

Bu notlar Samsun Üniversitesi Yazılım Mühendisliği bölümünde verilen Kriptoloji Dersi için uygun bazı kaynaklardan hazırlanmıştır. Herhangi bir şekilde orijinallik ve yayın niteliği yoktur. Sadece eğitim amaçlı ders notları niteliğindedir.

Hafta 7

Temel Şifreleme Yöntemleri

Kriptoloji Nedir?

Kriptoloji, kavram olarak şöyle tanımlanabilir: "Kriptoloji, haberleşen iki veya daha fazla tarafın bilgi alışverişini emniyetli olarak yapmasını sağlayan, temeli matematiksel zor problemlere dayanan tekniklerin ve uygulamaların bütünüdür."

Günümüzde kriptoloji, matematik, elektronik, optik, bilgisayar bilimleri gibi birçok disiplini kullanan özelleşmiş bir bilim dalı olarak kabul edilmektedir. Kriptolojinin iki temel alt dalı vardır:

Kriptografi

Kriptoanaliz

Kriptografi, belgelerin şifrelenmesi ve şifresinin çözülmesi için kullanılan yöntemlere verilen addır.

Kriptoanaliz, kriptografik sistemlerin kurduğu mekanizmaları inceler ve çözmeye çalışır. Kriptoanalizin kriptoloji önemi çok büyüktür çünkü ortaya konan bir şifreleme sistemini inceleyerek, zayıf ve kuvvetli yönlerini ortaya koymak için kriptoanaliz kullanılır.

Haberleşmede Emniyet Kavramları

Gizlilik: Taşınan bilginin içeriğinin gizli kalmasıdır.

Bütünlük: Taşınan bilginin içeriğinin yolda değiştirilememesidir.

Kimlik Doğrulama: Bilgiyi gönderen kişinin kimliğinin doğruluğundan emin olmaktır.

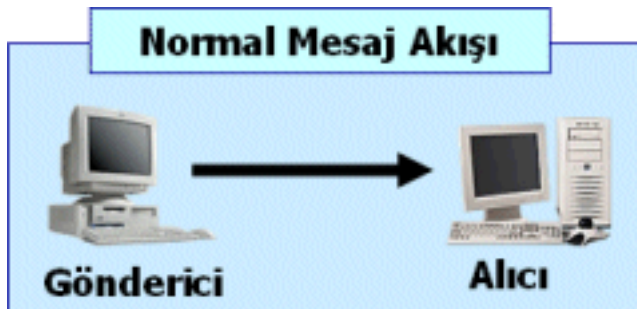
İnkâr Edememezlik: Bilgiyi gönderen veya işleyen kişinin yaptığı işi sonradan inkâr edememesidir.

Haberleşmenin Sürekliliği: Haberleşmenin kesintiye uğramadan yapılmasıdır.

Elektronik Tehditler

Haberleşen iki taraf, bilgisayar ağları, kablolu veya kablosuz iletişim kanalları kullanarak bir bilgiyi, mesajı bir taraftan diğerine iletirler.

Elektronik ortamda haberleşen taraflar çeşitli tehditlerle karşı karşıya kalırlar.

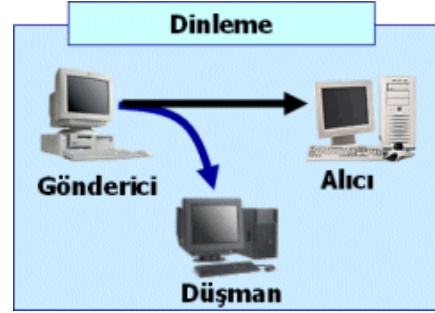


Elektronik Tehditler

Gizlilik İhlali !

