripto sistemlerinin en büyük avantajı, veri güvenli iletişim ve bu güvenli iletişimin çözümü işlemlerini yapmasının yanında elektronik imza gerçekleştirilmede kullanılmasıdır. Aldığımız bir güvenli iletişim ve bu güvenli iletişimin çözümü işlemini gerçekleştirdikten sonra karşılaşacağımız en büyük problem bu güvenli

metnin bize doğru kişiden gelip gelmediğidir. Metnin doğruluğu elektronik imzalar sayesindedir.

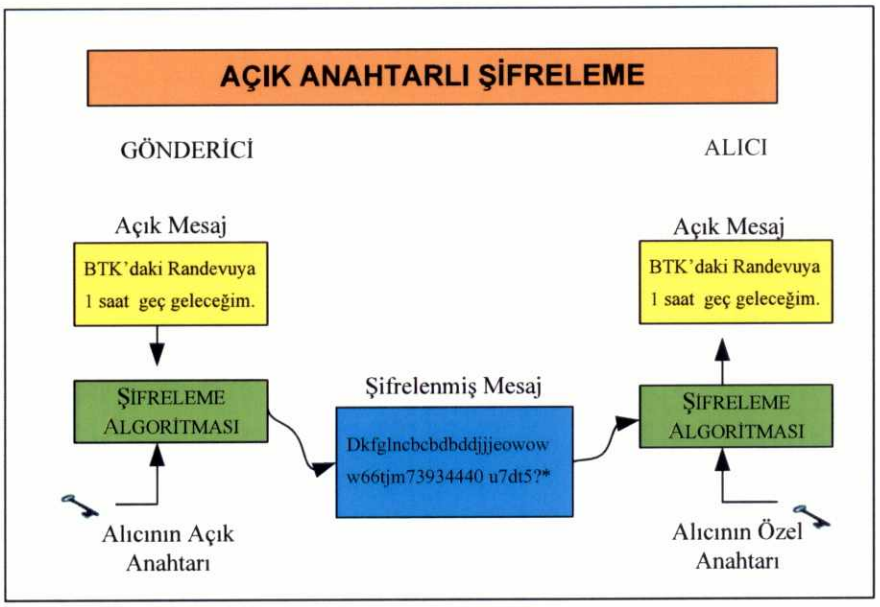
Modern algoritmalar da (açık anahtarlı) kripto sisteminde kullanılan anahtar ile kripto analizinde kullanılan anahtar birbirinden farklıdır. Anahtar çiftlerinin algoritmaları matematiksel özelliklerinden dolayı açık anahtar çifti her kullanıcı için farklıdır. Bu algoritmalara açık anahtarlı kripto sisteminin denilmesinin nedeni anahtarın genel kullanıma (kamuya/halka) açık olmasıdır.

A şahsının bir mesajı kriptolamak için kullandığı anahtar, ancak kripto analizi elinde bulunan B şahsı tarafından çözülebilir. Kripto analiz çözüm anahtarları özeldir. Yani gizlidir. Simetrik sistemler için de gizli anahtar kelimesi kullanıldığından, bu anahtara özel demek daha doğru olacaktır (Kodaz H. vd.,2010).

Yukarıda da bahsedildiği gibi A şahsı tarafından iletilecek kriptolu bir mesaj, sadece ona ait özel anahtar ile çözülür. Özel anahtarla atılan bir elektronik imzanın doğruluğu da, kişiye ait özel anahtar ile mümkündür. Bir kullanıcının açık anahtarıyla şifrelenen bir mesaj, yalnız ve ancak ona ait özel anahtar çözebilmektedir.

Aynı şekilde, herhangi bir kullanıcının özel anahtarıyla attığı sayısal imzanın doğrulanabilmesi, yalnızca o kullanıcının açık anahtarını kullanarak mümkün olabilmektedir. Açık anahtarlı kripto sistemlerinin blok diyagramı Şekil 2.1'de anlatılmaktadır (Kodaz H. vd.,2010).

Şekil 2.1. Açık anahtarlı kriptolama



Kaynak: TÜBİTAK-Bilgem,2012

Günümüzde kullanılan modern kripto sistemler matematikte hesaplanması zor problemler üzerine inşa edilirler. Güvenliği DLP (Diskret Logartima Problemi)'nin zorluğuna dayanan birçok kriptografi uygulaması vardır (Bkz. Ek-1). Bu uygulamalardan bazıları,

- Anahtar-Değiş tokuşu (Diffie and Hellman 1976)
- Açık anahtar kripto sistem (ElGamal 1985)
- Akıllı kartlar için kimlik tanımlama ve imza (Schorr 1989)
- Kimlik tanımlama şemaları (Brickell and McCurley 1990)
- Dijital imza şeması (ElGamal 1984)
- Rastgele üreteçler (Sundaram 1998) şeklinde listelenebilir.

2.1. Diffie- Helman Anahtar Alışverişi

Diffie ve Hellman, kriptografinin temel tabularından birini yıkarak alıcı ve göndericinin gizli bir anahtar üzerinde anlaşmaları için bir araya gelmek zorunda olmadan güvenli bir kanala ihtiyaç duymadan birbirleri ile anahtar paylaşımlarına dair bir sistem oluşturmuşlardır.

Bu oluşturdukları anahtar ile kripto sistemi açık anahtar temelini oluşturmuştur. Açık anahtar kripto sistemlerde anahtar iki parçadan oluşmaktadır. Bir parçası herkes tarafından, diğeri ise alıcı tarafından bilinmektedir. Bu sebeple anahtar paylaşımına ihtiyaç olmadığından açık anahtar kripto sistemi denilmektedir.

Bu sistemin matematiksel olarak ifadesi ise şöyledir.

Matematiksel olarak anahtar alışverişi tanımı şöyle yapılmaktadır. A ve B şahıslarının gizli bir anahtar belirlemek istediklerini düşünelim. A ve B şahısları p bir asal sayı ve **g** de modülo **p**'ye göre bir primitif kök olsun. **p** ve **g** herkes tarafından bilinsin. Anahtar alış verişi protokolü aşağıdaki gibidir.

A şahsı, $\mathbf{0 < a < p-1}$ olacak şekilde rastgele bir a tam sayısını (gizli) seçer, sonra

$\mathbf{u = g^a \pmod p}$ sayısını hesaplar ve u sayısını B şahsına gönderir. (2.1)

B şahsı, $0 < b < p-1$ rastgele bir b tam sayısını (gizli) seçer, sonra

$\mathbf{v = g^b \pmod p}$ sayısını hesaplar ve v sayısını A şahsına gönderir. (2.2)

B şahsı $\mathbf{u^b \pmod p}$ sayısını hesaplayarak ortak anahtar elde eder.

A şahsı $\mathbf{v^a \pmod p}$ sayısını hesaplayarak ortak anahtar elde eder.

$$\mathbf{u^b \equiv (g^a)^b \equiv g^{ab} \pmod p} \quad (2.3)$$

$$\mathbf{v^a \equiv (g^b)^a \equiv g^{ab} \pmod p} \quad (2.4)$$

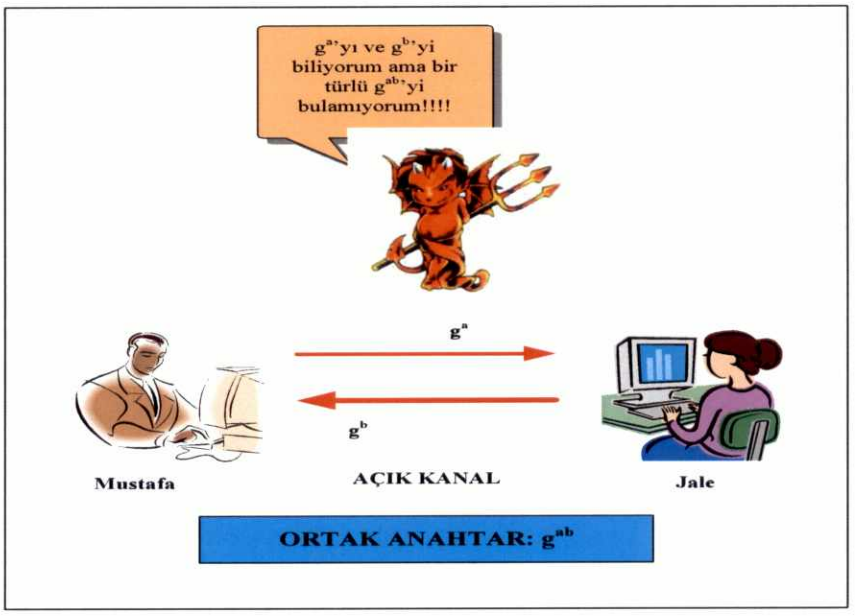
Ortak anahtar k sayısını $\mathbf{k: = g^{ab}\ (mod\ p)}$ (2.5)

Dolayısıyla, $\mathbf{u^b\ (mod\ p) = k = v^a\ (mod\ p)}$ olduğundan, (2.6)

DPL logartima problemine dayanır ki, bunun da çözümünün zor olduğundan bahsetmiştik.

Örneğin 15 kişilik bir network iletimi kullanılarak yapılacak bir haberleşmede anahtar sayısı büyük ölçüde azalacaktır. Eğer bu network paylaşımında klasik kripto sistemi kullanılsaydı 15 kişi için $\binom{15}{2} = 105$ anahtar kullanılacakken, modern kripto sisteminde ise 15 x 2 = 30 tane anahtar kullanmış olmaktadır (Şahin M., 2007, s 13).

Şekil 2.2. Diffie-Hellman Anahtar Paylaşım Protokolü



Kaynak: TÜBİTAK-Bilgem,2012

Örnek

Şimdi herkes tarafından bilinen $\boldsymbol{g}$ ve $\boldsymbol{p}$ asal sayıları sırayla **3** ve **11** olsun.

Ali'nin gizli seçtiği sayı **3**,

Veli'nin gizli seçtiği sayı **4** olsun.

Ali $\quad 3^3 = 27$ **(u)**

Veli $\quad 3^4 = 81$ **(v)**

değerlerini hesaplayıp çıkan sayıların **mod 11**'deki değerlerini alırlar ve birbirlerine gönderirler. Ellerine geçen bu yeni değerlerin de tekrar kendi anahtarlarıyla kuvvetlerini alırlar ve çıkan sonucu mod 11'te hesaplarlar.

$$\mathbf{u = g^a \ (mod\ p)} \text{ formülünden,} \qquad \text{(Eş. 2.1)}$$
$$\mathbf{3^3 = 27\ mod\ 11 = 5}$$

sayısını hesaplar ve Veli'ye gönderir.

$$\mathbf{v = g^b \ (mod\ p)} \text{ formülünden} \qquad \text{(Eş. 2.2)}$$

$$\mathbf{3^4 = 81\ mod\ 11 = 4}$$

sayısını hesaplar ve Ali'ye gönderir.
Ali gizli sayısını Veli'ye, Veli de gizli sayısını Ali'ye gönderirse;

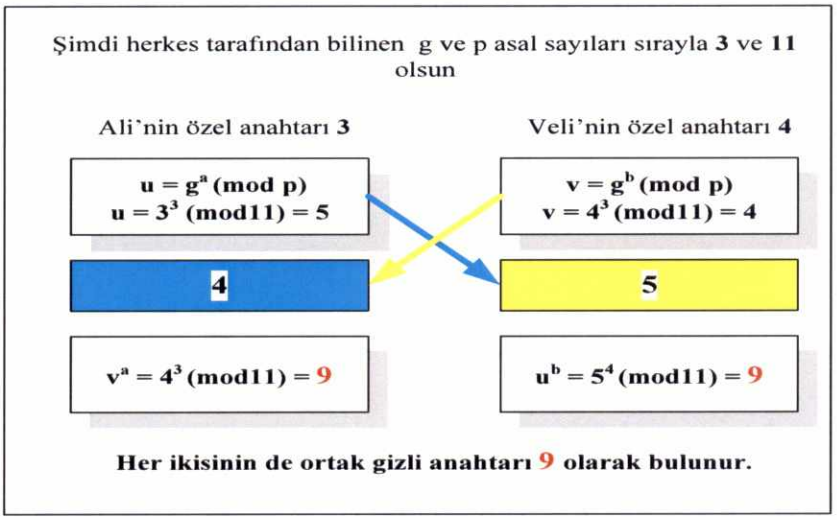
$$\mathbf{v^a : 4^3 = 64\ (mod\ 11) = 9} \qquad \text{(Eş. 2.6)}$$

$$\mathbf{u^b : 5^4 = 625\ (mod\ 11) = 9} \qquad \text{(Eş. 2.6)}$$

9 sayısı her ikisinin de ortak anahtarı olarak bulunur.

Yani iki şahsında sonuç olarak ellerinde **mod 11**'de **9** sayısı elde edilmektedir. Bu güvenli olmayan bir kanalda ortak anahtar paylaşımı olur.

Şekil 2.3. Anahtar Paylaşımına Örnek



Kaynak: Çinem vd.,2007

2.2. Açık Anahtar Kripto Sistemleri

Modern kripto sisteminde bir çok algoritma çeşitleri bulunmaktadır. Bunlardan en çok kullanılan ve yaygın olan iki tanesi RSA (Ron Rivest, Adi Shamir, Leonard Adleman) algoritması ve ElGamal kripto sistemleridir. RSA, pek çok uygulamada kullanılan bir algoritmadır. Mesajları güvenli olarak göndermek için kullanılabileceği gibi en önemlisi elektronik imzalarda da kullanılabilmektedir.

2.2.1. RSA Kripto Sistemi -Rivest-Shamir-Adleman

RSA bu anlamda ilk ve en ünlü açık anahtar kripto sistemlerinden biridir. RSA kripto sistem algoritması 1977 yılında R.Rivest, A.Shamir ve L.Adleman tarafından bulunmuş ve daha sonra modern kripto sistem algoritmalarına (genel açık anahtar kripto sistemi) uygun biçimde geliştirilmiştir. Bu algoritma, modern kripto sistem algoritmalarında ve elektronik imza işlemlerinde güvenli bir şekilde kullanılmaktadır. İlk bakışta son derece basit matematiksel ilişkilere dayanan bu yöntemde iki ayrı anahtar bulunmaktadır. Anahtar paylaşım mantığı çerçevesinde, anahtarlardan biri herkes tarafından bilinen, diğeri de gizli (özel) olan anahtardır.

Herkes açık anahtarını yayınlar ve kendisine güvenli haberleşme için kripto sistemli bir mesaj göndermek isteyen birisi bu anahtarı kullanarak gönderir. Gönderilen bu mesajı gizli anahtarı elinde bulunduran şahıs çözebilir. Gizli anahtar da sadece sahibinde bulunur. Böylece, herkes çözüm için gerekli anahtarı bilmeden, güçlü bir kripto sistemi ile mesajlarını gizleyebilir.

Bu kripto sistemi ile yaşamlarında hiç bir araya gelmemiş, hiç karşılaşmamış ve birbirini tanımayan kişiler bile birbirlerine mesajlar gönderebilir. Örneğin İnternet sitesinden alışveriş yapan bir A şahsı, tanımadığı bu internet sitesine girmesiyle, sitenin genel kullanıma açık anahtarını alır, kart numarasını bu açık anahtar ile kriptolayarak gönderir. Kripto sistemini, bilgiyi gönderen dahil hiç kimse çözemez. Yalnızca internet sitesinde bulunan gizli (özel) anahtarla gelen kart numarasını şahsı sanal alemde girdiği internet sitesi çözebilir. Böylece şahsın özeli olan kart numarasının üçüncü şahıslar tarafından bilinemeyeceğinden emin olur.

RSA kripto sisteminin güvenliği asal çarpanlara ayırma problemine dayanır. Bu problem modern bilgisayar teknolojisine rağmen bilinen algoritmalarla makul bir zamanda çözümü zor olan problemlerdir.

Konu ile ilgili olarak anahtar alış-verişine gerek duymaksızın A şahsının B şahsına açık yazısını göndermek istediğini düşünelim. Bunun için B şahsı sırasıyla aşağıdaki işlemleri yapar.

1. Alıcı birbirinden farklı iki tane farklı $\boldsymbol{p}$ *ve* $\boldsymbol{q}$ gizli iki asal sayı seçer ve bu iki sayının çarpımlarına $\boldsymbol{N}$ sayısı,

$$\mathbf{N} := \mathbf{p} \,.\, \mathbf{q} \tag{2.7}$$

N sayısını ilan eder.

2. Daha sonra $(\mathbf{p}-\mathbf{1})\,(\mathbf{q}-\mathbf{1})$ çarpımını hesaplar. Bu sayı RSA'da

$$\varphi(N) = (p-1)(q-1) \qquad \text{olarak gösterilir.} \qquad (2.8)$$

Buradaki φ(N) Euler fi fonksiyonudur.

3. $1 < e < \varphi(N)$ olacak şekilde **ebob** (e, $\varphi(N)$) = **1** olacak şekilde e sayısı seçer.

4. ***N*** ve ***e*** sayılarının herkes tarafından bilinmesine müsaade eder. Buradaki gizli anahtar d şu şekilde bulunur.

ebob (e, φ(N)) = 1 olduğundan,

5. **d.e ≡ 1 (mod φ (N))** şartını sağlayan bir tek d tamsayısı vardır.

φ (N)) , p ve q asalları sadece alıcı tarafından bilindiğinden (2.10)'nolu işlemi çözerek denklemi bulur.

1. Gönderen kişi halka açık olduğu için (N, e)'ye ulaşabilir. Kapama fonksiyonu

$$E_k(x) := x^e \ (\mathbf{mod}\ N) \qquad (2.9)$$

kullanarak çıkan sonucu alıcıya gönderir.

2. **d** sayısı sadece alıcı tarafından bilindiğinden kapalı mesajı alan alıcının elinde, N,e sayıları ile gizli p ve q asalları ve ayrıca daha önceden hesaplanan $\varphi(N)$ sayısı vardır. Alıcı ilk olarak;

$$d.e \equiv 1 \ (\mathbf{mod}\ \varphi(N)) \qquad (2.10)$$

şartını sağlayan ***d*** sayısı belirler.

3. Daha sonra $\mathbf{y = E(x)}$ kapalı yazısını alan alıcı, açma fonksiyonu kullanarak

$$D(\mathbf{y}) := \mathbf{y}^{\mathbf{d}} \ (\mathbf{mod\ N}) \qquad (\mathbf{x}, \mathbf{y} \in \mathbf{Z_N}) \tag{2.11}$$

ifadesinden **E** açık yazısı elde etmiş olur.

(Not: Burada y, e *ve* N bilinirken x 'in bulunmasının **"diskrete logaritma problemi"** olduğuna dikkat edelim.)

Örnek

Örnekte konunun anlaşılması bakımından aşağıda verilen değerler küçük seçilmiştir.

Kabul edelim ki Bora $p = 17$ *ve* $q = 7$ asallarını seçmiş olsun.

$$\mathbf{N = p.q = 17.7 = 119}$$

$$\boldsymbol{\varphi}\mathbf{(N) = (p - 1).(q - 1) = 16.6 = 96\ olur.}$$

Kabul edelim ki Bora sayısını da e = 7 olarak seçsin. Bölme algoritmasını kullanarak (bkz. Ek-4):

$$\mathbf{d.e \equiv 1\ (mod\ \varphi\ (N))} \tag{Eş.2.9}$$

$$\mathbf{d.7^{-1} \equiv 1\ (mod\ 96)}$$

d'nin bulunması Euclid algortimasınnın (bkz. Ek-2) ters işlemine dayanır, şöyleki;

$$d = \frac{1 + k.\varphi\ (N)}{e}$$

Yukarıdaki eşitlikten k'ya değerler verilerek tam bölüm sağlanır.

k = 0 için; $d = \frac{1+0.96}{7} = \frac{1}{7}$ olmaz,

k = 1 için; $d = \frac{1+1.96}{7} = \frac{97}{7}$ olmaz,

k = 2 için; $d = \frac{1+2.96}{7} = \frac{193}{7}$ olmaz,

k = 3 için; $d = \frac{1+3.96}{7} = \frac{1}{5}$ olmaz,

k = 4 için; $d = \frac{1+4.96}{7} = 55$ olur.

Yani, Bora'nın açma anahtarı yukarıdaki formülden; d = 55 olarak bulunur.

Bora, N = 119 ve e = 7 bulduğu bu sayıları ilan eder.

Ali'de örneğin Türk alfabesinden **B T K** mesajını dörtlü gruplar halinde Tablo *2.1*'den faydalanarak kodlayarak Bora'ya göndermek istersin.

Tablo 2.1. Türk Alfabesi

A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	
15	16	17	18	19	20	21	22	23	24	25	26	27	28	

Kaynak:EKİN,A. Bülent,2010

B T K mesajı Tablo 3.1. den faydalandığında;

B : 1, T : 23 , K : 13 değerlerini aldığı gözükür.
Ali, Tablo 3.1'i kullanarak BTK'nın bu değerleri olan; 1, 23 ve 13 olarak göndermek istesin.

Ali'nin kapama fonksiyonunda yerine yazıldığında;

$$\mathbf{E_k(x) := x^e \ (mod\ N)} \qquad \text{(Eş.2.8)}$$

$$\mathbf{1^7 \ (mod\ 119) = 1}$$
$$\mathbf{23^7 \ (mod\ 119) = 65}$$
$$\mathbf{13^7 \ (mod\ 119) = 55}$$

y = 1, 65 ve 55 kapalı yazısını kanal üzerinden Bora'ya gönderir.

Bora y kapalı yazısını alınca açık yazıyı elde etmek için kendi açma anahtarı olan d'yi kullanır. Yani E_k kapalı yazısını alan alıcı, açma fonksiyonu kullanarak,

$$\mathbf{D_k(y) := y^d \ (mod\ N)} \qquad \mathbf{(x, y \in Z_N)} \qquad \text{(Eş.2.10)}$$

ifadesinden E_k açık yazısı elde edilir.

$$\mathbf{1^{55} \ (mod\ 119) = 01}$$
$$\mathbf{65^{55} \ (mod\ 119) = 23}$$
$$\mathbf{55^{55} \ (mod\ 119) = 13}$$

bulunur. Bulunan bu değerler Tablo 3.1'de yerine yazılırsa Ali'nin gönderdiği **B T K** kriptosu çözülmüş olur.

2.2.2. RSA'da imza

RSA (Ron Rivest, Adi Shamir, Leonard Adleman) pek çok uygulamada kullanılan bir algoritmadır. Mesajları kapatmak için kullandığımız gibi elektronik imzalar için de kullanılmaktadır.

RSA kripto sisteminde olduğu gibi; A ve B şahısları,

(N_A , e_A) ve (N_B, e_B) açık anahtarlarını ilan ederken **d_A ve d_B** açma anahtarlarını gizlerler.

$$E_B(D_A(x)) = y \longrightarrow E_A(D_B(y)) = x \quad N_A < N_B \text{ ise,}$$

$$D_A(E_B(x)) = y \longrightarrow D_B(E_A(y)) = x \quad N_A > N_B \text{ ise,}$$

$$D_A(x) = x^{da} \pmod{N_A}$$

$$E_B(\ ) = (x^{da})^{eB} \bmod N_B$$

$$E_A(D_B(E_B(D_A(x)))) = E_A(D_A(x)) = x$$

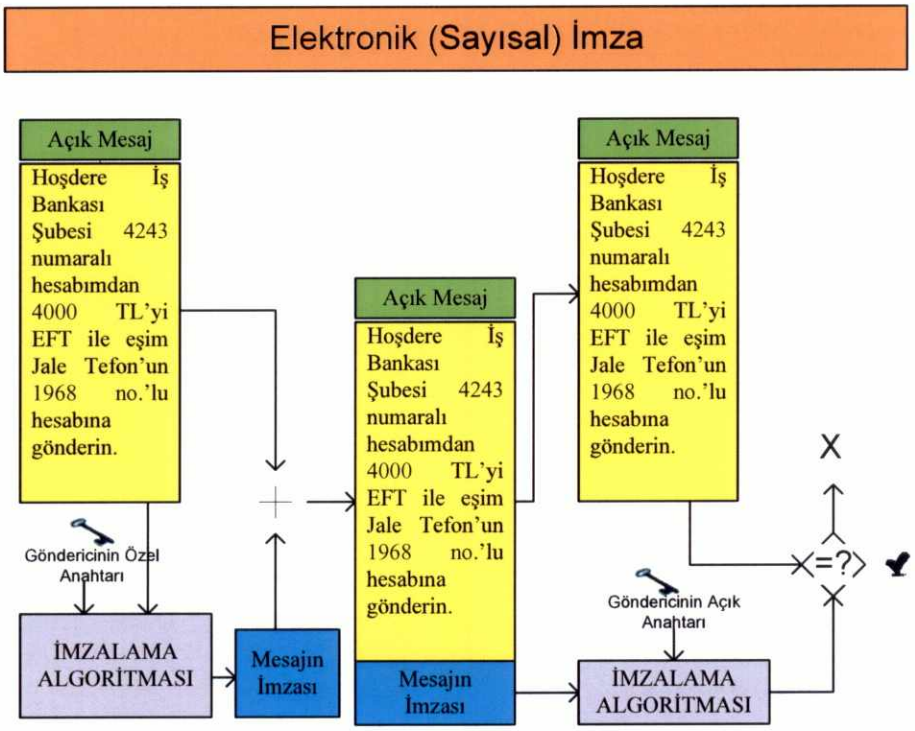
Eğer, $N_A > N_B$ ise A şahsı B şahsına,

$$D_{dA}(E_{eB}(x))$$

ifadesini gönderir ve benzer işlem yapılır.

Şekil 2.4.'de elektronik imzalı mesajın gönderilmesi ve alınması anlatılmıştır.

Şekil 2.4. Elektronik imzalı mesaj gönderilmesi ve alınması



Kaynak: TÜBİTAK-Bilgem

Gönderilecek mesajdan matematiksel yollarla üretilen sabit uzunlukta sayısal bilgisi olan mesaj özeti, her mesajın farklı bir özeti olması ve dolayısıyla mesajda yapılacak en ufak bir değişikliğin imzayı geçersiz kılması sağlanmış olur.

Elektronik imza da son adım, mesaj özetinin gönderen tarafın özel anahtarıyla güvenli olarak gönderilmesidir. Elektronik imza mesaja eklenir ve mesaj ile birlikte alıcıya gönderilir.

Kağıt ortamında kullandığımız elle atılan imzalarla aynı şartları taşıyan elektronik imzalar günümüzde çoğu alanlarda kullanılmaktadır. Elektronik imzalar, Dijital Sertifikalar kullanılarak yaratılır ve doğrulanırlar. Ekonomi, finans, sanal alışveriş, veri gönderme vb. işlemleri gerçekleştirmede kişiye ait özel Sayısal Sertifikaya ihtiyaç vardır.

Hayatımızın her alanına giren teknolojik işlemlerde, örneğin kamu kurum ve kuruluşlarında, banka işlemlerinde, sınav işlemlerinde vb. diğer işlerde elektronik imza kullanılmaktadır (Şahin M., 2007, s.25)

Devlet işlerinde, ekonomide, finans alanında, ticaret alanında vb. diğer işlemler artık elektronik ortamda yapılmaktadır. Yapılan bu işlemlerdeki en temel sorun; bilginin bütünlüğü, inkâr edilmemesi ve geçerliliğinin sağlanmasıdır. Elektronik imza kullanımındaki bu yasal boşluğu gidermek için hazırlanan 5070 sayılı Elektronik İmza Kanunu, 23 Temmuz 2004 tarihinde yürürlüğe girmiştir.

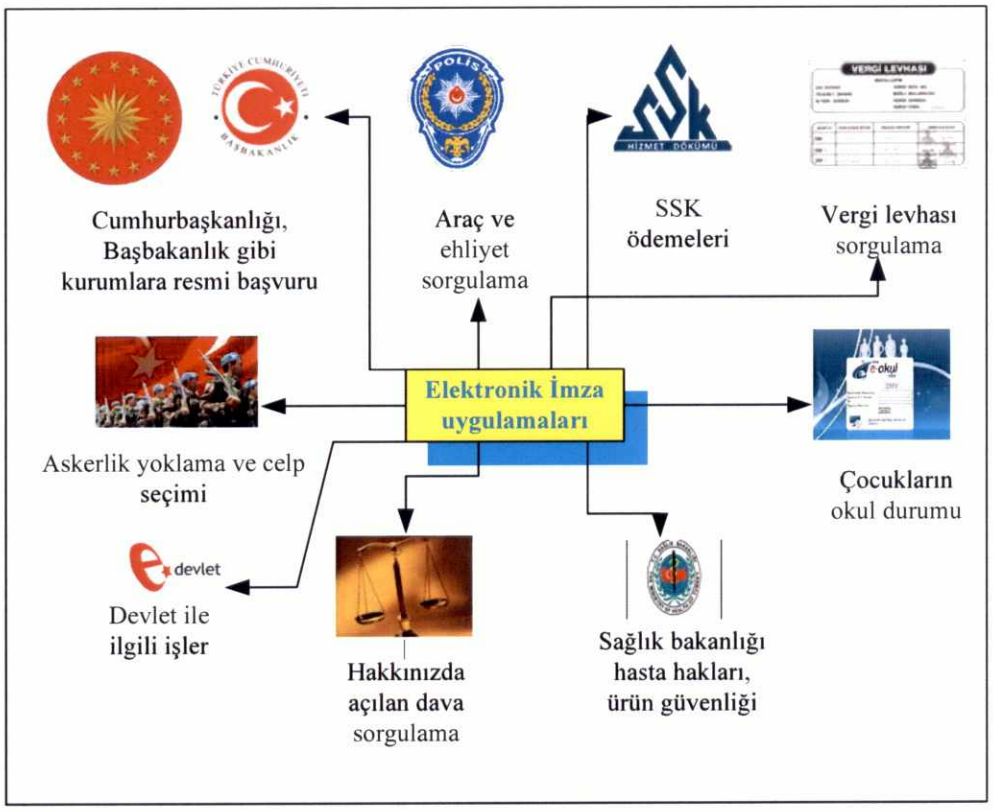
Güvenli elektronik imza Kanunda,

- Elle atılan ıslak imza ile aynı hukukî sonucu doğurması,
- Elle atılan ıslak imza ile aynı ispat gücünü haiz olması,
- Usulüne göre güvenli elektronik imza ile oluşturulan elektronik verilerin senet hükmünde olması,
- Bu verilerin aksi ispat edilinceye kadar kesin delil sayılması,

olarak tanımlanmaktadır. Kanun ile bu konudaki boşluklara meydan vermeyecek şekilde hukuki açıdan getirilmiş önemli yeniliklerdir.

İlgili mevzuatın verdiği yetkiler kapsamında elektronik imza hukuki işlemlerde kullanılabilir. Bugün, çok fazla yaygınlaşmış olmamsına rağmen elektronik imza birçok alanda kullanılmaktadır (Şekil 2.5. Elektronik İmza Uygulamaları).

Şekil 2.5. Elektronik İmza Uygulamaları



Kaynak: https://www.google.com.tr/ elektronik+imza

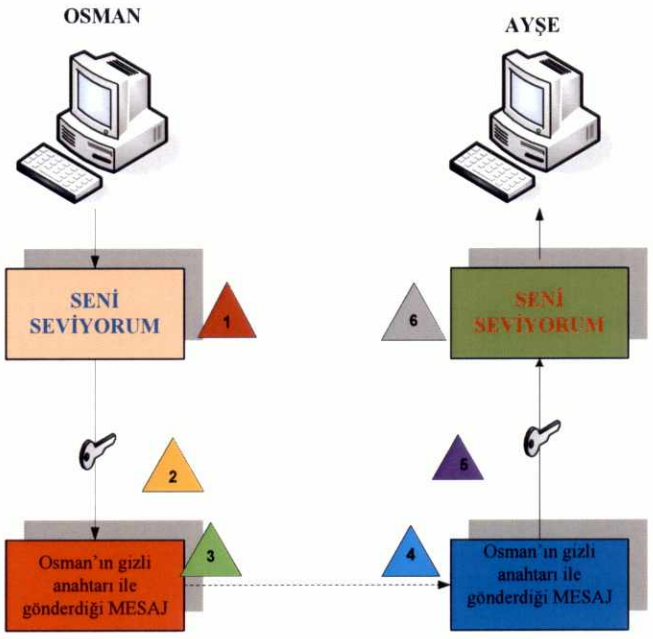
Gündelik yaşamımızda yazdığımız dilekçelerde, trafik, sınav, bankacılık v.b. aklımıza gelebilecek her türlü işlemlerde elektronik imza kullanılmaktadır. Bu imzalar karşılaştırılarak imzanın kime ait olduğu anlaşılabilir. Elektronik imza mesaja bağlı ve sadece gönderici tarafından hesaplanabilen bir niceliktir.

Örnek

Sistemimizde Osman, Kemal ve Ayşe adında 3 kullanıcının var olduğunu düşünelim. Osman, Ayşe'ye "seni seviyorum" mesajını güvenli bir kanal üzerinden göndermek istesin. Kemal, Ayşe'nin eski sevgilisi. Osman seni seviyorum mesajını güvenli olarak Ayşe'ye göndermek zorunda ki, Ayşe hem mesajın yolda herhangi bir değişikliğe uğramadan Osman'dan geldiğinden emin olmalıdır. Bu durumda Osman,

Ayşe'ye seni seviyorum mesajını içeren paketi aşağıda Şekil 2.6'de gösterilen aşamalardan geçerek gönderebilecektir.

Şekil 2.6. Dijital imza da haberleşme örneği



Kaynak: ŞEN Evren, 2008

1. Osman Ayşe'ye göndermek istediği "Seni Seviyorum" mesajını hazırlar.

2. Osman sadece kendisine ait olan ve kimsenin bilmediği "gizli anahtar" ile mesajı gönderir.

3. İletilecek mesaj gizli metin olarak gönderilmeye hazırdır. Mesajı açmak ve bilgiyi okumak isteyen kişi, mesajın sadece Osman'ın açık anahtarıyla açabilecektir.

4. Kapalı mesaj Ayşe'ye ulaşır .

5. Ayşe mesajı okumak için Osman'ın açık anahtarını kullanır.

6. Ayşe kapalı mesaj paketini Osman'ın açık anahtarıyla açar ve okur. Kapalı mesaj sadece Osman'ın açık anahtarıyla açılabildiği ve bu açık anahtarın sadece gizli anahtarla kapalı mesajda kullanılmasından dolayı, Ayşe mesajın Osman tarafından gönderildiğinden emin olur.

Gerçek hayatta yukarıdaki transfere "Hash" (karmaşıklık) adı verilen bir aşama daha vardır. Bu aşamanın hash fonksiyonunun sisteme dahil edilmesi ile mesajın iletimi esnasında içeriğinin (Integrity) değişmediğinden emin olunmaktadır (Şen E., 2008). Konu detaylı olarak bir sonraki bölümde anlatılmıştır.

2.3. Elgamal Kripto Sistemi

Açık anahtarlı kripto sistemler de bir başka güçlü kripto sistemi ise 1985'de Taher ElGamal tarafından tasarlanan ElGamal kripto sistemidir. ElGamal kripto sistemi DLP problem üzerine dayandırılmış bir açık anahtar kripto sistemidir. Bu sistemin matematiksel olarak ifade biçimi ise;

Zp deki DLP (Diskret Logaritma Problemi) zor olacak şekilde bir **p** asalı seçilir.

α, $(\mathbf{Z}_p^*, *)$ devirli çarpımsal grubun primitif elemanı olsun.

Z_p^* kümesi mod p 'ye göre çarpma işlemine bir devirli grup oluşturur. Bu grubun üretecine ise α denir.

(α, sayısı mod p'ye göre bir primitif köktür)

$$P:= \mathbf{Z}_p^*, C:= \mathbf{Z}_p^* \times \mathbf{Z}_p^*, K:= \{(p, \alpha, a, \beta) : \beta = \alpha^a \ (\mathrm{mod} p)\} \qquad (2.16)$$

öyle ki **p**, α ve β herkes tarafından bilinirken **a** gizli tutuluyor.