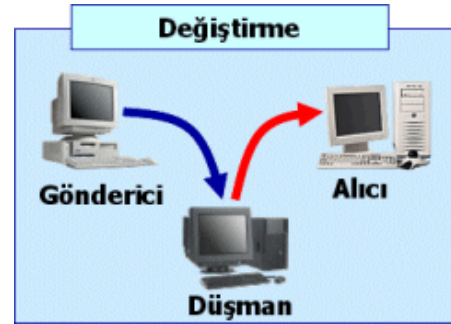
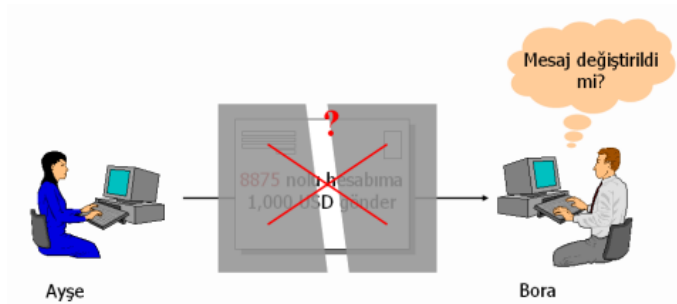
Haberleşme kanalını dinleyen saldırgan gönderici ile alıcı arasındaki mesaj trafiğini dinleyebilir ve elde ettiği mesajları okuyarak bu haberleşmenin gizliliğini bozar.

Bu tehdit dinleme tehdidi olarak bilinir.



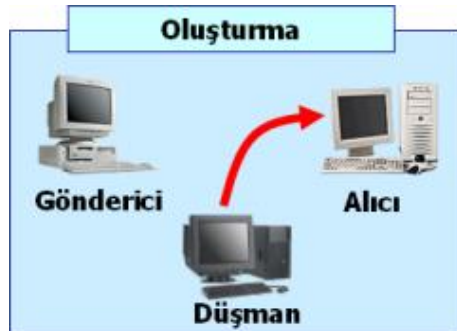
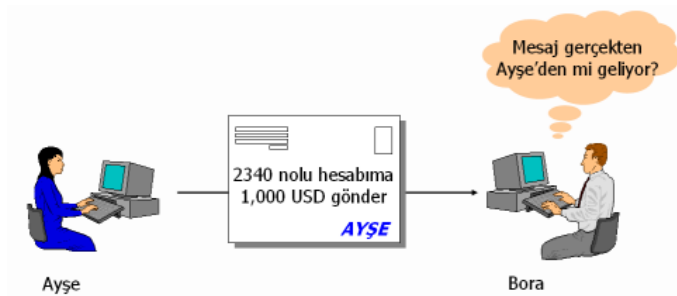
Bütünlük İhlali !

Haberleşmeye müdahale edip göndericinin mesajlarını değiştiren saldırgan, alıcıya giden mesajı istediği şekle sokabilir. Bu tehdit mesajın bütünlüğünü bozan değiştirme tehdididir.



Kimlik Doğrulama İhlali !

Saldırgan, alıcıya göndericinin kimliğini taklit ederek bir mesaj gönderebilir. Bu durumda eğer alıcı güvenilir bir kimlik doğrulaması yapmıyorsa yanlış mesajlarla kandırılabilir. Bu tehdit oluşturma tehdididir.



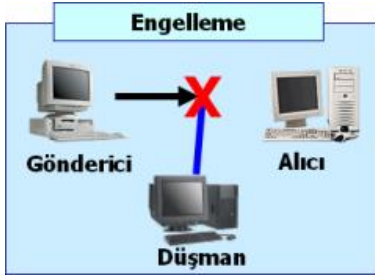
İnkâr Edememezlik İhlali !

Mesajı gönderen veya alan tarafın bu işi yaptığını inkar etmesi söz konusu olabilir. Bu kötü niyetli girişimi boşa çıkaracak mekanizmalara ihtiyaç vardır.



Süreklilik ihlali!

Saldırgan, haberleşen iki taraf arasındaki hattı veya haberleşme araçlarını kullanılmaz hale getirerek haberleşmenin sürekliliğini engellemeye çalışır.



Elektronik Tedbirler

Elektronik haberleşmedeki tehditlere karşı yine elektronik tedbirler alınarak korunma sağlanabilir. Bu tehditlere karşı alınabilecek tedbirler ve kullanılabilecek yöntem ve araçlar aşağıda görülmektedir.

Gizlilik sağlamak için veri şifreleme yöntemleri kullanılır.

Bütünlük sağlamak için özetleme algoritmaları, mesaj özetleri, elektronik imzalar kullanılır.

Kimlik doğrulaması için özetleme algoritmaları, mesaj özetleri, elektronik imzalar, sertifikalar kullanılır.

İnkâr edememezlik için elektronik imzalar, işlem kayıtları kullanılır.

Süreklilik için yedek sistemler, bakım, yedekleme, alternatif haberleşme kanalları kullanılır.