$\mathbf{k} = (\mathbf{p}, \alpha, \mathbf{a}, \beta)$ ve rastgele seçilen $\mathbf{1} < \mathbf{k} < \mathbf{p} - \mathbf{1}$ sayısı için kapama fonksiyonu (k gizli),

$$\mathbf{y_1} := \mathbf{a^k} \ (\mathbf{mod p}) \text{ ve } \mathbf{y_2} := \mathbf{x}\,\beta^{\mathbf{k}} \ (\mathbf{mod\ p}) \text{ olmak üzere,} \qquad (2.17)$$

$$\mathbf{E_K}\,(\mathbf{x}, \mathbf{k}) : = (\mathbf{y_1}, \mathbf{y_2}) \text{ 'dir.} \qquad (2.18)$$

$y_1, y_2 \in \mathbf{Z_p^*}$ için açma fonksiyonu,

$$\mathbf{D_K}\,(\mathbf{y_1}, \mathbf{y_2}) := \mathbf{y_2}\,(\mathbf{y_1^a})^{-1} \ (\mathbf{mod\ p})\text{'dir.} \qquad (2.19)$$

B şahsının bir α sayısı seçip, gizli tuttuğunu düşünelim.
A şahsı, B şahsına bir $\mathbf{x}$ açık yazısını göndermek istesin,

A şahsı, rastgele bir k sayısı seçer ve $\mathbf{E_K}\,(\mathbf{e}, \mathbf{k}) = (\mathbf{y_1}, \mathbf{y_2})$ ifadesini hesaplayıp, B şahsına gönderir. Kapalı yazı $\mathbf{x}$ açık yazısına ve rastgele seçilen $\mathbf{k}$ sayısına bağlı olduğundan, aynı açık yazı $\mathbf{k}$ sayısına bağlı olarak bir çok sayıda kapalı yazı olarak kapatılabilir.

B şahsı kendine gelen kapalı yazıyı açmak için açma fonksiyonu şu şekilde kullanır;

$$\mathbf{D_K}\,(\mathbf{y_1}, \mathbf{y_2}) := \mathbf{y_2}\,(\mathbf{y_1^a})^{-1} \ (\mathbf{mod\ p})\mathbf{'dir.} \qquad (\text{Eş.2.19})$$

$$= \mathbf{x}\,\beta^{\mathbf{k}}((\alpha^{\mathbf{k}})^{\mathbf{a}})^{-1} \ (\mathbf{mod\ p}) \qquad (\text{Eş.2.17})$$

ile birleştirilirse

$$= \mathbf{x}\,\alpha^{\mathbf{ak}}\,\alpha^{-\mathbf{ak}} \ (\mathbf{mod\ p}) \qquad (\text{Eş.2.19})$$

$$= \mathbf{x} \ (\mathbf{mod\ p}) \qquad (\text{Eş.2.19})$$

x açık yazısını elde eder.

B şahsı, **a** sayısını gizli tuttuğundan **x** açık yazısını sadece kendisi hesaplayabilir.

$\beta \equiv \alpha^a \pmod p$ kongürüansından **a** sayısını hesaplamak bir DLP logaritma problemine dayanır.

a sayısını hesaplamadan $y_1^a \equiv \alpha^{ka} \pmod p$ hesaplanabilirse ElGamal kripto sistemi kırılabilir.

Fakat $\alpha^k \pmod p$ ve $\alpha^a \pmod p$ bilinirken $\alpha^{ka} \pmod p$ ifadesini makul bir zamanda hesaplayan bir yöntem bilinmemektedir.

Konunu daha iyi anlaşılması için bir örnek ile görelim.

Örnek

$$p = 2597,\ \alpha = 2 \text{ olsun.}$$

B şahsı, $a = 765$ sayısını seçmiş ise

$$\beta \equiv 2^{765} \pmod{2597} \qquad \text{(Eş.2.16)}$$

$$= 949 \text{ 'dir.}$$

p, α ve β sayıları herkes tarafından bilinirken, a sayısı yalnızca B tarafından bilinir.

A şahsı, $x = 1299$ açık yazısını B şahsına göndermek için,

(1) Rastgele bir k sayısı seçer. $k = 853$ sayısını seçmiş olsun.

(2) Kapama fonksiyonu kullanarak,

$$y_1 \equiv 2^{853} \pmod{2597} \qquad \text{(Eş.2.17)}$$

$$= 435$$

$$y_2 \equiv 1299 \cdot 949^{853} \pmod{2597}$$

$$= 2396$$

$y = (y_1, y_2) = (435, 2396)$ kapalı yazısını hesaplar ve B şahsına gönderir.

B şahsı, kendisine gelen y kapalı yazısına açma fonksiyonu uygular,

$$x \equiv 2396 \cdot (435^{765})^{-1} \pmod{2597} \qquad \text{(Eş.2.19)}$$

$$= 1299$$

açık yazısını elde eder.

Buraya kadar gördüğümüz örneklerde mesajı alan kişi mesajın kimden geldiğini belirleyememektir. Şimdi, bu sorunun üstesinden gelen elektronik imzayı inceleyelim.

2.4. Kriptografik Hash Fonksiyonu

$|X| > |Y|$ sonlu kümeler olmak üzere

$$h: X \rightarrow Y$$

anlamı; büyük kümeden küçük kümeye giden her fonksiyon bir hash fonksiyonudur.

Aşağıdaki özellikleri gerçekleyen **h** fonksiyonuna kriptografik hash fonksiyonu denir. Yani, büyük kümelerden küçük kümelere eşleme yapılmasıdır.

1. $\forall x \in X$ için $h(x)$ ifadesini hesaplamak kolay,

2. Verilen bir **y** için **y = h (x)** olacak şekilde **x** bulmak zor, (2.20)

3. $\mathbf{h}(\mathbf{x}_1) = \mathbf{h}(\mathbf{x}_2)$ (üst üste binme)
(3.21)

olacak şekilde farklı $\mathbf{x}_1$ ve $\mathbf{x}_2$ değerlerini bulmak ise zordur.

Açık yazının tümünü imzalamak yerine, açık yazının hash fonksiyonundaki görüntüsü, yani açık yazının bir ***özeti*** imzalanır.

Herkes tarafından bilinen bir **h** hash fonksiyonu alalım. A şahsının B şahsına bir x açık yazısı göndermek istediğini düşünelim.

A şahsı bu işle için aşağıdaki protokolü uygular:

(E_A : bilinen kapama fonksiyonu, D_A : gizli açma fonksiyonu)

A şahsı ilk önce $\mathbf{h}(\mathbf{x}) = \mathbf{m}$'yi hesaplar (2.21)

A şahsı $(\mathbf{E_B}(\mathbf{x});\ \mathbf{E_B}(\mathbf{D_A}(\mathbf{m}))$ ikilisini B şahsına gönderir. (2.22)

B şahsı ise aşağıdaki protokolü uygular:

(E_B : bilinen kapama fonksiyonu D_B : gizli açma fonksiyonu)

B şahsı kendi açma fonksiyonunu kendisine gelen,

$$(\mathbf{E_B}(\mathbf{x});\ \mathbf{E_B}(\mathbf{D_A}(\mathbf{m})) \qquad \text{(Eş.2.21)}$$

ikilisine uygular.

$$\mathbf{D_B((E_B(x);\ E_B(D_A(m))\ =\ (x;\ D_A(m))}\ \text{ikilisini elde eder.} \qquad (2.23)$$

Yani **x** açık yazısını ve $\mathbf{D_A(m)}$ ifadesini bulur.

Sonra B şahsı A şahsının herkes tarafından bilinen kapama anahtarını $\mathbf{E_A(m)}$ ifadesini uygular.

$$\mathbf{E_A(D_A(m))\ =\ m}\ \text{sayısı hesaplanır.} \qquad (2.24)$$

h fonksiyonu herkes tarafından bilindiğinden; B şahsı **h(x)** ifadesini hesaplar. Eğer

$$\mathbf{h(x)\ =\ m'} \qquad (2.25)$$

eşitliğini elde ederse, açık yazının A şahsından geldiği ve değiştirilmediğini doğrulamış olur. Yani,

$$\mathbf{m = m'} \qquad (2.26)$$

ise mesajın bütün olduğuna inanılır.

Şahin (2007, s.31) " Pratikte en çok kullanılan hash fonksiyonlarından bazıları MD5, SHA-1'dir (Stinson 1995)".

Örneğin "***akşam saat 9 da dost kitapevinin önünde***" mesajını göndermek istiyorsunuz. Bu mesajın bilgisayar dilinde karşılığı doğal olarak 0 ve 1'lerden oluşan bir dizi olacaktır. Bu diziye de tamamen hayali olarak örnek vermek gerekirse; 010011100000001010011 olsun. 01001110011111010011 "hash" fonksiyonuna dahil olduktan sonra hash sonucu tamamen farklı 01000010110111111010 olacaktır. Burada hatırlaması ve bilinmesi gereken en önemli nokta ***"hash sürecinin sadece tek yönlü olmasıdır"***.

Yani, hash fonksiyonu sonucu ortaya çıkan bir bilginin, hash fonksiyonu uygulanmadan önceki orijinal bilgiye ulaşmanın yolu yoktur. Bu süreci kimyasal bir

reaksiyon gibi düşünebilirsiniz. Örneğin, atom bombasında kullanılan Uranyum çekirdeğinin zincirleme reaksiyonu sonrasında patlamasından sonra yeniden çekirdek haline dönmesi imkânsız olduğu gibi.

Bu durumda hash sonucu karşıdaki bilgisayara gönderildiği esnada, orijinal mesajın da hash sonucuyla birlikte gönderilmesi gerekmektedir. Alıcı bilgisayar, orijinal mesaja hash fonksiyonunu uygulayıp, kendisine orijinal mesajla gönderilen hash sonucuyla karşılaştırır.

Eğer alıcı bilgisayarın oluşturduğu hash sonucu, mesajla birlikte gönderilen hash sonucuyla aynıysa, alıcı bilgisayar kendisine gelen orijinal mesajın üzerinde değişiklik yapılmadığından emin olur.

Hash sonucunun orijinal mesajla birlikte gönderilme sebebi, orijinal mesaj metninin gönderilme esnasında değişikliğe uğramamasıdır. Bu hash sürecinin sayısal sertifika (elektronik imza) sürecine dahil edilmesinin sebebi de tam olarak budur. Aşağıda verilen örnek ile konu daha iyi anlaşılacaktır.

Örnek

1. A şahsı "**KÖYÜMÜZE GERİ DÖNELİM**" mesajını hash fonksiyonuna sokar ve çıkan hash sonucunu gizli anahtarıyla B şahsına göndermek istesin.

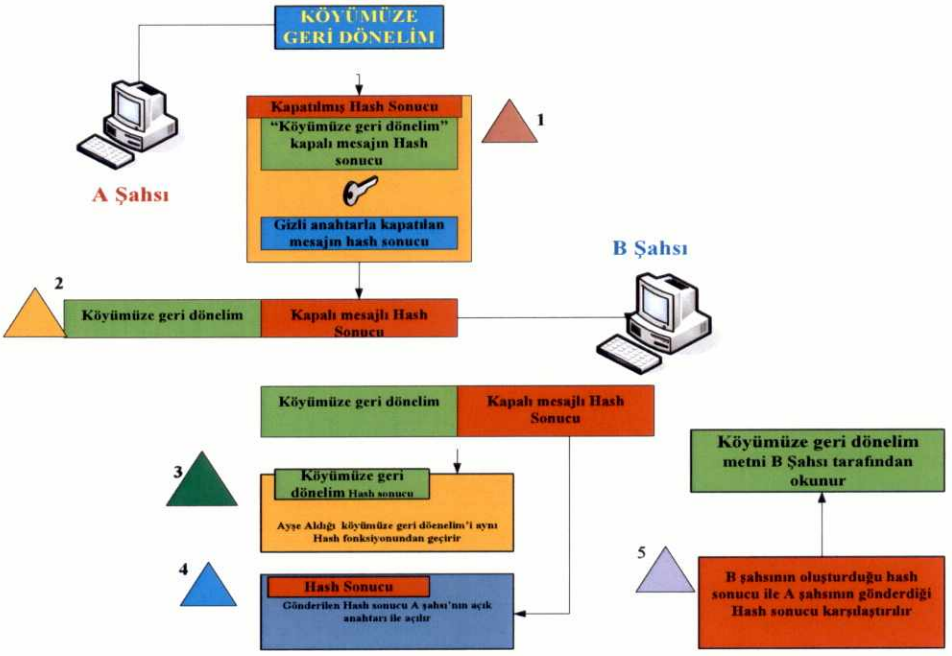
2. A şahsı, B şahsına mesajı göndermeden önce mesajın kendisiyle birlikte mesajın kapalı hash sonucunu da ekler. Daha sonra B şahsına mesajı gönderir.

3. B şahsı birbirine eklenmiş halde gelen paketteki mesajın kendisini yani "**KÖYÜMÜZE GERİ DÖNELİM**" metnini ayırır ve aynı hash fonksiyonundan geçirir.

4. B şahsı aynı zamanda hash sonucunu birbirine ekli olan paketten ayırır ve A şahsının açık anahtarıyla kriptolanmış hash sonucunu açar.

5. B şahsı, 3 üncü ve 4 üncü aşamalardaki hash sonuçlarını birbiriyle karşılaştırır. Sonuçlar aynı çıkarsa, B şahsı gönderilen bu mesajın üzerinde oynama yapılmadığını ve A şahsından geldiğinden emin olarak mesajı güvenle açarak okur. Yukarıda verilen bu aşamaların ayrıntılı anlatımı Şekil 2.7 'deki gibidir.

Şekil 2.7. Hash Fonksiyonu Örneği



Kaynak: ŞEN Evren, 2008

Elektronik sertifika, elektronik kimlik ya da elektronik imzanın resmi olarak işleyişi yukarıda anlatılan sistem gibi gerçekleşmektedir. Mesajın güvenli ve emin bir şekilde değiştirilmeden iletilmesi elektronik imza için birinci derecede önem taşımamaktadır.

Yukarıda verilen örnekte mesajı üçüncü bir C şahsı tarafından elde edilmesi veya okunması halinde, içeriğinin değiştirildiği anlaşıldığı için hash sonuçları farklılık gösterecektir. Mesajın C şahıs tarafından okunmaması için, A ve B şahısları arasında oluşturulacak güvenli iletişim yolu sayesinde sağlanmaktadır. Daha açık olarak;

elektronik imza dışında bütün paket transferleri sadece A ve B şahsı tarafından bilinen güveni bir anahtarla iletilmektedir. (Şen E, 2008).

2.5. Eliptik Eğri Kriptografisi (EEK)

Açık anahtarlı (modern kripto) kripto sistemlerinin algoritmalarının güvenliği zor matematiksel problemlere dayalı olmasının yanında uzun anahtar değerlerine de sahip olmasına bağlıdır. Bu açık anahtarlama (modern kripto) sistem algoritmalarının en büyük dezavantajıdır. Büyük anahtar değerlerinin kullanılması hem süre açısından hem de donanımsal uyuşmazlık açısından düşük performans gösterir.

RSA'da güvenlik büyük basamaklı asal sayılarladır. EEK sisteminde ise güvenlik seviyesine ulaşabilmek için daha küçük asallar kullanılır. Bu da gönderilen bir mesajın kapama ve açma işlemlerinde kolaylık sağlamaktadır.

RSA'da 1024-bitlik anahtar kullanılarak sağlana güvenlik, EEK ile 160-bit anahtar kullanılarak sağlanmaktadır. Bu açık anahtarlı algoritmalar içinde çok önemli bir avantajdır.

Yerlikaya (2002, s.6,) EEK ile ilgili olarak kablosuz ağlardaki kullanımı aşağıdaki ifadesi ile dile getirmektedir.

> "Yeni gelişen teknolojiyle birlikte kablosuz ağların kullanımı geniş anahtar değerlerine sahip kripto algoritmalarının kullanımını zorlaştırmıştır. EEK daha düşük anahtar değerlerini kullanması ve aynı güvenlik seviyesini sağlaması sayesinde kablosuz ağlarda kullanımına çok uygundur"

2.6. Modern (Açık Anahtarlı) ve Simetrik (Gizli Anahtarlı) Kripto Sistemlerinin Karşılaştırması

Gizli anahtarlı kripto sistemi ile açık anahtarlı kripto sistemlerinin güçlü ve zayıf yönlerine baktığımızda karşımıza Tablo 2.2'deki tespitler çıkmaktadır.

Tablo 2.2. Modern (Açık Anahtarlı) ve Simetrik (Gizli Anahtarlı) Kripto Sistemlerin Karşılaştırma Tablosu

SİMETRİK (GİZLİ ANAHTAR) KRİPTO SİSTEMİ	ASİMETRİK (AÇIK ANAHTAR) KRİPTO SİSTEMİ
Kuvvetli Yönleri	
Algoritmalar hızlıdır	Anahtar yönetimi ölçeklenebilir
Algoritmaların donanımla gerçeklenmesi kolaydır	Kripto-analize karşı dirençlidir
"Gizlilik" güvenlik hizmetini yerine getirir	Bütünlük, kimlik doğrulama ve inkâr edememezlik güvenlik hizmetleri sağlanabilir.
Kriptolama anahtar uzundur	Açık anahtar kriptolamaya göre nispeten kısadır
Anahtarın güvenlik açısından sık sık değiştirilmesi gerekir	Özel/genel anahtar çiftinin uzun süreler boyunca değiştirilmesine gerek duyulmaz
Büyük ağlar için yönetilmesi gereken çok sayıda anahtar bulunabilirken	Kriptolamada gereken anahtar çifti daha az olabilmektedir
Zayıf Yönleri	
Ölçeklenebilir değildir	Algoritmalar genel olarak yavaş çalışırlar. Simetrik kriptografi algoritmalarına göre yaklaşık 1500 kat daha yavaştırlar.
Emniyetli anahtar dağıtımı zordur	Anahtar uzunluğu bazı durumlar için kullanışlı değildir. Mobil cihazlar için klasik algoritma anahtar uzunlukları sorunludur

Kaynak: EREN A. Murat, 2005 ve SÖZBİLİCİ Ş.,2005

3. KRİPTOGRAFİNİN ÜLKE UYGULAMALARI

Bilgi ve iletişim teknolojilerindeki hızlı gelişmeler yeni bir çağ yaratmıştır. Bilgi çağı olarak adlandırılan bu çağda ekonomide ve sosyal yaşamda klasik paradigmalar yetersiz kalmakta; teknolojik gelişmeler yeni yapılar, yaklaşımlar yaratmaktadır. Bu nedenle, bilgi güvenliğine ilişkin ulusal bir politika oluşturmanın temel koşullarından birisi, bilgi ve iletişim teknolojilerinde gözlenen gelişmelerin bilinmesidir. Bu noktada, söz konusu teknolojik gelişmelerin ne olduğunu ve ne yönde olacağını doğru anlamak ve içeriğini doğru belirlemek son derece önemlidir:

Güvenli ses/veri haberleşmesinde kullanılan kripto sistemi, internetin yaygınlaşması ve bir ticaret medyası halini almaya başlamasıyla, bilgi güvenliğinin sivil uygulamalarına tanık olmaya başlamıştır.