Şifreleme Nedir?

Şifreleme, bir bilginin özel bir yöntemle değiştirilerek farklı bir şekle dönüştürülmesi olarak tanımlanabilir.

Şifreleme işlemi sonucunda ortaya çıkan yeni biçimdeki bilgi, şifre çözme işlemine tabi tutularak ilk haline dönüştürülebilir.

Şifreleme yönteminde aranan bir takım özellikler vardır.

Şifreleme ve şifre çözme işleminin zorluğu ihtiyaç duyulan güvenlikle doğru orantılı olmalıdır. Çok önemli olmayan bir bilginin şifrelenmesi için bilginin kendisinden daha fazla işgücü ve zaman harcanması verimli olmayacaktır.

Anahtar seçimi ve şifreleme algoritması özel koşullara bağlı olmamalıdır. Şifreleme yöntemi her türlü bilgi için aynı şekilde çalışmalıdır.

Şifreleme Özellikleri

Şifrelemede yapılan hatalar sonraki adımlara yansımamalı ve mesajın tamamını bozmamalıdır. Saldırılarına karşı bu özellik koruyucu olacaktır. Ayrıca haberleşme hattında meydana gelen bir hata bütün mesajın bozulmasına neden olmayacağı için bu özellik tercih edilmektedir.

Kullanılan algoritmanın karıştırma özelliği olmalıdır. Mesajın şifrelenmiş hali ile açık hali arasında ilişki kurulması çok zor olmalıdır.

Kullanılan algoritmanın dağıtma özelliği olmalıdır. Mesajın açık hali şifreli hale gelirken içerdiği kelime ve harf grupları şifreli mesajın içinde olabildiğince dağıtılmalıdır.

Basit Şifreleme Yöntemleri

Mono Alfabetik Şifreleme

Sezar Şifresi

Tablo Yöntemi

Poli Alfabetik Şifreleme

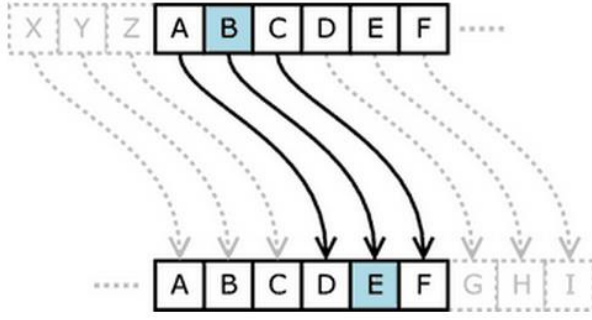
Vigenere tablosu

Tek Kullanımlık Karakter Dizisi

Sezar Şifresi

Sezar yöntemi mono alfabetik şifrelemenin tipik bir örneğidir.

Sezar döneminde kullanılan bu yöntemde harflerin yeri değiştirilir. Şifrelenecek metindeki harfler alfabede 3 harf kaydırılarak değiştirilir.



Sezar Şifresi : $c_i = E(p_i) = p_i + 3 \bmod 29$

Açık Mesaj : YARIN ONDAO KULDA BULUŞ ALIM

Şifreli Mesaj : BDTKP RÖGDR NYOGD EYOYÜ DOKÖ

Tablo Yöntemi

Bu yöntemin biraz daha gelişmiş olan tablo yönteminde ise alfabedeki her harf başka bir harfle yer değiştirir ama bu bir kurala bağlı olmadan karışık bir şekilde yapılır.

Mono Alfabetik Şifrelemenin Zayıflığı

Mono alfabetik şifreleme yöntemleri bilgisayar yardımıyla çok kısa sürede kırılabilir. Bu yöntemler kullanılan dildeki harflerin yerini değiştirir ama harflerin kullanım sıklığını (frekansını) değiştirmez.

Örneğin Türkçe'de en çok kullanılan harf olan "a" harfi tablo yöntemi kullanılarak "c" harfi ile yer değiştirilirse elde edilecek şifreli metinde en çok tekrar eden harfin "c" olduğu görülür ve bunun "a" harfi olabileceği tahmin edilerek şifre çözülmeye başlanabilir.

Vigenere tablosu

Bu tip şifrelemede, mono alfabetik yöntemlerden farklı olarak bir harf değiştirilince her seferinde aynı harfe dönüşmez. Bu yöntemlere güzel bir örnek Vigenere tablosudur.