Gelecekte bilgi sınırsız bir kullanım alanına sahip olacaktır. Bu sınırsız kullanımda güvenliğin alınması gereken önlemlerin tespit edilmesi ve yapılması gerekenlerin düzenlenmesi gerekmektedir. Tarihte sadece askeri ve yönetim haberleşmede önemli olan güvenlik günümüzde her alanda kendini hissettirir olmuştur. Bilgi güvenliğin ve kriptolojik sistemleri kullanmak ülkelerin ulusal güvenliklerinin de bir parçası olmuştur.

Bugün kriptolu haberleşme konusunda ise ülkelerin öngördüğü yasal düzenlemeler farklılıklar göstermektedir. Elektronik haberleşme cihazlarında bilgi güvenliği sağlamada kullanılan kriptografi ile ilgili olarak, diğer ülkelerde kriptografik yazılım ve donanım kullanımı, ithalatı, imalatı ve yasal düzenlemeleri hakkındaki son durum ve gelişmeler aşağıda özet halinde verilmiştir.

3.1. Ülke Değerlendirmeleri

3.1.1. Amerika Birleşik Devletler (ABD)

Birey hakları, mahremiyeti ve özgürlükler ülkesi olan ABD'de devlet, yasal ve yasal olmayan suçlar ve devlete karşı işlenen suçlar arasında gerekli dengeleri kurmuştur. Bu

konuda 1952 yılında, Savunma Bakanı'nın yetki, kontrol ve yönlendirmesinde ve Bakanlık bünyesinde bağımsız bir teşkilat olan "Ulusal Güvenlik Teşkilatı (NSA)[1]" kurulmuştur. NSA, ABD çıkarları doğrultusunda bir yanda uluslararası istihbarat yapmak ve öte yanda Amerikan devletinin bilgi güvenliğini sağlamaktan sorumludur. (Ersoy E, 2003).

NSA, istihbarat işlerini yapan bir yapıdadır. ABD İstihbarat Topluluğu içinde, CIA, FBI, ve Ordu İstihbarat ve Savunma Bakanlığı gibi toplam 13 federal kurumdan birisidir. Kuruluşundan beri değişmeyen kuraldır. Ayrıca, 1972 yılında kurulan "Merkezi Güvenlik Birimi[2], NSA ve ordu istihbarat birimleri arasında tam bir işbirliği sağlanarak Savunma Bakanlığının kriptografik çalışmaları tek bir bünyede toplanmıştır.[3]

NSA'ın görevlerinde; yabancılara oturma izni, gerçek ve tüzel kişiliklerin gizlilik haklarını ihlal etme gibi bir görevi bulunmamaktadır. Bunun dışında, yasanın tanıdığı hak doğrultusunda "***kimlik bilgilerine***" erişme hakkına sahiptirler. Haberleşme özgürlüğü kapsamına giren "***hükümet kayıtlarının***" NSA tarafından tutulması yasayla engellenmiştir.

NSA ulusal bilgi güvenliği ve teknolojik gelişmeler doğrultusunda "ithalat ve ihracat politikalarının" belirlenmesinde görevli değildir. Kripto üretimi, kontrolü ve srtifika verilmesi türünde bir görevi ve iş alanı yoktur. Bu politikalar "Başkanlık" tarafından belirlenir. Özel sektör, ürettiği bir kripto sistemini kamuya satarken bile NSA'ın onayını almak zorunda değildir. Özel sektöre isteğe bağlı olarak danışmanlık hizmeti vermektedir.

"Amerika Standartlar Enstitüsü"[4] tarafından "Federal Bilgi İşleme Standartları[5] " yayınlarıyla ilgi güvenliği standartları belirlenmektedir.

---

[1] Ulusal Güvenlik Teşkilatı -National Security Agency
[2] Central Security Service
[3] Bkz. The National Security Agency, http://www.nsa.gov/about_nsa/faqs_internet.html.
[4] National Institute of Standarts and Technology
[5] Federal Information Processing Standarts

Dünya ülkelerinde yeni bir kavram olarak "yaşamsal altyapıların korunması" [6] gündemdedir. Yaşamsal altyapıların korunması ve düzenlemelere uyulması bakımından Devlet içinde bazı kuruluşlar tespit edilmiştir. Ticaret Bakanlığı iletişim ve enformasyon sektörüne; Hazine Bakanlığı bankacılık ve finans sektörüne, FBI polis, acil durum ve adalet konularına; CIA dış istihbarata; Dışişleri Bakanlığı dışişleri sektörüne; Savunma Bakanlığı savunma sektörüne liderlik edecek kurumlar olarak belirlenmişlerdir (Ersoy E, 2003).

Devlet içinde belirlenen bu kuruluşlar, gereksiz hükümet düzenlemelerinden kaçınmak ve özel ve kamu kuruluşları arasında gerekli işbirliğini sağlamaktadır. Bilim ve Teknoloji Politikalar Genel Müdürlüğü, Ulusal Bilim ve Teknoloji Konseyi'nin programları aracılığıyla araştırma ve geliştirme çalışmalarını için görevlendirilmiştir (Ersoy E, 2003).

ABD'de kriptografik teçhizatı Wassenaar ilkeleri [7] gereğince "***mühimmat***" sınıfına sokulmaktadır. 1998 senesinde düzenlenen Wassenaar ile, kriptografik ürünler; hem askeri hem de ticari ürün vasfına alınmıştır. Bu düzenlemeye imza atan ülkeler, kripto ithalat ve imalatında uyumlu politikalar izleme niyetindedirler.

Ancak bu sözleşmenin bir yaptırımı bulunmamaktadır. ABD, kriptografik yöntemlerin gücüne bir sınırlama getirilmesi tarafındadır. Zira örgütlü bir topluluğun kötü niyetli kullanımıyla böyle büyük bir güce sahip olmasında çok önemli sorunlar yaratabileceğini savunmaktadır. (Ersoy E, 2003).

ABD, 2000'li yılların başına kadar 1998yılındaki Wassenaar düzenlemesinin aksi yönünde, ticari çıkarlarının yani liberalizmin[8] ağır basması ile kriptografik sistemlerin ihracat politikalarında yeni düzenlemeler yapmıştır. İnternet tarayıcılarında 56 bit anahtar uzunluğunda kriptoya izin verirken, ABD 2000'li yılların başından itibaren 128 bit anahtar uzunluğunu ihraç etmeye başlamıştır [9].

---

[6] Critical infrastructure protection
[7] Konvansiyonel Silâhlar ile Çift Kullanımlı Malzeme ve Teknolojilerin ihracat kontrollerini yapmayı amaçlayan bir "Silah Kontrol Rejimi"dir.
[8] Ekonomide kişisel serbestliği ve bireysel davranışların özgürlüğünü savunan görüş.
[9] Bkz. The National Security Agency, http://www.nsa.gov/about_nsa/faqs_internet.html.

Kripto algoritma ve anahtarının muhafaza ve emniyetinde "Güvenilir Üçüncü Kuruluş" (Trusted Third Party) diye adlandırılan bu kuruluşların onay kurumlarından en belirgin farkı gizli anahtar bilgilerini ya ellerinde bulundurmaları, ya da bu bilgilere ulaşacak yöntemlere sahip olmalarıdır.

3.1.2. İngiltere ve Almanya

NSA dışında, Avrupa da bu konularda diğer örnek kurum olarak İngiltere'deki Kamu Haberleşmesi Başkanlığı (GCHQ) [10] ve Almanya'daki Enformasyon Teknolojileri Güvenlik Kurumları (BSI) gösterilebilir[11]. İngiltere'deki Kamu Haberleşmesi Başkanlığı, işlevsel olarak NSA'ya çok yakındır. GCHQ'nun da oluşumu soğuk savaş dönemlerinden kalmadır.[12]

Almanya'daki Enformasyon Teknolojileri Güvenlik Kurumu (BSI), NSA ve GCHQ kurumlarından farklı olarak, istihbarat işlevi yoktur. BSI bir Alman kamu kurumu olarak, bilgi ve bilgisayar sistemleri güvenliği konularında araştırma yürütmektedir. Araştırma sonuçları, kamuda güvenlik uygulamalarının yapılmasına yarar sağlamaktır. Kurum adli olaylarda, istihbarat birimlerince talep gelmesi halinde onlara danışmanlık hizmeti vermektedir.[13]

Alman Parlamentosu 1995 yılında "Telekomünikasyon İzleme Kanunu" adı altında, ülkede üretilen ve kullanılan kablolu telefon, mobil telefon, ISDN [14] ve bilgisayar şebekesi tarayıcılarının, devlet birimleri tarafından gerektiğinde dinlenmesini adına hazırlanan gerekli düzenlemeleri onaylamıştır.

---

[10] Kamu Haberleşmesi Başkanlığı -Government Communications Headquarters (GCHQ)
[11] Enformasyon Teknolojileri Güvenlik Kurumu-Bundesamt für Sicherheit in der Informationstechnik (BSI).
[12] Bkz. Government Communications Headquarters, http://www.gchq.gov.uk/
[13] Bkz. Bundesamt für Sicherheit in der Informationstechnik, http://www.bsi.de/
[14] Tümleşik Hizmetler Sayısal Şebekesi (Integrated Services Digital Network)

Düzenleme ile, dinlemede hakim kararı olmadan yapılmasına izin vermemektedir. ***Almanya, bu düzenleme ile Avrupa ülkeleri arasında bireyi devlete karşı üst düzeyde güvenceye alma öncülüğünü yapmıştır*** (Ersoy E, 2003).

3.1.3. Çin ve İran

Gerçek ve tüzel kişiler ve yabancı şirketler imal ettikleri kripto algortiması ve anahtarını Çin ve İran hükümetine vermek ve rapor etmek zorundadır. Kripto düzenlemelerinde en katı kurallar geçerlidir. [15]

3.1.4. Rusya, Kazakistan, Moğolistan, Pakistan, Singapur, Tunus ve Vietnam

Kriptografi konusunda çok sıkı düzenlemeler uygulayan ülkelerin başında gelmektedir. Kripto yazılımları kullanılmadan önce kayıt altına alınması ve onaylanması zorunludur. Bilgi ve iletişim adı altında Federal Ajans isimli düzenleyici bir kurum bulunmaktadır.[16]

3.1.5. Norveç

İmal ve ithalatında herhangi bir kontrol bulunmamaktadır.[17] Wassenaar anlaşması üyesi olup; ürün ihracatı kontrol altındadır. Kontrol Dışişleri Bakanlığı sorumluluğundadır. Kriptografi düzenlemeleri Elektronik Bilgi Güvenliği Cemiyeti (SEIS) [18] tarafından yapılmaktadır. Bu topluluk da Kamu ve özel sektör örgütleri ortaklaşa çalışmaktadır. Bu cemiyet düzenlemelerde İsveç standardını temel alarak bunu Norveç standardı olarak kabul etmeyi planlamaktadır.[19]

---

[15] Messmer, Ellen. Şifreleme kısıtlamalar: düzenlemeler şifreleme ürünlerin ithalat ve ihracat ile ilgili karar dünya çapında satın etkiler. Network World. pp.69. Haziran 2004 .

[16] Messmer, Ellen. Şifreleme kısıtlamalar: düzenlemeler şifreleme ürünlerin ithalat ve ihracat ile ilgili karar dünya çapında satın etkiler. Network World. pp.69. Haziran 2004

[17] Bkz. EPIC Electronic Privacy Information Center, An International survey of Encryption Policy, 1999, sayfa 80. OECD DSTI/ICCP/ REG(98)4/FINAL, "Inventory of Controls on Cryptography Technologies", 1999, sayfa 28.

[18] SEIS (Elektronik Bilgi Güvenliği Kurumu- Secure Electrnic Information in the Society)

[19] Bkz OECD DSTI/ICCP/ REG(99)13/FINAL, "Inventory of Approaches to Authenticatio and Certification in a global Networked Society", sayfa 62.

3.1.6. Fransa

2000'li yılların başına kadar Fransa'da da kriptografik yazılım ve donanım ABD'de olduğu gibi "mühimmat" olarak tanımlamakta ve işlem görmekteydi. Kanunlar ve düzenlemeler ile kriptografik donanım ve yazılım ihracatı ve kullanımı devlet denetimindedir. Fransa'da faaliyet gösteren yabancı şirketler "ulusal güvenlik" nedeni ile kullandıkları anahtarları Fransız hükümetine bildirmek zorunda kalmışlardır. Bu uygulanan politikadan 2000'li yılların başında vazgeçilmiş kriptografi kullanımına serbestlik getirilmiş ve desteklenmiştir. Kripto yazılım ve donanımın imal veya ithal edilmesinde beyan esastır. Sertifikalandırma yöntemi ile de ihracat ve ithalatı kontrol altında tutulmaktadır.[20]

3.1.7. Japonya

Japonya kripto serbestliğini baştan beri savunmuştur. Kriptografi ithal veya imalatı öncelikle ekonomiyi canlandırması açısından bakmakta, ulusal güvenlik yönünden bir tehdit unsuru olarak algılamamaktadır (Ersoy E, 2003).

3.1.8. Avrupa Birliği

Avrupa Birliği, kripto ihracat ve ithalatında liberal politikalar izlemiştir. Üye ülkelerce, gizliliği tehdit eden her türlü önlemin insan haklarına aykırı olduğunu ve bu durumun serbest ticaretin gelişimini engelleyeceği görüşü hakimdir. 2000'li yılların başında alınan kararlar ve düzenlemeler neticesinde, kriptolojik ürünlerin ihracatında sınırlamalar büyük ölçüde kaldırılmıştır. Kaldırılan bu sınırlamalar ile; üye ülkeler başta olmak üzere, Kanada, Japonya, ABD, Avustralya ve Yeni Zelanda'nın da bulunduğu 10 ülkeden birinde olduğunu beyan etmeleri yeterli olacaktır. Buradaki beyan edilmesindeki amaç, üye ülkeler ve sayılar kriptoloji ithalatı veya imalatında pazar payı en yüksek olan ülkelerdir (Ersoy E., 2003).

---

[20] Bkz. Address by Prime Minister Lionel Jospin at the 20th Summer Forum on Communication, http://www.internet.gouv.fr/english/textesref/hourtin99.htm
France in the Information Society, http://www.internet.gouv.fr/english/textesref/letter.htm
Preparing France's Entry into the Information Society http://www.internet.gouv.fr/anglais/sommaire.htm

3.1.9. Ekonomik Kalkınma ve İşbirliği Örgütü- OECD

OECD,[21] 29 üye ülkesi bulunan Paris merkezli bir örgüttür. Kriptografi sistemleri konusunda sorumlu bakanlık olarak, "Kriptografi Teknolojilerindeki Kontroller" adlı birimce yapılmaktadır. Bu birimin 1999 yılında yayımladığı raporunda; kriptografik ürünlerin ihracat ve ithalatından sorumlu kurumlar arasında ekonomi, sanayi ve ticaret bakanlıklarını işaret etmektedir. OECD üyesi olan Avustralya ve Türkiye'de kriptografik ürünlerin ihracatı ve ithalatından sorumlu bakanlıklar olarak Savunma Bakanlıkları oldukları belirtilmiştir.[22] Ancak, ülkemizde KANUN'nun yürürlüğe girdiği tarih olan 2008 yılından bu tarafa bu sorumluluk BTK tarafından yapılmaktadır.

3.2. Ülkelerin Kripto İmalatı, İthalatı ve Düzenlemeleri

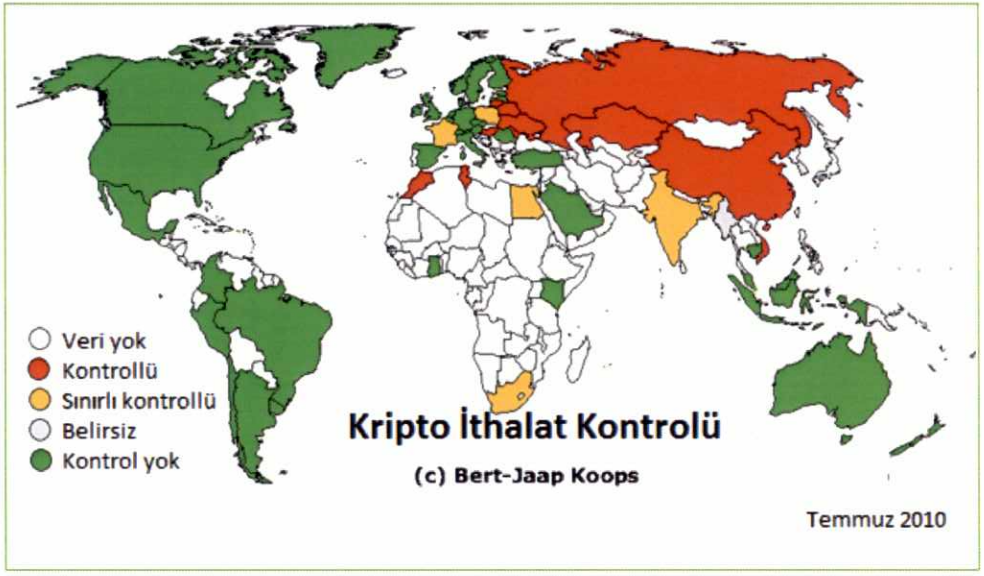
Güvenli haberleşmede kriptografi kullanımı gelecekte iletişim teknolojisinin her alanında kaçınılmaz olacaktır. Ülkeler bu konuda mevcut uygulamalarda yaptıklarının yanı sıra yeni teknolojik gelişmeler karşısında gelecekte ne gibi önlemler ve yaptırım uygulayacakları şimdiden bilinemez. Yukarıda belli başlı bazı ülke uygulamalarından bahsederken diğer ülkeler de kriptografi ihracatı, imalatı ve kanunla verilen düzenlemeler ile ilgili olarak

Şekil 3.1 ve Şekil 3.2'de ayrıntılı olarak verilmeye çalışılmıştır. Bu veriler ışığı altında ülkelerin en genel kripto politikaları da Tablo 3.1'de gösterilmiştir.