Poli alfabetik şifreleme yöntemleri de bilgisayar yardımıyla ve frekans sayımı ile çok kolay ve çabuk çözülebilmektedir.

	0					5					10					15		
	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O
A	a	b	c	ç	d	e	f	g	ğ	h	ı	i	j	k	l	m	n	o
B	b	c	ç	d	e	f	g	ğ	h	ı	i	j	k	l	m	n	o	ö
C	c	ç	d	e	f	g	ğ	h	ı	i	j	k	l	m	n	o	ö	p
Ç	ç	d	e	f	g	ğ	h	ı	i	j	k	l	m	n	o	ö	p	r
D	d	e	f	g	ğ	h	ı	i	j	k	l	m	n	o	ö	p	r	s
E	e	f	g	ğ	h	ı	i	j	k	l	m	n	o	ö	p	r	s	ş
F	f	g	ğ	h	ı	i	j	k	l	m	n	o	ö	p	r	s	ş	t
G	g	ğ	h	ı	i	j	k	l	m	n	o	ö	p	r	s	ş	t	u
Ğ	ğ	h	ı	i	j	k	l	m	n	o	ö	p	r	s	ş	t	u	ü
H	h	ı	i	j	k	l	m	n	o	ö	p	r	s	ş	t	u	ü	v
I	ı	i	j	k	l	m	n	o	ö	p	r	s	ş	t	u	ü	v	y
İ	i	j	k	l	m	n	o	ö	p	r	s	ş	t	u	ü	v	y	z
J	j	k	l	m	n	o	ö	p	r	s	ş	t	u	ü	v	y	z	a
K	k	l	m	n	o	ö	p	r	s	ş	t	u	ü	v	y	z	a	b
L	l	m	n	o	ö	p	r	s	ş	t	u	ü	v	y	z	a	b	c
M	m	n	o	ö	p	r	s	ş	t	u	ü	v	y	z	a	b	c	ç

Vigenere tablosu

Bu yöntemde oluşturulan tablo ve bir anahtar kelime kullanılarak şifreleme yapılır.

Şifreleme

Açık Mesaj (sütun) : BULUŞ MAYER İANKA RA

Anahtar Kelime (satır) : KALEM KALEM KALEM KALEM...

Şifreli Mesaj : LUZAĞ ZAJIF UABÖM DA

Şifre Çözme

Şifreli Mesaj (tablo) : LUZAĞ ZAJIF UABÖM DA

Anahtar Kelime (satır) : KALEM KALEM KALEM KALEM...

Açık Mesaj (sütun) : BULUŞ MAYER İANKA RA

Tek Kullanımlık Karakter Dizisi (One-time Pad)

Bu basit şifreleme yönteminde rastgele üretilen bir karakter (harf veya rakam) dizisi kullanılarak şifreleme yapılır.

Açık mesaj içinde yer alan her karakter, üretilen dizide karşısına denk gelen karakterle işleme sokularak (Örneğin modüler toplama işlemi) şifreli mesaj elde edilir. Mesajı çözmek için rastgele dizinin bilinmesi gereklidir. Bu yöntem Vernam şifreleme yöntemi denir.

Açık Mesaj : BULUSMAYERİANKARA

Rastgele Dizi : DEFYPLCNMLJKHFGH

Şifreli Mesaj : RLDYDOY....

Bu yöntemin güvenliği rastgele üretilen diziye bağlıdır. Bu dizi gerçekten rastgele üretilmelidir, eğer bir kurala bağlı olarak üretilirse ve bu kural saldırgan tarafından bilinirse sistem kırılabilir. Bu tehdit dışında sistem mükemmel bir şifreleme sistemidir ve ilk olarak 1917'de bulunup "teletype" makinelerinde kullanılmıştır.

One-time pad algoritması ile şifreleme yapan örnek bir teletype cihazı.



Güvenli Şifreleme Yöntemleri

Simetrik Kriptografi nedir?