---

[21] Ekonomik Kalkınma ve İşbirliği Örgütü (Organization for Economic Co-operating and Development)
[22] Bkz. OECD DSTI/ICCP/ REG(98)4/FINAL, "Inventory of Controls on Cryptography Technologies", 1999, sayfa 28.

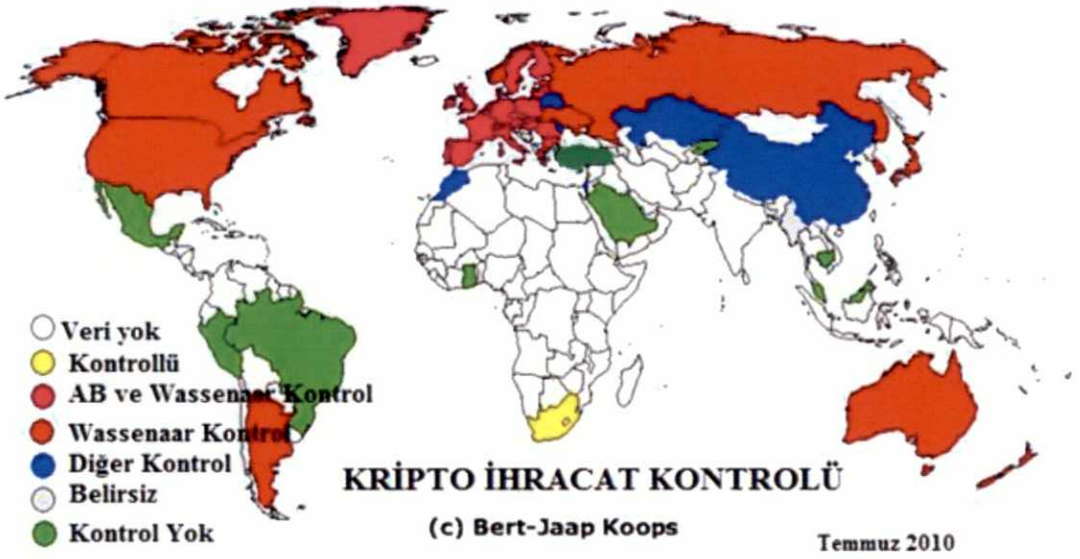
Şekil 3.1. Kripto İthalat Kontrolü



Kaynak: BERT-JAAP Koops, 2010[1]

[1] Yeşil renk: Kripto ithalatın bir sınırlama bulunmadığını,
Kırmızı renk: Kripto ithalatında bir sınırlama bulunmaktadır.

Şekil 3.2. Kripto İhracat Kontrolü



Kaynak: BERT-JAAP Koops, 2010[2]

[2] Yeşil renk: Kripto ihracatında bir sınırlama bulunmadığını,
Kırmızı ve koyu pembe renk: Kripto ihracatında wassenaar kontrollü bir sınırlama bulunduğu (anahtar uzunluğu gibi),

Tablo 3.1. Dünya ülkelerindeki kriptoloji ithalat/imalat rejimi ve düzenlemeleri

SIRA NO.	ÜLKE	İTHALAT/İHRACAT	ÜLKE KANUNLARI
1.	**ABD**	Wassenaar Anlaşmasına bağlı	Mevcut
2.	**ALMANYA**	Wassenaar Anlaşmasına bağlı	Serbest
3.	**ARJANTİN**	Kontrol yok	Mevcut değil
4.	**AVUSTRALYA**	Kontrol var	Mevcut
5.	**AVUSTURYA**	Wassenaar Anlaşmasına bağlı	Serbest
6.	**BANGALDEŞ**		Serbest
7.	**BELERUS**	Kontrol var	Lisansa Tabi
8.	**BELÇİKA**	Wassenaar Anlaşmasına bağlı	Lisansa Tabi
9.	**BREZİLYA**		Çalışmalar var
10.	**BULGARİSTAN**	Wassenaar Anlaşmasına bağlı	Serbest
11.	**ÇİN**		Lisansa Tabi
12.	**ÇEK CUMHURİYETİ**	Beyan Usulü	Mevcut değil
13.	**DANİMARKA**	Wassenaar Anlaşmasına bağlı	Mevcut değil
14.	**ENDONAZYA**	Kontrol yok	Mevcut değil
15.	**ESTONYA**	Wassenaar Anlaşmasına bağlı	Mevcut değil
16.	**FAS**	Lisansa Tabi	Lisansa Tabi
17.	**FİNLANDİYA**	Kontrol yok	Mevcut değil
18.	**FİLİPİNLER**	Kontrol yok	Mevcut değil
19.	**FRANSA**	Wassenaar Anlaşmasına bağlı	Serbest
20.	**GÜNEY AFRİKA**	Wassenaar Anlaşmasına bağlı	Kişisel ve Tüzel Serbest
21.	**GÜNEY KORE**	Wassenaar Anlaşmasına bağlı	Mevcut değil
22.	**HİNDİSTAN**	Kontrol Altında	Lisans zorunlu
23.	**HOLLANDA**	Wassenaar Anlaşmasına bağlı	Mevcut değil
24.	**HONG KONG**	Wassenaar Anlaşmasına bağlı	Serbest

25.	**İNGİLTERE**	Wassenaar Anlaşmasına bağlı	Mevcut
26.	**IRAK**	Lisansa Tabi	Lisansa Tabi
27.	**İRAN**	Lisansa Tabi	Lisansa Tabi
28.	**İRLANDA**	Kontrol yok	Mevcut değil
29.	**İSPANYA**	Wassenaar Anlaşmasına bağlı	Mevcut
30.	**İSRAİL**	Savunma Bakanlığı kontrolünde	Savunma Bakanlığınca yapılıyor
31.	**İSVEÇ**	Kontrol Yok	Mevcut değil
32.	**İSVİÇRE**	Kontrol Yok	Mevcut değil
33.	**İTALYA**	Wassenaar Anlaşmasına bağlı	Düzenlemeler kayıt altında
34.	**JAPONYA**	Wassenaar Anlaşmasına bağlı	Mevcut değil
35.	**KANADA**	Wassenaar Anlaşmasına bağlı	Serbest
36.	**KENYA**		
37.	**KIRGIZİSTAN**	Kontrol yok	Mevcut değil
38.	**KOLOMBİYA**	Kontrol yok	Mevcut değil
39.	**KOSTARİKA**	Kontrol yok	Mevcut değil
40.	**KUZEY KORE**	Lisansa Tabi	Lisansa Tabi
41.	**KÜBA**	Lisansa Tabi	Lisansa Tabi
42.	**LİBYA**	Lisansa Tabi	Lisansa Tabi
43.	**LÜKSEMBURG**	Wassenaar Anlaşmasına bağlı	Mevcut değil
44.	**MALEZYA**	Kontrol yok	Mevcut değil
45.	**MEKSİKA**	Kontrol yok	Mevcut değil
46.	**MISIR**	İzin gerekli	İzin gerekli
47.	**MOLDOVA**	Güvenlik Bakanlığınca Lisanslı	Güvenlik Bakanlığınca Lisanslı
48.	**NORVEÇ**	Wassenaar Anlaşmasına bağlı	Mevcut değil
49.	**PAKİSTAN**	Telekom Yasaları Mevcut	İzin Telekomdan alınıyor

50.	**PERU**	Kontrol yok	Mevcut değil
51.	**POLANYA**	Wassenaar Anlaşmasına bağlı	Mevcut değil
52.	**PORTEKİZ**	Wassenaar Anlaşmasına bağlı	Mevcut değil
53.	**ROMANYA**	Wassenaar Anlaşmasına bağlı	Mevcut değil
54.	**RUSYA**	Ticaret Bakanlığından Lisansa Tabi	İzne Tabi
55.	**SAUDİ ARABİSTAN**	Kontrol Yok	Yasak
56.	**SİNGAPUR**	Kontrol yok	Mevcut değil
57.	**SUDAN**	Lisansa Tabi	Lisansa Tabi
58.	**SURİYE**	Lisansa Tabi	Lisansa Tabi
60.	**TUNUS**	Kontrol İzinli	Düzenlemeler İzinli
61.	**TÜRKİYE**	İzne Tabi	Mevcut
62.	**UKRAYNA**	Wassenaar Anlaşmasına bağlı	Mevcut
63.	**YENİ ZELLANDA**	Wassenaar Anlaşmasına bağlı	Mevcut değil
64.	**YUNANİSTAN**	Wassenaar Anlaşmasına bağlı	Serbest

Kaynak: BERT-JAAP Koops, 2010

4. MEVCUT DURUM ve TÜRKİYE ANALİZİ

Elektronik haberleşeme cihazları ile kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerin kodlu veya kriptolu haberleşme yapabilmesi, 10.11.2008 tarih ve 5809 sayı ile yürürlüğe giren Elektronik Haberleşme Kanunu'nun 39 uncu maddesinde

> *"Telsiz haberleşme sistemleri üzerinden kriptolu haberleşme yapmaya Türk Silahlı Kuvvetleri, Jandarma Genel Komutanlığı ve Sahil Güvenlik Komutanlığı, Milli İstihbarat Teşkilatı, Emniyet Genel Müdürlüğü ve Dışişleri Bakanlığı yetkilidir. Ayrıca yukarıda belirtilen kurumlara ait olanlar dışında kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerin haberleşme hizmeti içinde kodlu veya kriptolu haberleşme yapma usul ve esasları Kurum tarafından belirlenir"*

hükmü kapsamında izne bağlanmıştır.

Kanun maddesi kapsamında;

> Kod veya kriptolu haberleşme yapma hizmetinden yararlanacak kamu kurum ve kuruluşlar ile gerçek ve tüzel kişiler için bahse konu haberleşme cihazlarının ithal veya imal edilme şartlarının usul ve esaslarının belirlendiği Yönetmelik de 23.10.2010 tarih ve 27738 sayılı Resmi Gazetede yayınlanarak yürürlüğe girmiştir.

Ülkemizde bu konu 2006 yılından başlamak üzere her yıl Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı kapsamında ele anılmaktadır. Bu alanda yapılan çalışmaların tartışıldığı konferans; üniversiteler, özel sektör temsilcileri, kamu kurumları ve ulusal ve uluslararası kuruluşlara yayın sunan bilim adamlarının katılımı ile gerçekleşmektedir. Bilgi güvenliği ve kriptoloji kavramlarının, toplumun her kesimince anlaşılması, bilinçlendirilmesi ve birikimlerinin sunulmasına adı büyük katkılar sağlamaktadır.

4.1. Haberleşmenin Kontrolü

Güvenli veri veya ses haberleşmesinde yasa dışı durumların takip ve denetlenmesi (her türlü telefon dinlemesi, internet kontrolü vb.) ülkemizde mutlaka hâkim kararıyla yapılmak zorundadır. Yasal dinlemelerde saplama olarak bilinen paralel/uç alma yöntemi kullanılmaktadır.

Türkiye'de iletişimin kontrol edilmesi tek bir merkez olan Kurum bünyesinde faaliyet gösteren Telekomünikasyon İletişim Başkanlığınca (TİB) yürütülmektedir. Telekomünikasyon İletişim Başkanlığı;

> 23.07.2005 tarihli Resmi Gazetede yayımlanarak yürürlüğe giren ve 2559, 2803 ve 2937 sayılı Kanunlarda değişiklik yapan 5397 sayılı Kanun ile kurulmuş olup, 23 Temmuz 2006 tarihinden itibaren ilgili mevzuatın öngördüğü iş ve işlemleri tek merkezden yürütmektedir.

Kısaca, ***TİB, dinleme yapacak birim ile dinlenilecek iletişim aracının hizmetini sağlayan kurum (operatör) arasında kontrol birimi olarak yer almaktadır.*** Yasal olarak yapılacak sinyal bilgilerinin dinlenmesinde hakim kararı zorunludur. Hakim tarafından verilen onay doğrultusunda, TİB bünyesinde; Millî İstihbarat Teşkilatı Müsteşarlığı, Emniyet Genel Müdürlüğü ve Jandarma Genel Komutanlığının ilgili birimlerinden birer temsilci tarafından gerekli olan sinyal bilgilerine ulaşılmakta ve kayıt altına alınmaktadır.

TİB aynı zamanda internet ortamında yapılan yayınlarda;

> 04/05/2007 tarihli ve 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" 23/05/2007 tarihinde yürürlüğe girmiş ve 30/11/2007 tarihli 26716 sayılı Resmi Gazetede yayımlanan "İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik" te belirtilen katalog suçlarını içermesi halinde ve yasadışı

durumlarda hakim kararı ile erişimlerini de engellemektedir. Yönetmelikte katalog suçları olarak ve aşağıda sayılan suçları işleyenler hakkında erişimler engellenmektedir. Bunlar;

- İntihara yönlendirme,
- Çocukların cinsel istismarı,
- Uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma,
- Sağlık için tehlikeli madde temini,
- Müstehcenlik,
- Fuhuş,
- Kumar oynanması için yer ve imkân sağlama,
- Atatürk aleyhine işlenen suçlardır.

Görünen odur ki, geleceğin haberleşme sistemleri; kısıtlamalar, yasaklamalar ve oldubittiler ile sınırlamamın mümkün olmadığı teknolojiler çağı olacaktır. İnsanlar artık yaşamın vazgeçilemez bir parçası olan haberleşme cihazları ile güvenli haberleşme yapabilmeleri ve teknolojinin kötü amaçlı kullanımının bir şekilde önüne geçilmesini beklemektedir. Bu beklenti içinde olanların bir kısmı gerekli tedbirlerin alınmasını devletten beklerken bir kısmı da teknoloji dünyasının bu konuda sunduğu yenilikleri araştırarak bireysel bazda çözüm yolu bulmaya çalışmaktadır.

Kişi hak ve özgürlükleri, yaşam hakkından başlamak üzere, konut edinme, seyahat etme, çalışma, dilediği gibi iletişim kurma, düşündüklerini açıklama ve yayma gibi, insan iradesiyle gerçekleştirilebilecek her türlü hareket tarzının güvence altına alınmasını içermektedir. Bu özgürlükler, başta uluslararası sözleşmeler olmak üzere, ülkelerin anayasa ve yasalarıyla çeşitli düzeylerde koruma altına alınmaktadır.

Hukuk bir gün herkes için geçerli olacağı kuralı dahilinde, illegal işler ile mücadelede bile hukuk kuralları içinde kişi hak ve özgürlükleri gözeterek, düzeni ve güvenliği sağlamada hassas dengeler kurarak düzeltilmelidir. Bu kural bütün demokratik toplumların en vazgeçilmez önceliği olarak kabul edilmektedir.

Filhakika Anayasa'nın [1] "***Temel hak ve hürriyetlerin korunması***" başlıklı 40. Maddesi'nde,

> "Anayasa ile tanınmış hak ve hürriyetleri ihlal edilen herkes, yetkili makama geciktirilmeden başvurma imkânının sağlanmasını isteme hakkına sahiptir" hükmü yer almaktadır. Kısaca Devletin, kişi özel hayatını, mahremiyetini ve dokunulmazlığını garanti altına alacak ve bu konuda her türlü ihlale karşı kişisel başvuru yollarını kolaylaştırıcı önlemleri almak zorunluluğu bulunmaktadır.

Yine Anayasa'nın 40. Maddesi'nin son fıkrasında

> "Kişinin, resmi görevliler tarafından vaki haksız işlemler sonucu uğradığı zararda, kanuna göre, Devletçe tazmin edilir. Devletin sorumlu olan ilgili görevliye rücu hakkı saklıdır" ifade edilmektedir. Bu çerçevede, kişisel sırların hukuka aykırı olarak resmi görevliler tarafından dinlenmesi, kayıt altına alınması ya da ifşa edilmesinden dolayı doğacak maddi ve manevi zararların tazminini devletten isteme hakkı bulunmaktadır.

Haberleşme özgürlüğünün gizliliğinin ihlal edilmesi ile ilgili olarak ayrıca Avrupa İnsan Hakları Sözleşmesi'nin "Özel hayatın ve aile hayatının korunması" başlıklı 8 inci Maddesi'nde şu ifadelere yer verilmiştir:

1. Herkes özel ve aile hayatına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahiptir.
2. Bu hakkın kullanılmasına bir kamu otoritesinin müdahalesi, ancak ulusal güvenlik, kamu emniyeti, ülkenin ekonomik refahı, dirlik ve düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için, demokratik bir toplumda,

---

[1] Bir devletin nasıl yönetileceğini belirleyen, kişi hak ve özgürlüklerini düzenleyen yasalar bütününe anayasa denir.

zorunlu olan ölçüde ve yasayla öngörülmüş olmak koşuluyla söz konusu olabilir." denilmektedir

Türkiye Cumhuriyeti Anayasası'nın "***Haberleşme Hürriyeti***" başlıklı 22. Maddesi'nde ise

> "***Herkes, haberleşme hürriyetine sahiptir. Haberleşmenin gizliliği esastır***" hükmü ile, Anayasa'nın 22. Maddesi'ndeki düzenlemenin devamında, bu temel özgürlüğün hangi amaçla ve nasıl kısıtlanacağına yönelik istisnaya yer verilmiştir.

Buna göre;

> "***Milli güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlakın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak usulüne göre verilmiş hakim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; haberleşme engellenemez ve gizliliğine dokunulamaz. Yetkili merciin kararı yirmi dört saat içinde görevli hakimin onayına sunulur. Hakim, kararını kırk sekiz saat içinde açıklar; aksi halde, karar kendiliğinden kalkar. İstisnaların uygulanacağı kamu kurum ve kuruluşları kanunda belirtilir***." hükmü yer almaktadır.

Güvenli haberleşme yapma hakkı demokratik hukuk sistemlerinde kişilerin temel hak ve hürriyetlerden en iyi biçimde ve eksiksiz yararlanmasını temin etmekle de görevlidir. Kolluk güçlerince her bireyin toplumsal bir suçlu olarak görülmesi, ilgili mevzuatlarla verilen hakların baskı unsuru olarak kullanılması ve ilkesiz bir şekilde hak ve hukuka uygun olmayan önlem alması söz konusu değildir.

Kişinin hak ve özgürlüğünü zedeleyerek bilgi alınmasındaki müdahale niteliği taşıyan tekniklerin uygulanması zorunluluğunda da, mutlaka kanuna ve hâkim kararına dayanılmalıdır.

Ülkemizde bu konuda yapılan çalışmalar ve araştırmalar neticesinde TBMM'ne, Ulusal Bilgi Güvenliği Teşkilatı ve Görevleri Hakkında Kanun Tasarısı sunulmuştur. Kanun; ulusal güvenliği ilgilendiren bilgilerin korunması, Devletin bilgi güvenliği faaliyetlerinin geliştirilmesi, gerekli politikaların üretilmesi ve belirlenmesi, kısa ve uzun dönemli planların hazırlanması, kriter ve standartlarının saptanması, ihracat ve ithalat izinlerinin ve sertifikalarının verilmesi, bilgi sistemlerinin teknolojiye uyumunun sağlanması, uygulamanın takip ve denetimi kamu ve özel kurum ve kuruluşların arasında koordinasyonun sağlanması amacıyla bir teşkilatın kurulması ve görevlerine ilişkin esas ve usullerin düzenlenmesi hükümlerini barındırmaktadır (Görür H., 2010).

4.2. Kriptografinin Günlük Yaşamda Kullanım Alanları

Bilgi teknolojilerinin getirdiği büyük yenilikler günlük hayatımızın vazgeçilmezleri olmuşlardır. Özellikle mobil iletişim sistemleri ile kablolu ve kablosuz ağlardaki teknoloji hız kesmeden yoluna devam etmektedir. Küçülen dünyamızda, ülkelerin ekonomik, politik, finansal, eğitim ve öğretim, sağlık ve eğlence hayatları hakkında bilgi edinmek ve bu bilgiler erişmek çok kolaylaşmıştır.

Bu kadar kolay erişilebilir bilgilerin güvenli bir şekilde korunması ve yetkisiz erişimlerin engellenmesi kripto yazılım ve donanımları ile donatılan sistem ve cihazları ile mümkün olmaktadır.

Kriptografinin günlük hayatımızda kullanım alanlarına baktığımızda;

- ATM[2] cihazlarında,
- İnternet bankacılığında,
- Çağrı merkezlerinde (henüz ülkemizde kullanılmıyor),
- Parola oluşumlarında (henüz ülkemizde kullanılmıyor),
- e-Ticarette,
- İnternet alışverişlerinde,
- e-Seçim çalışmalarında (henüz ülkemizde kullanılmıyor),
- İhbarlarda (henüz ülkemizde kullanılmıyor),
- Tanık/Kanıt sistemlerinde (henüz ülkemizde kullanılmıyor),
- e-Para, e-Cüzdan işlemlerinde (henüz ülkemizde kullanılmıyor),
- Hastane kayıtlarında,
- Askeri ve istihbarat alanlarında,
- e- Noterlik: Sayısal Sertifikalarda,
- TV kanallarında,
- GSM Mobil telefonlarda,

kısaca bilginin değerli olduğu her alanda kullanıldığı görülmektedir.

Alışveriş yaparken, istihbaratta kullanımına mutlak ihtiyaç var. Mobil telefon kullanırken, internette dolaşırken, e-postalarımızı okurken, arabalarımızı uzaktan kilitlerken, internetten alış veriş yaparken, uçak bileti alırken hiç farkında olmasak da kullandığımız bir bilim dalıdır. Bu bilim dalı ülkemizde genç nesiller tarafından yeterince iyi tanınmamaktadır.

[2] Bankamatik-Automatic Teller Machine

4.3. Türkiye Analizi

Diğer taraftan, 10.11.2008 tarih ve 5809 sayı ile yürürlüğe giren Haberleşme Kanunu'nun 39 uncu maddesinde

> "***Telsiz haberleşme sistemleri üzerinden kriptolu haberleşme yapmaya Türk Silahlı Kuvvetleri, Jandarma Genel Komutanlığı ve Sahil Güvenlik Komutanlığı, Milli İstihbarat Teşkilatı, Emniyet Genel Müdürlüğü ve Dışişleri Bakanlığı yetkilidir. Ayrıca yukarıda belirtilen kurumlara ait olanlar dışında kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerin haberleşme hizmeti içinde kodlu veya kriptolu haberleşme yapma usul ve esasları Kurum tarafından belirlenir***"

hükmü yer almaktadır. Bu madde kapsamında gerçek ve tüzel kişilerin de yasal olarak haberleşme hizmeti içinde kodlu veya kriptolu haberleşme yapmalarına imkân tanınmaktadır.

Kanun'un 39 uncu maddesi kapsamında haberleşme hizmetinden yararlanacak gerçek ve tüzel kişilerce haberleşme yapma usul ve esaslarında ele alınacak konularla, sabit ve mobil telefon görüşmeleri, e-mailler, internet bağlantıları ve uydu haberleşmesin de bireylerin güvenli haberleşme yapmalarına imkân tanıyan ve Kurum tarafından hazırlanan bu Yönetmelik 23.10.2010 tarih ve 27738 sayılı Resmi Gazetede yayınlanarak yürürlüğe girmiştir.

Haberleşme cihazları üzerinden güvenli haberleşme de kullanılan klasik kripto sistemleri çok gerilerde kalmıştır. Açık anahtarlı kripto sistemlerine ilişkin tezin üçüncü bölümünde verilen matematiksel veriler ve kripto sistemlerinde en son gelinen gelişmeler anlatılmıştır. Hayatımızın her alanına giren güvenli haberleşme de, elinizde bulunacak anahtarın veya algoritmanın çözümünü bile zorlu kılmaktadır.

Anayasa ve Avrupa İnsan Hakları mahkemesince, kişilerin haberleşme hürriyetleri en temel hak olarak görmüştür. Bu en temel hak olan haberleşme hürriyetinde, güvenli haberleşme altyapılarının oluşturulması zaruridir.

Yayımlanan söz konusu Yönetmelik ile, ülkemizde güvenli haberleşmede kripto sistemini kullanacak kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerce, haberleşme cihazlarında kripto yazılımı veya donanımı kullanmasında dünya ve Avrupa birliği ülkelerinde belirtilen serbestlikler yanında aşağıda belirlenen gerekçeler dahilinde usul ve esaslar belirlenmiştir. Yönetmelik usul ve esasları belirlenirken;

- Ülkemizde Gerçek ve tüzel kişilerce gerçekleştirilecek güvenli haberleşme cihazlarında kullanılacak kriptolu haberleşme cihazlarının, ithal veya imal edilmesi aşamasından dünya ülkelerinde örneği olduğu gibi izin ve başvuru aşamalarında, kullanılacak cihaz ve ekipmanlarının **"kullanıcı"** bazında değerlendirilerek buna göre her bireyi kontrol altına almak ve bu cihazlara ait algoritma ve anahtarı muhafaza etmek mümkün değildir.

  Bu konunun takibi ve güvenliliği açısından haberleşme cihazlarının ithal veya imal etme aşamasında, kripto sistemine ait anahtar ve algoritmalarının ithalatçı veya imalatçı firmalarca ilgili mercileri verilmesi sağlanmalıdır. Örneğin, bugün ülkemizde 68 milyon GSM abonesi bulunmaktadır.

  Bu abonelerin % 1'lik bir kesiminin güvenli haberleşme için kriptolu cihaz kullanmasına imkan tanıdığınızda 680.000 bin kişiden kullandığı haberleşme cihazına ait kripto anahtarını ve algoritmalarının denetim birimlerine teslim etmesi halinde, anahtar ve algoritmanın saklanmasının zorluğu,

- Genellikle ev, iş yeri, garaj, fabrika, depo, antrepo ve büyük alışveriş merkezleri gibi kapalı lokal alanlarda ya da mülkiyeti kullanıcıya ait kampüs veya açık alanlarda kullanım amacına göre belirlenen frekans bandlarında ve çıkış gücünde kullanılan, diğer sistemleri enterfere etmeyen ve enterferansa

açık olarak kullanılan ve herhangi bir frekans kısıtlamasında izne tabii olmayan kısa mesafe erişimli alçak güçlü telsiz cihazlarının (oyuncak telsiz, Alçak güçlü Telsiz cihazı PMR, Yol ve demiryolları sistemlerinde kullanılan telemetri cihazları, kablosuz mikrofonlar vb.) gerçek ve tüzel kişilerce kripto sistemi özelliği ile kullanımı ve denetimi serbest olması gerektiği,

- Herhangi bir kamusal alanda telli veya telsiz haberleşme sistemi altyapısı ve herhangi bir dış ünite bağlantısı olmayan, kriptolu haberleşmeyi bireysel kullanım amaçlı lokal alanda çevrim içerisinde kullanılan ve bu tür cihazların kontrol ve denetimlerinin mümkün olamayacağı için kapalı devre haberleşme sistemleri herhangi bir izne tabi bırakılmamalı kapsam dışı olarak değerlendirilmesi,

- Haberleşme cihazlarında kripto kullanımında; teknik ve diğer özelliklerin donanım veya yazılım bazında değiştirilmemesi, bu tür cihazların emniyet ve muhafaza tedbirlerin alınması, cihazları kullanan gerçek ve tüzel kişilerce sağlanması,

- Haberleşme cihaz kullanımında, çağdışı ve teknolojinin ilerlemesi karşısında olan bir zihniyet ile hala yazılım ve donanım bazında; Milli olmasının zorunlu hale gelmesi beklenemez.

Dünya ve Avrupa ülkelerinde bu tür haberleşme cihazı kullanıcısına en katı kuralları olan ülkelerde bile yazılım ve donanımlar serbest bırakıldığı gibi ülkemizde de kripto yazılım veya donanımı kullanıcılarına milli kripto kullanımını zorlamak ve bu konuda alınacak önlemler ve düzenlemeler ile teknolojinin önünde durmak söz konusu değildir.

Milli kripto kullanmak her gerçek ve tüzel kişi ile Kamu Kurum veya kuruluşların belirleyeceği inisiyatifler doğrultusunda, ülke menfaatleri göz önüne alınarak verecekleri bir karar olması,

- Yolcu beraberinde veya pota yolu ile yurtdışından ithal edilecek haberleşme cihazlarında, kişi bazında kripto algoritması ve anahtarını yetkili mercilere verme zorunluluğu getirilmesi,

- Yabancı devletlerin Türkiye'deki diplomatik temsilciliklerine münhasıran kendi hükümet merkezleri ile haberleşme yapmak veya kendi iç güvenlik amaçlarıyla kullanmak üzere mütekabiliyet esaslarına bağlı olarak kodlu veya kriptolu haberleşme sistemi kurma ve işletme izni Dışişleri Bakanlığınca sağlanması,

gerekçeleri gösterilmek sureti ile yayımlanarak yürürlüğe girmiştir.

Kanun ve buna istinaden yayımlanan Yönetmelik çerçevesinde, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilere elektronik haberleşme cihazlarında kod ve kripto kullanım serbestliği getirmesi ile başlayan bu süreçte izin başvurularının başlaması kaçınılmazdır.

Kurumca, yetkilendirme ve hizmet türlerine göre tutulan istatistiki bilgiler ışığı altında işletmeci sayıları bakımından bugün gelinen durum Tablo 4.1.'de gösterilmektedir.

Tablo 4.1. Yetkilendirme ve Hizmet Türlerine Göre İşletmeci Sayıları

Yetkilendirme Türü	Hizmetler	İşletmeci Sayısı
Görev Sözleşmesi	Uydu ve Kablo TV Hizmetleri	1
İmtiyaz Sözleşmesi	GSM Hizmeti	3
	IMT-2000/UMTS Hizmetleri	3
	Çeşitli Telekomünikasyon Hizmetleri	1
Bildirim Kapsamında Hizmet Veren İşletmeciler	Uydu Haberleşme Hizmeti	31
	Uydu Platform Hizmeti	8
	Altyapı İşletmeciliği Hizmeti	89
	İnternet Servis Sağlayıcılığı Hizmeti	198
	Sabit Telefon Hizmeti	44
	Kablolu Yayın Hizmeti	16
	GMPCS Mobil Telefon Hizmeti	5
	Sanal Mobil Şebeke Hizmeti	31
	Hava Taşıtlarında GSM 1800 Mobil Telefon Hizmeti	1
Kullanım Hakkı Kapsamında Hizmet Veren İşletmeciler	GMPCS Mobil Telefon Hizmeti	2
	Ortak Kullanımlı Telsiz Hizmeti	77
	Altyapı İşletmeciliği Hizmeti	5
	Sabit Telefon Hizmeti	175
	Rehberlik Hizmeti	12
	Sanal Şebeke Mobil Hizmeti	10
TOPLAM		**712**

Kaynak: BTK 2013 yılı 1 inci. çeyrek "Üç Aylık Pazar Verileri Raporu (Haziran 2013)[3]

Geniş band internet hizmeti, e- imza ve GSM mobil telefon sistemlerinde abone sayıları her geçen gün artmaktadır. Zira pazar analizlerine kısaca bakıldığında;

[3] http:// http://www.btk.gov.tr/kutuphane_ve_veribankasi/pazar_verileri/ucaylik13_1.pdf

- 2003 yılında sadece 18.604 geniş bant internet abonesi bulunmaktayken, bu rakam bugün 20 milyon,
- Mobil telefon abone sayısı 68 milyon,
- Elektronik imza 750 bin,
- TÜRKSAT'ın Türkiye'de toplam Kablo TV abone sayısı 1.260.769,
- GMPCS Mobil Telefon hizmet grubunda toplam abone sayısı 6390,
- Kablo İnternet hizmeti 500 bin,
- Uydu haberleşme hizmeti 10 bin,
- OKTH hizmeti 1752 olup,

bu hizmetlerde işletmeciler tarafından gelecek ithal ve imal edilecek cihaz ve sistemlerde kod veya kripto donanım ve yazılım izin talepleri için gerekli altyapıların hazırlanması kaçınılmazdır.

SONUÇ VE ÖNERİLER

Kriptografi, güvenli bilgi ve iletişim sistemlerinin önemli bir bileşenidir. Gelişmiş ülkelerde, özellikle vatandaşların gizlilik haklarının korunması da dahil olmak üzere, ***kamu güvenliği, ulusal güvenlik ve yasaların uygulanması*** faaliyetlerinde kriptolu cihaz ve sistemler kullanılmaktadır.

Kriptografi politikası milletlerarası arenada belirlenirken;

- Milli egemenlik,
- Kamu güvenliği ve kamu düzeni,
- Ülke ekonomik çıkarları ve ortak temel hedefler,

konuları göz önüne alınmaktadır.

Bu politikaların belirlenmesinde geçmiş yıllara bakıldığında;

- Bilgisayar ve iletişim, pahalı ve nadir,
- İletişim ağları analog ve ses odaklı,
- Telekomünikasyon sektöründe oyuncu sayısı az ve kontrol edilebilir,
- Süper güçler ekonomiye tartışmasız egemen,
- Güvenlik tehditleri (Soğuk Savaş),
- Kriptografinin askeri ve diplomatik amaçlarla kullanılması,

Günümüzde ve gelecekte ise;

- Bilgisayar ve iletişim kolay, ucuz ve fazla,
- Telekomünikasyon çok sayıda oyuncu içermekte,
- İletişim ağları dijital (ses ve görüntü),
- İletişim ortak altyapı ve birden fazla (örneğin, uydu, kablosuz),
- Süper güçlerin ekonomisi önemli değil,
- Güvenlik tehditleri, Soğuk Savaş dönemlerine oranla çok daha heterojen,
- Kriptografinin kamu kurum ve kuruluşlar ile gerçek ve tüzel kişilerce de önemli uygulamalarda kullanılması,

hususları karşımıza çıkmaktadır.

Geleneksel olarak, kriptografi bugüne kadar güvenlik ve istihbarat kuruluşlarınca kullanılmıştır. Ancak son yıllarda Amerika ve AB ülkelerinde büyük işletmecilerce ve bireylerce de çok çeşitli amaçlarla kullanılmaktadır. Ülkemizde ise, 5809 sayılı Kanun çerçevesinde usul ve esasları belirlenen Yönetmelik hükümleri ile kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerce de elektronik haberleşme cihazlarında kod veya kripto kullanımına imkan tanınmıştır.

Elektronik haberleşme cihazı üzerinden güvenli haberleşme yapabilme imkânı sunan kriptolu haberleşmenin gücünün iyi bilinmesi, gerekli altyapı çalışmalarının sağlanması, yazılım ve donanım bazında yerli üreticilerin desteklenmesi gelecekteki kripto politikalarını belirlememiz adına büyük önem arz etmektedir.

Bu tez çalışmasında; ulusal ve uluslararası kitap, yayın, rapor, master ve doktora tezleri, ulusal ve uluslararası düzenlemeler, inceleme, tavsiye dokümanları ve diğer ülke analizleri doğrultusundaki inceleme ve araştırmalara dayalı olarak yapılan tespitler yer almaktadır.

Bu tespitler neticesinde, Kamu Kurum ve Kuruluşları ile Gerçek ve Tüzel Kişilerin Haberleşme Hizmeti İçinde Kodlu veya Kriptolu Haberleşme Yapma Usul ve Esasları Hakkında Yönetmelik ile belirlenen usul ve esaslarda BTK'yı ilgilendiren hususlar ve uygulamaya yönelik öneriler aşağıda maddeler halinde özetlenmiştir.