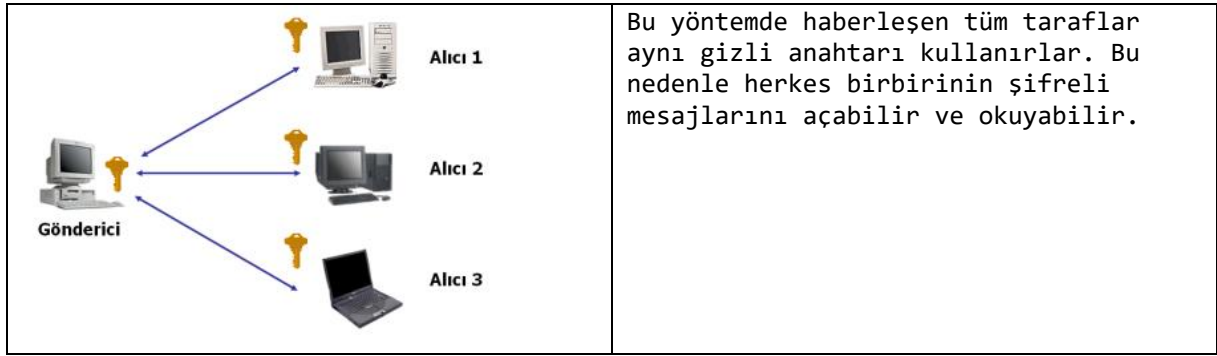
Simetrik şifrelemede, şifreleme ve şifre açma işlemi aynı anahtar ile yapılır. Simetrik kriptografide bu anahtar gizli tutulmalıdır. Bu nedenle, bu tip sistemlere gizli anahtarlı kriptografi sistemi adı da verilmektedir.

Bu sistemde haberleşen taraflar:

- Aynı şifreleme algoritmasını kullanırlar
- Birbirine uyumlu gerçeklemeler kullanırlar
- Aynı anahtarı kullanırlar

Anahtar Yönetimi

Birden-Çoğa (One-to-Many) Anahtar Yönetimi



Çoktan-Çoğa (Many-to-Many) Anahtar Yönetimi

	<table> <tr> <th>Kullanıcı Sayısı</th><th>Anahtar Sayısı</th></tr> <tr> <td>3</td><td>3</td></tr> <tr> <td>4</td><td>6</td></tr> <tr> <td>10</td><td>45</td></tr> <tr> <td>100</td><td>4,950</td></tr> <tr> <td>1,000</td><td>499,500</td></tr> <tr> <td>10,000</td><td>49,995,000</td></tr> <tr> <td>n</td><td>$n*(n-1) / 2$</td></tr> </table>	Kullanıcı Sayısı	Anahtar Sayısı	3	3	4	6	10	45	100	4,950	1,000	499,500	10,000	49,995,000	n	$n*(n-1) / 2$
Kullanıcı Sayısı	Anahtar Sayısı																
3	3																
4	6																
10	45																
100	4,950																
1,000	499,500																
10,000	49,995,000																
n	$n*(n-1) / 2$																

Simetrik Kriptografik yöntemleri

Blok Şifreleme Algoritmaları

Bu tip algoritmalar şifrelenecek veriyi sabit uzunlukta bloklar olarak şifreleme fonksiyonuna alırlar ve aynı uzunlukta şifrelenmiş veri blokları üretirler. Bu algoritmalara örnek olarak AES, DES, IDEA, Skipjack, RC5 vb. verilebilir. Bu algoritmalar aşağıdaki özellikleri gerçeklemeye çalışırlar:

Karıştırma: Anahtar ve şifrelenmiş mesaj arasındaki ilişki olabildiğince karışık olmalıdır.

Dağıtma: Tek bir açık mesaj karakterinin etkisi olabildiğince fazla şifrelenmiş karaktere yansıtılmalıdır.

Transpoze İşlemi: Şifrelemeye başlamadan önce açık mesajın içeriği değişik bir sıraya konur.

Yer Değiştirme İşlemi: Tekrar eden kalıplar başka kalıplarla değiştirilir.

Bit Katarı (dizi) Şifreleme Algoritmaları

Bu tip algoritmalar veriyi akan bir bit dizisi olarak alırlar. Vernam tipindeki bu algoritmalarda rastgele bit dizisi üretiminin kendini tekrarlamayan bir yapıda olması gereklidir. Örnek algoritmalar RC2, RC4 vb.

DES-Data Encryption Standart

DES algoritması bir Block Cipher algoritmasıdır. Yani şifrelenecek metin bloklar halinde şifreleme işleminden geçirilir.