ÖNERİLER

1. **Kamu kurum ve kuruluşlarınca kripto cihaz ve sistemlerinde milli kriptonun kullanılmasının zorunlu olması:**

Her alanda olduğu gibi haberleşme alanında da gelecekte milli değerlere sahip çıkan ve üretim yapan toplumlar ayakta kalabileceklerdir. Üretimde bilginin güvenliği ve

muhafazası en önemli unsurlardan birisidir. Bu çerçevede, belirlenecek politikalarda özellikle haberleşme alalında milli kriptolama kullanılmasının zorunlu hale getirilmesinin önemli olduğu düşünülmektedir.

Milli kriptolama politikası belirlenirken;

1. Kamu güvenliği, iç ve dış tehditler ve ulusal güvenlik nedenleri ile toplumunun bütün meşru unsurlarının kullanacağı yaygın bir kripto sistemi,
2. Bölgesel güç dengelerinde liderlik yapabilme adına kripto yazılımlarının geliştirilmesi,
3. Gelecekte etkin ve sürdürülebilir rekabet ortamı ve bu ekonomik değerden pay alabilme,
4. İhtisaslaşmış kuruluşlarla işbirliği,

hususları dikkate alınmalıdır.

Bu çerçevede, Yönetmelik ile belirlenen usul ve esaslarda, kamu kurum ve kuruluşlarına getirilen milli kripto kullanması ***esastır*** ifadesinin, kamu güvenliği, ulusal güvenlik ve ülke çıkarlarının korunması açısından ***zorunlu*** olarak değiştirilmesinin uygun olacağı,

2. Kripto sistemlerinde kullanılan elektronik haberleşme cihaz ihracatı ve imalatında uygulanacak esasların net olarak belirlenmesi:

Yönetmelik ile, kripto cihazlarının ithal veya imal edilme şartları belirlenmiştir. Kamu güvenliği ve ülke güvenliği konuları düşünüldüğünde belirlenen bu şartlara ilave veya ikincil bir düzenleme olarak;

- İthalatçı ve imalatçı firmalara lisans alma zorunluluğu getirilmesinin,lisanslama işlemlerinde firmanın faaliyet alanı olarak ticaret sicil gazetesinde haberleşme alanı şartının aranmasının,

- İmalat ve ithalatçı firmalardan, ithal veya imal ettiği ürünler için tüketici hakları için en az 10 yıllık süre için, donanım ve yazılım bazında teminat alınmasının,
- İthalatçı firmalarca ithal edilecek kripto cihaz ve sistemlerine izin işlemlerinde kripto anahtar uzunluğuna bir sınırlamanın getirilmesinin,
- İç piyasadaki ürün teşviklerini yavaşlatacak ithalatlarda, imalatçıların rekabet edebilmeleri ve ekonomik güç olabilmelerinin önündeki engellerin kaldırılmasının,
- Ülke dışındaki yabancı rakiplerin pazar payının çoğunluğunu ele geçirmesi halinde, bu durumun imalatçıları olumsuz yönde etkilememesi adına yazılım ve donanım bazında ithalat aşamasında teknik veriler ile sınırlar belirlenmesinin (Kurum tarafından belirlenecek teknik veriler doğrultusunda ithaline izin verilmelidir),

uygun olacağı,

3. Kripto sistemlere ithalat ve imalat lisanslarının verilmesi:

Kriptolu cihaz ithal veya imal edecek firmalar için bir lisanslama rejimi tarif edilmelidir. İhracat ve ithalat aşamasında verilecek lisans türleri bakımından mevzuatların verdiği yetki çerçevesinde;

1. ***İthalat Lisansı*** veya ***İthalat Sertifikası*** (Güçlü kripto içermesi bakımından kripto yetenekleri ile belirli en fazla 5 yıl süre için verilecek yetki),

2. İhtisas kuruluşlarına verilecek ***İmalat Lisansı*** veya ***İmalat Sertifikası*** (Kurum, üniversite ve araştırma kuruluşlarına 5 yıl süre ile verilecek yetki),

3. Kişisel gayretleri sonucunda kripto yazılımı ve donanımı yapan kişilere verilecek ***Bireysel Lisans*** veya ***Bireysel Sertifika*** (Güçlü kripto içermeyen gerçek ve tüzel kişilerin kullanımı için verilecek kripto sistem yetkisi)

verilmesinin uygun olacağı,

4. Kripto imal ve ithalinde uygulanacak standartların tespit edilmesi:

Standardizasyon, kriptografinin güvenlik mekanizmasının önemli bir yapı taşıdır. Elektronik haberleşme cihazlarında kullanılacak kripto sitemlerinde milli ve milletlerarası standartların belirlenmesi, ithalat ve imalat aşamaları ve pazar analizi bakımından önemlidir.

Kriptolama standartları belirlenirken; öncelikle bilgi ve iletişim sistemleri, bilgisayar ağları, mobil teknolojiler, telsiz sistemleri ve altyapı sistemleri göz önüne alınmalıdır. Standart belirlenmesinde amaç, yazılım ve donanım bazında imalat yapacak firmalara yol göstermesi, bu firmaların iç ve dış piyasada rekabet edebilmesi açısından önemli bir referans kaynağı oluşturulmasıdır. Bu konuda aşağıda temel başlıklar halinde belirlenen standartların Yönetmelik hükümlerine ilave edilmesi veya altında ikincil bir düzenleme yapılarak usulün nasıl gerçekleştirileceğinin bir mevzuata bağlanmasının uygun olacağı,

- Veri Kriptolama Standardı,
- Güvenli Hash Standardı,
- Dijital İmza Standardı,
- Saklanacak kripto algoritması ve anahtarları için Kriptolama Standardı,
- Kullanıcı Kimlik Tespit Standardı,
- Bilgisayar Ağ Erişim Kontrolü ve veri doğrulama standardı,
- Güçlü Kripto Standardı,
- Zayıf Kripto Standardı,
- Arayüz standartları.

5. **Kriptonun algoritma ve anahtarının, emniyeti ve alınması gereken muhafaza tedbirleri:**

Haberleşmede kişisel verilerin korunması esastır. Yönetmelik,

> ***"Emniyet ve muhafaza tedbirleri"*** **başlıklı maddesi ile** ***"(1) Kodlu veya kriptolu elektronik haberleşme cihaz/sistem kuran ve işleten kamu kurum ve kuruluşları ile gerçek ve tüzel kişiler, sistemlerinin yetkisiz kimselerin eline geçmesini ve yetkisiz kişilerce kullanılmasını engelleyici muhafaza tedbirlerini alır.***
> ***(2) Üreticiler tarafından Kuruma teslim edilecek olan kodlu veya kriptolu elektronik haberleşme cihaz/sistemlerine ait kod veya kripto algoritması ve anahtarları Kurum tarafından muhafaza edilir"*** hükmü ile alınacak tedbirleri belirlemiştir.

Yönetmeliğin bu hükmü gereğince üreticiler tarafından Kuruma teslim edilecek kod veya kripto algoritması ve anahtarının Kurum tarafından muhafaza edilmesi şartı getirilmiş ama nasıl muhafaza edileceği net olarak belirlenmemiştir.

Üreticiler tarafından teslim edilecek kripto algoritma ve anahtarının Kurum tarafından muhafazasında, nitelikli ve bilgili personel desteği ile ***"güvenli bir birimin"*** oluşturulmasının uygun olacağı,

6. **Kripto yazılım ve donanım bazında çalışma yapacak enstitüler, üniversiteler veya bilimsel araştırma-geliştirme yürüten ihtisas sahibi kuruluşların teşvik edilmesi:**

Yönetmelik, Kurum ile protokol yapan enstitüler, üniversiteler veya bilimsel araştırma-geliştirme çalışmaları yürüten ihtisas sahibi kuruluşlara, kodlu veya kriptolu haberleşme sistemleri için yapılacak başvuruların değerlendirilmesi konusunda işbirliği yapma imkânı getirmiştir.

İhtisas sahibi kuruluşlar, başvurularının değerlendirilmeleri dışında, kripto yazılım ve donanımları bakımından günümüzde ve gelecekte oluşacak pazar taleplerinin karşılanabilmesi için teşvik edilmelidirler. Pazar payı bu kadar büyük olan bu sektörde, isteklere cevap verilmesinin, piyasaya arz edilecek izinsiz kripto yazılım ve donanımların önüne geçilmesinin ve yerli üretimin teşvik edilmesi için de ihtisaslaşmış kuruluşlarca işbirliği yapılmasının önemli olduğu değerlendirilmektedir.

Bu konuda Ulaştırma, Denizcilik ve Haberleşme Bakanlığı tarafından çıkarılan,

> ***"Elektronik Haberleşme, Uzay ve Havacılık Sektöründe Araştırma Geliştirme Projelerinin Desteklenmesine İlişkin Yönetmelik"***

kapsamında, yerli üretimin desteklenmesi adına kripto yazılım ve donanımı yapacak ihtisas sahibi kuruluşlara da kaynak aktarılmasının faydalı olacağı düşünülmektedir.

Bahse konu Yönetmelik ile, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'na gelen projelerin incelenmesinin ardından ön değerlendirme Grubu'na gönderilmesi ve projelerin mevzuata uygunluğunun Haberleşme Genel Müdürlüğü ile Kurum tarafından belirlenen öncelikli projeler arasında bulunup bulunmadığı konusunda tespit yapılma aşamada Kurumun, kripto yazılım ve donanım bazında cihaz ve sistem imal edecek yerli üreticileri desteklemesinin ve teşvik etmesinin uygun olacağı,

7. **İzinsiz kripto cihaz ve sistem kullanımında uygulanacak cezaların yeniden belirlenmesi:**

Mülga Yönetmeliğin "Müeyyideler" başlıklı hükmünde,

> ***"İzinsiz kriptolu telsiz cihaz ithal veya imal ederek satışını yapan kuruluşlar ile bu cihazları kullanan kuruluşların cihazları mühürlenerek ilgili hakkında 2813 sayılı Telsiz Kanunu ve 3763 sayılı "Harp Araç ve***

> ***Gereçleri ile Silâh, Mühimmat ve Patlayıcı Madde Üreten Sanayi Kuruluşlarının Denetimi Hakkında" Kanun uyarınca da gerekli yasal işlemler yapılır"***

ifadesi yer almaktadır.

3763 sayılı Kanunun amacı ise,

> ***"harp araç ve gereçleri ile silâh, mühimmat ve patlayıcı madde üreten sanayi kuruluşlarının kurulması, işletilmesi ve yükümlülükleri ile denetimine ilişkin esas ve usulleri düzenlemektir"***

olarak ifade edilmiştir.

Mülga Yönetmelik, izinsiz olarak kriptolu telsiz cihazlara getirdiği müeyyideler ile, atıfta bulunduğu 3763 sayılı Kanun kapsamında mühimmat sınıfında değerlendirerek ağır hapis cezalarına hükmetmiştir.

Mevcut Yönetmelikte izinsiz kriptolu cihaz kullanılmasındaki müeyyide 5809 sayılı Kanun'un 60 ve 63 hükümlerini içermektedir. Kanun'un idari yaptırımlar başlıklı 60 ıncı maddesinde ***işletmecilere*** uygulanacak idari para cezası ile piyasa gözetim ve denetiminde aykırılık halinde, cihaza teknik uyumluluk hükümlerince para cezasına hükmetmiştir. Söz konusu maddede izinsiz kriptolu cihaz kullanımı ile ilgili olarak bağlayıcı bir hüküm bulunmamaktadır.

Kanun'un "Cezai hükümler" başlıklı 63 üncü maddesinde ise Kurumdan izin alınmadan, "Bu Kanunun 39 uncu maddesine aykırı olarak kodlu ve kriptolu haberleşme yapan ve yaptıranların beş yüz günden bin güne kadar adli para cezası ile cezalandırılacağı" ifade edilmiştir.

Mülga Yönetmelikte sadece Telsiz sistemlerinde izinsiz kriptolu cihaz imal veya ithal edilmesine ilişkin müeyyideler bulunmaktaydı. Elektronik haberleşme cihazlarının tümünü kapsayan mevcut Yönetmelik ile izin alınmadan kullanılacak

kriptolu cihazlar için getirilen müeyyidelerin daha caydırıcı bir hale getirilmesi gerektiği değerlendirilmektedir.

Bu aşamada, Kurumdan izin alınmadan ithal veya imal edilecek kriptolu cihazların kamu güvenliği ve ülke güvenliğine karşı bir tehdit olmaması adına izinsiz cihazlar için yeniden belirlenecek müeyyidelerin Yönetmelik hükümlerine ilave edilmesi veya altında ikincil bir düzenleme yapılmasının uygun olacağı,

8. Deneme, test veya benzeri amaçlı imal ve ithal edilecek kriptolu cihazlara verilecek iznin belirlenmesi:

Kanunun "Deneme izni" başlıklı 10 uncu maddesinde,

> ***"Kurum, elektronik haberleşme hizmetinin verilebilmesi, elektronik haberleşme şebekesi ve altyapısının işletilebilmesi için başvuruda bulunan gerçek ve tüzel kişilere deneme veya gösterim amaçlı geçici izin verebilir. Bununla ilgili usul ve esaslar Kurum tarafından belirlenir"***

hükmü bulunmaktadır.

Deneme izinleri ile ilgili olarak usul ve esasların belirlendiği Elektronik Haberleşme Sektörüne İlişkin Yetkilendirme Yönetmeliği ilgili 23 üncü maddesinde,

> ***"Kurum, Türkiye Cumhuriyeti kanunlarına göre kurulmuş sermaye şirketleri, araştırma–geliştirme kuruluşları ile kamu kurum ve kuruluşlarının, test ve/veya deneme ve/veya gösterim amaçlı olarak kurmak ve kullanmak istedikleri elektronik haberleşme altyapı ve hizmetlerine geçici süre ile izin verebilir"***

hükmü, ayrıca Telsiz İşlemlerine İlişkin Usul ve Esaslar Hakkında Yönetmeliğin "Geçici süreli kullanımlar" başlıklı 10 uncu maddesinde,

> ***"Kanunun 10 uncu maddesi kapsamında verilen deneme izinleri hariç olmak üzere; geçici olarak düzenlenen fuar, sergi, konferans, konser, spor, araştırma, geliştirme, test ve benzeri faaliyetlerde kullanılacak telsiz cihaz ve sistem izinleri için faaliyet öncesinden aşağıda belirtilen belgeler ile Kuruma başvurulur"***

hükümleri yer almaktadır.

Yukarıda açıklanan Kanun maddesi ve Yönetmelikler çerçevesinde; deneme, test veya benzeri amaçlı ithal edilen veya imal edilen kriptolu haberleşme sistem ve cihaz izinlerine ilişkin mevcut Yönetmelikte herhangi bir usul ve esas belirlenmemiştir. Araştırma–geliştirme, test deneme ve/veya gösterim amacı ile fuar ve sergilerde kurmak ve kullanmak istedikleri kodlu veya kriptolu haberleşme cihazlarına ilişkin düzenlemelerin Yönetmelik hükümlerine ilave edilmesi veya altında ikincil bir düzenleme yapılmasının uygun olacağı,

değerlendirilmiştir.

KAYNAKLAR

BELLOVİN S.M. ,1998, "Cryptography And The Internet, in Proceedings of CRYPTO '98"

BERT-JAAP Koops, 2013, "Summary Of International Crypto Controllers"

BTK, 2013, SAS Daire Başkanlığı, "Yetkilendirme ve Hizmet Türlerine Göre İşletmeci Sayıları" Bilgi Teknolojileri ve İletişim Kurumu, Ankara

CEYLAN Cenk, 2009, "Geleceğin Bilgisayarları, Şifre Sistemleri ve Kuantum Kriptoloji"

CHRISTOF Paar, JAN Pelzl, 2009, "Stream Ciphers", Chapter 2 of "Understanding Cryptography, A Textbook for Students and Practitioners"
Current Public-Key , 2000, "Cryptographic Systems', Paper of Certicom, dd.

ÇELİK Osman, 2004, "Kriptolojiye Giriş"

ÇİNEM Canan, AKLEYLEK Sedat, AKYILDIZ Ersan, 2007, "Şifrelerin Matematiği- Kriptografi",s, 7, 30, 33, 34, 35, 80, 102, 103, 104

DEMİR Bünyamin, 2004, "Kriptoloji"

DERELİ T., VERÇİN A., ,2009, "Kuantum Mekaniği Temel Kavramlar ve Uygulamaları"

DİFFİE W., Hellman M.E., 1976, "New Directions in Cryptography", IEEE Trans.

Doç. Dr. GELERİ Aytekin, 2010, Dinle(n)me Paranoyası

DOĞAN Yasir A, 2006, Sfınks Dizi Kriptolama Algoritmasının Vhdl İle Yazılımı ve Fpga Üzerinde Gerçeklenmesi, Yüksek Lisans Tezi, İTÜ,

EKİN A.Bülent , 2006, "Kriptoloji"-A.Ü.Fen Fakültesi Matematik Bölümü

El Gamal T., ,1998,"A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms.Advances in Cryptology: Proceedings of CRYPTO 84"

ERDEM Mustafa Ruhan, 2005, "5271 Sayılı CMK'da Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi"

EREN A. Murat, 2005, "Açık Anahtarlı Kriptografi",

ERSOY Erkut, 2003, "Ulusal Bilgi Güvenliği Raporu ve Teknolojik Gelişmeler"

GEÇKİNLİ C. N., 2009, "Rasgelelik (Rastlantısallık) Kavramına Genel Bir Bakış", UEKAE Dergisi, Sayı 1, s96-103,

GOLDSMİTH, M., ,1983,'The Supreme Court and Title III: Rewriting the law of electronic surveillance', The Journal of Criminal Law & Criminology, Vol.74, No.1, , s.46

GÖRÜR Hamit, 2010, Ceza Muhakemesi Hukuku'nda Telekomünikasyon Yoluyla İletişimin Denetlenmesi, İzmir

JAAP Koops Bert, 1999, The crypto controversy

JOHN Wiley & Sons, 1996, SCHNEİDER B. "Applied Cryptography Second Edition",New York

KALISKA B., 2001, "the mathematics of the rsa public-key cryptosystem", rsa laboratories ny

KAPOR B, 2009, Pandya P. Data Encryption, Computer and Information Security Handbook

KARA Orhun, Kriptolojide Temel Kavramlar, Tübitak-Bilgem, 2012

KOBLİTZ, N.,, 1994, 'A Course in Number Teory and Cryptography', Springer-Verlag, New York

KODAZ H., 2002, Veri İletiminde Güvenlik İçin Kriptolama, Selçuk Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi.

KODAZ H., 2003, RSA Şifreleme Algoritmasının Uygulaması, İnceleme

KODAZ Halife, BOTSALI Fatih M. 2010, Simetrik ve Modern Kriptolama Algoritmalarının Karşılaştırılması- -Bilgisayar Mühendisliği Bölümü, Selçuk Üniversitesi, Alaeddin Keykubad Kampüsü, Konya

KOLTUKSUZ A. ,1999, " Cryptography in Action" ISCIS'99,

KRİSHNAMURTHY M, Seagren ES, Alder R, Bayles AW, Burke J, Carter S, Faskha E., 2008, Basics of Cryptography and Enryption, How to Cheat at Securing Linux,

KUTLAY Mustafa, 2001, "Adamı Olan Cep'te İstediğini Dinliyor"

MENEZES A., OOSCOT P., VENSTONE S., 1996, "Handbook of Aplied Cryptograpy", October

METİN Şengül, 2007, Güvenli ses haberleşmesi, İstanbul Üniversitesi Fen Bilimleri Enstitüsü, Yüksek Lisans,POLLARD Rho,"Algorithm"

QUANTIS, 2011, True RANDOM NUMBER Generator Exploiting QUANTUM PHYSICS, http://www.idquantique.com/. Erişim: 2011.

RİVEST R.,. Shamir A., Adleman L.,1978, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, v.. 120-126.

SALOMAA, A. „1990, 'Public-Key Cryptography', Springer-Verlag, New York

Savaş, E., 1994. "Dizi Şifreleme Sistemleri ve Doğrusal Karmaşıklık", *Yüksek Lisans* ,İ.T.Ü. Fen Bilimleri Enstitüsü, İstanbul.

SHANNON, C.E., 1949, "Communication theory of secrecy systems", Bell System Technical Journal, 28, 656-715

STALLİNGS W., 1998, "Cryptography and Network Security: Principles and Practice",

STAPKO T. , 2008, Security Protocols and Algorithms, Practical Embedded Security,

ŞAHİN A. Behzat, SELÇUK Gökhan, "İletişim Ağ Güvenliğinde Son Aşama: Kuantum ve Fiber Optik Ortamda Kuantum Temelli Rastsal Sayı Üretimi"- Tübitak Proje-

ŞAHİN Murat, 2007, Bilgi Güvenliği ve Sayılar Teorisi-A.Ü.Fen Bilimleri Enstitüsü Yüksek Lisans Tezi, Ankara, s,12, 12, 16, 25, 31

ŞAHİN Murat, 2009, "Sonlu Cisimlerde Diskret Logaritma Problemi", A.Ü. Matematik Ana Bilim Dalı, Ankara, Doktora Tezi,

ŞEN Evren, 2008, "Kriptografi Ve Kullanım Alanları"

SÖZBİLİMCİ Şuayp, 2005, "Kriptoloji ve bir RSA Uygulaması",

SCHNEIER B., 1996, "Applied Cryposystem: Protocols, Algorithms and source Code in C, 2th Editin.

TARHAN C. Foster M., 2001, "İnceleme"

TEKTAŞ M. ,Baba F. ,Çalışkan M., 2003, "Kriptolama Algoritmalarının Sınıflandırılması ve Bir Kredi Kartı Uygulaması" 3. International Advanced Technologies Symposium, , ANKARA

TMMOB Elektrik Mühendisleri Odası, 2009, "İletişim Özgürlüğüne Müdahale Raporu"

TOYRAN M., PEDERSEN .B. Thomas, HASEKİOĞLU A.S. Atilla, CAN M.Ali, BERBER Savaş, 2011, "Bilgi Güvenliğinde Kuantum Teknikleri"

TÜBİTAK-Uekae, 2008, "Milli Kriptolama Sistemleri"

TRAPPE W., 2002, 'Introduction To Cryptography With Coding Theory',

VASİF V. Nabiyev, GÜNAY Asuman, Kriptolama yönteminin tespiti amacıyla çeşitli kriptolama algoritmalarının araştırılması- Karadeniz teknik üniversitesi M.f. Bilgisayar Mühendisliği Bölümü

VERNAM G., 1926, "Cipher Printing Telegraph Systems For Secret Wire And Radio Telegraphic Communications", J. Am. Institute of Electrical Engineers, Vol. XLV, 109-115.]

YERLİKAYA T, BULUŞ E, BULUŞ N., 2006, "Modern Kriptolama Algoritmalarında Anahtar Değişim Sistemleri"

YERLİKAYA Tarık, BULUŞ Ercan, ARDA Derya, 2003, Modern Kripto Sistemler ve Uygulamaları

YERLİKAYA Tarık, BULUŞ Ercan, BULUŞ Nusret, 2006, "Kripto Algoritmalarının Gelişimi Ve Önemi"

YERLİKAYA Tarık, BULUŞ Ercan, BULUŞ Nusret, 2007, "Kriptolama Algoritmasının Pollard Rho Yöntemi İle Kriptanalizi."

EKLER

Ek-1

Matematik Ön Bilgi

Çarpanlara ayırma matematiğin yüzyıllardır üzerinde uğraştığı ve büyük sayıların çarpanlara ayrılması için pratik bir yol bulamadığı bir konudur. Her ne kadar matematik bir tanım olmasa da şimdi "***ZOR***" kavramını tanımlamamız gerekir.

Keyfi büyüklükte herhangi iki **p** ve **q** asal sayılarını aldığımızda bunların çarpımı olan N sayısını oluşturmak çok kolaydır.

$$p.q = N$$

Şimdi matematiğin hemen hemen tarihi kadar eski olan iki problemi inceleyelim.

Çarpanlara Ayırma Problemleri

Problem: **N** bilindiğinde **p** ve **q**'nun bulunmasıdır.

Bilinen bütün yöntemlerin ve mevcut teknolojilerin sınırsızca kullanarak makul zaman içerisinde bir problemin çözülmesine "***Zor***" diyeceğiz. "***Zor***"'un karşıtı olarak "***Kolay***"'ı tanımlayacağız.

Diskret logartima problemi

$p > 2$ *asal sayı olmak* üzere $Z_p^* = \{1,2,3, \dots p-1\} = \{g, g^2 g^3 g^4 \dots \dots g^{p-1}\}$'dir.

Bir g tamsayısı vardır ki bu g tamsayısına modüleye göre bir primitif kök denir. Matematikte p verildiği zaman g'nin bulunma yöntemleri mevcuttur.

Her bir **a** tamsayısı için,

$$1 \leq a \leq p-1 \text{ için } a \equiv g^t (mod\ p) \text{ ve } 1 \leq t \leq p-1$$

olacak şekilde bir **t** tamsayısı vardır.

Bu t tamsayısına **a**'nın **g** tabanından diskret logaritması denir ve

$$\mathbf{D}\log_{\mathbf{g}}\mathbf{a} := \mathbf{t} \text{ ile gösterilir.}$$

Diskret logaritma, bildiğimiz doğal logaritma ile aynı özelliktedir.

$$\boldsymbol{Dlog}_g^1 = \mathbf{0}$$

$$\boldsymbol{Dlog}_a\boldsymbol{b} = \boldsymbol{log}_a + \boldsymbol{log}_b$$

$\boldsymbol{k} \in \boldsymbol{Z}$ olmak üzere,

$\boldsymbol{Dlog}_a^k = \boldsymbol{k}\,\boldsymbol{Dlog}\,\boldsymbol{a}$ 'dır.

Bunlar Diskret logaritma tanımından elde edilecek sonuçlardır.

Problem: $\boldsymbol{a}, \boldsymbol{g}$ *ve* $\boldsymbol{p}$ tamsayıları bilinirken $\boldsymbol{t}$'nin bulunması,

p=11 ve g=2 alırsak

$2^2 \equiv 4 \pmod{11}$ $\quad 2^6 \equiv 9 \pmod{11}$ $\quad 2^{10} \equiv 1 \pmod{11}$

$2^3 \equiv 8 \pmod{11}$ $\quad 2^7 \equiv 7 \pmod{11}$

$2^4 \equiv 5 \pmod{11}$ $\quad 2^8 \equiv 3 \pmod{11}$

$2^5 \equiv 10 \pmod{11}$ $\quad 2^9 \equiv 6 \pmod{11}$

Böyle bir tabloda p ayısı keyfi büyük olduğunda oluşacak tablo hafızalara sığmayacak şekilde olur.

$$\mathbf{Z}_{11}^* = \{1,2,3,4,5,6,7,8,9,10\} = \{2, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, 2^{10}\}$$

Fermat: p asal, $a \in \mathbf{Z}$ ve $p \nmid a$ olsun.

$a^{p-1} \equiv 1 \pmod{p}$ $\quad \left[a^p \equiv a \pmod{p}\right]$

Euler: $n \in \mathbf{Z}$ ve $n > 1$, ebob(a , n) = 1 olsun.

$a^{\varphi(n)} \equiv 1 \pmod{n}$

$\varphi(n) :=$ " $1 \le x < n$ ve ebob(x , n) = 1 olan x tamsayılarının sayısı "

$\varphi(1)=1 \qquad \varphi(2)=1 \qquad \varphi(3)=2 \qquad \varphi(4)=2 \qquad \varphi(5)=4$

1° p asal sayı ve $k \in \mathbf{Z}^+$ ise $\varphi(p^k)=p^k-p^{k-1}=p^k(1-1/p)$

2. ebob (a,b) = 1 ise $\varphi(a.b)=\varphi(a).\varphi(b)$

Örneğin; $\varphi(6)=\varphi(2.3)=\varphi(2).\varphi(3)=1.2=2$

3° $n=p_1^{k_1}\cdot p_2^{k_2}\cdot p_3^{k_3}\cdots p_r^{k_r}$ ise $\varphi(n)=n\cdot(1-1/p_1)(1-1/p_2)\ldots(1-1/p_r)$

$\boxed{504=2^3\cdot 3^2\cdot 7 \quad \text{için} \quad \varphi(504)=504\cdot(1-1/2)(1-1/3)(1-1/7)=144}$

(Not: Eğer bir **N** tamsayısı verildiğinde **N**'nin çarpanlara ayrılışını bilmiyorsak $\boldsymbol{\varphi(N)}$ değerini bulmak sayma problemine dayandığından zordur.)

Ek-2

Modüler Aritmetik

Modüler aritmetikte, bölme işlemine dayanan bir sayı sistemidir. Bölme işleminde bir a tamsayısının n tamsayısı ile bölünmesinden elde edilen bölüm b, kalan k sayısı olsun:

$$\mathbf{a = n.b + k}$$

Bölme kuralına göre;

$$\mathbf{0 \leq k \leq (n - 1)}$$

olacaktır.

Modüler aritmetik belli bir sayıya (modüle) göre diğer bütün sayıları o modülün kalan kümesindeki sayılarla ifade eder.

$$\mathbf{a \equiv k\ (modn)}$$

şeklinde gösterilir.

Örneğin:

19 ve 23 sayıları 2'e bölündüğünde her ikisinde de kalan 1'dir. Yani $19 \equiv 1 \pmod 2$ ve $23 \equiv 1 \pmod 2$ olarak gösterilir.

Ek-3

EN BÜYÜK ORTAK BÖLEN (E.B.O.B.)

İki veya daha fazla doğal sayıdan her birini bölebilen en büyük doğal sayıya bu sayıların en büyük ortak böleni denir ve e.b.o.b. biçiminde gösterilir.

EN KÜÇÜK ORTAK KAT (E.K.O.K.)

İki veya daha fazla doğal sayıdan her birini bölünebilen (her birinin katı olan) bu sayıların en küçük ortak katı denir ve e.k.o.k. biçiminde gösterilir.

A pozitif tam sayısı a × b ile tam bölünebiliyor ve e.k.o.k.(a ; b) = x ise, A sayısı x ile tam bölünür

a ve b pozitif tam sayı olmak üzere, $\frac{a}{b}$ 'nin en sade biçimi $\frac{x}{y}$ olmak üzere,

$$\frac{a}{b} = \frac{x}{y} \text{ ise,}$$

E.b.o.b. (a;b) = $\frac{a}{x} = \frac{b}{y}$ ve

E.k.o.k. (a;b) = b . x = a . y 'dir.

En sade biçimdeki, $\frac{a}{b} = \frac{c}{d}$ kesirleri ile tam bölünebilen en küçük pozitif kesir,

$$\frac{e.k.o.k(a;c)}{e.b.o.b\ (b;d)} \text{ 'dir.}$$

E.b.o.b (a;b) = x ise $e.b.o.b.\left(\frac{a}{x} = \frac{b}{x}\right) = 1$'dir.

E.b.o.b.(x × a ; x × b) = x × E.b.o.b.(a ; b)

E.k.o.k.(x × a ; x × b) = x × E.k.o.k.(a ; b)

a ile b ardışık iki doğal sayı ise,E.b.o.b.(a ; b) = 1,

E.k.o.k.(a ; b) = a × b dir.

a, b, c ardışık üç doğal sayı ise,E.b.o.b.(a ; b ; c) = 1 dir

Ek-4

Tamsayılar

Tamsayılar kümesi Z sembolü ile gösterilir ve {....,-3, -2,-1, 0, 1, 2, 3,....} sayılarından oluşur.

Tamsayılar için Bölme Algoritması (Öklid Algoritması)

Kabul edelim ki a ve b tamsayılar $b \geq 1$ olmak koşuluyla a'nın b'ye bölümü q tamsayısı gibi bir bölüm ve r tamsayısı gibi bir kalan verir.

$$a = b.q + r \qquad 0 \leq r \leq b$$

Her a ve b tamsayısı için bir tane q ve r tamsayıları vardır. Kalan r sayısı b'den küçük bir sayı olmalıdır.

Örnek;

$a = 26$, $b = 4$ olsun. Buna göre

$26 = 6.4 + 2$ bulunur.

Böylece $q = 6$, $r = 2$ olmaktadır.

Asal Sayı

1'den büyük, sadece 1 ve kendisine bölümünde 0 lakanı veren tamsayılara asal sayı denir. Asal olmayan sayılara ise bölünebilir sayı denir.

Aritmetiğin Temel Problemi

$n \geq 2$ olan her tamsayı k tane asal sayının çarpımı şeklinde tek olarak yazılabilir.

$n = p_1^{e1} . p_2^{e2}....p_k^{ek}$. Buradan $p_1, p_2,....p_k$ farklı asal sayılardır ve $e_1, e_2,....,e_k$ ise pozitif tamsayıdır.

Örnek:

$11520 = 2^8 \times 3^2 \times 5$

Ek-5

İkilik Taban Aritmetiği

Günlük yaşantımızda kullandığımız sayılar genelde onluk tabanlıdır ve onun kuvvetlerine göre sıralanmıştır.

Örneğin;

$8421 = 8 \times 10^3 + 4 \times 10^2 + 2 \times 10^1 + 1 \times 10^0$ olur.

Onluk tabanındaki bir sayıyı 2'lik tabanına çevrilmesi,

Örneğin;

21 sayısının ikilik tabanına çevirirsek,

$21/2 = 10$ kalan 1

$10/2 = 5$ kalan 0

$5/2 = 2$ kalan 1

$2/2 = 1$ kalan 0

$(1\ \ 0\ \ 1\ \ 0\ \ 1)_2$ sonucu elde edilir.

İkilik tabanda toplama, çıkarma, çarpma ve bölme işlemleri onluk tabanda yapıldığı gibi yapılır. Bu işlemlere ek olarak AND, OR ve XOR işlemleri ikilik tabana özgüdür.

Örneğin;

İki sayıyı XOR işlemine sokalım. Seçtiğimiz sayılar 15 ve 11 olsun.

$15 = (1111)_2$

$11 = (1011)_2$

kuralı uygularsak; $(1111) + (1011) = (0100)_2$

sayısı onluk tabanında: $0 \times 2^0 + 0 \times 2^1 + 1 \times 2^2 + 0 \times 2^3 = 4$

Yani 15 ve 11 sayılarının XOR'laması 4 sayısını verir.

ÖZGÜNLÜK BİLDİRİMİ

Uzmanlık tezi olarak sunduğum bu çalışmayı, bilimsel ahlak ve geleneklere aykırı düşecek bir yol ve yardıma başvurmaksızın yazdığımı, yararlandığım eserlerin kaynakçada gösterilenlerden oluştuğunu, bunlardan her seferinde değinme yaparak yararlandığımı ve Bilgi Teknolojileri ve İletişim Kurumu Meslek Personeli Sınav, Görev, Çalışma Usul ve Esasları Hakkında Yönetmeliğe uygun olarak hazırladığımı belirtir, bunu onurumla doğrularım.

Bilgi Teknolojileri ve İletişim Kurumu tarafından belli bir zamana bağlı olmaksızın, tezimle ilgili yaptığım bu beyana aykırı bir durumun saptanması durumunda, ortaya çıkacak tüm ahlaki ve hukuki sonuçlara katlanacağımı bildiririm.

20./..06./2013

Mustafa TEFON

ÖZGEÇMİŞ

1965 yılında Kayseri ili Yeşilhisar ilçesinde doğdu. İlk, orta ve lise öğrenimini Ankara'da tamamladı. 1984 yılında girdiği A.Ü. Fen Fakültesi Fizik Mühendisliği bölümünden 1989 yılında mezun oldu. 1993 yılında Ulaştırma Bakanlığı Telsiz Genel Müdürlüğünde Telsiz Monitör Uzmanı olarak göreve başladı. 2000 yılında kurulan Telekomünikasyon Kurumunda Teknik Düzenleme ve Standardizasyon Dairesi Başkanlığında yaklaşık 11 yıl Test ve Ölçüm Laboratuarında, cihazların test ve ölçümleri ile standartları ile ilgili olarak çalıştı. 2006-2011 yılları arasında Spektrum Yönetimi Dairesi Başkanlığı'nda, 2012 yılından itibaren ise Teknik Düzenleme Dairesi Başkanlığında çalışmalarına devam etmektedir.