Ayrıca DES algoritması simetrik şifreleme prensibine dayanmaktadır. Yani DES, veri bloklarını şifrelemek ve deşifrelemek için aynı anahtarları kullanmaktadır.

DES 64 Bitlik düz metin blokları üzerinde işlem yapmaktadır. 64 bitlik veri blokları, 56 bitlik bir anahtarın kontrolünde şifrlenerek yine 64 bitlik şifrelenmiş metin bloklarına dönüştürülür. Deşifrelenirken de 64 bitlik şifrelenmiş veri blokları, 56 bitlik bir anahtarın kontrolünde deşifrelenerek yine 64 bitlik deşifrelenmiş metinlere(düz metne) dönüştürülür.

DES de şifreleme ve deşifreleme için yer değiştirme, permütasyon gibi bir dizi işlem yürütülerek gerçekleştirilmektedir. Bu işlemlerin sırası şifreleme ve deşifreleme için birbirlerinin tam tersi şeklindedir. Şimdi DES algoritmasını basit olarak inceleyelim;

1. IP(Initial Permutation) şifreleme işleminde kullanılacak ilk permütasyondur. Verilen bir düz metin(x) üzerine ilk permütasyon uygulanarak x_0 elde edilir.

$x_0 \rightarrow IP(x)$

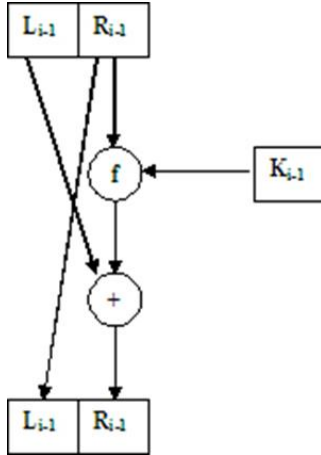
$L_0 = x'$ in ilk 32 biti

$R_0 = x'$ in son 32 biti

2. Ardından 16 defa tekrarlanan bir fonksiyonla yeni değerler hesaplanır. L_i R_i ($1 \leq i \leq 16$) aşağıdaki kurala göre hesaplanır:

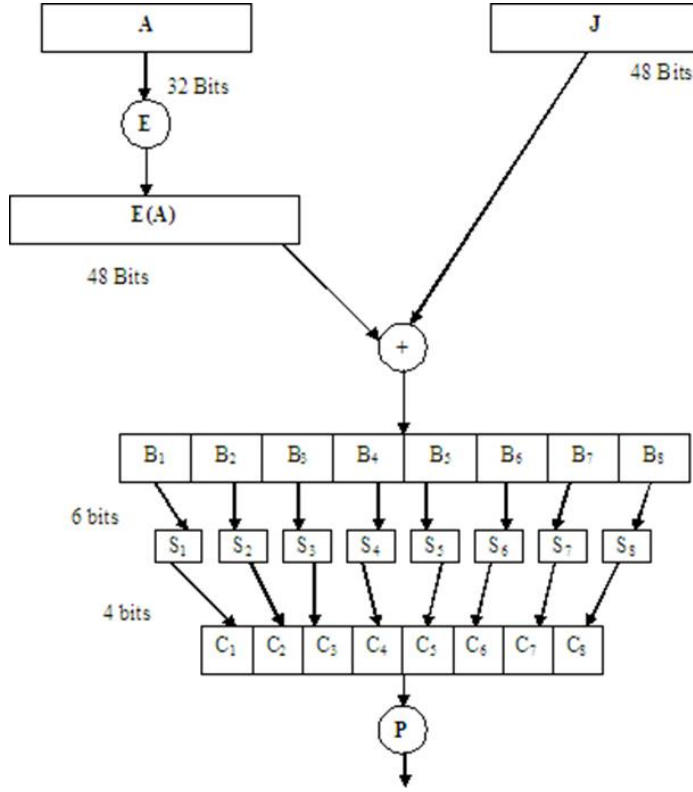
$L_i = R_{i-1}$

$R_i = L_{i-1} \text{ XOR } f(R_{i-1}, K_i)$



3. En son olarak da $R_{16}L_{16}$ ya IP^{-1} uygulanarak şifreli metin elde edilir.

f fonksiyonu iki parametre alır. Birincisi 32 bitlik bir bitstring(A), ikincisi de 48 bitlik bir bitstring(J). Sonuç olarak 32 bitlik bir bitstring oluşturulur.

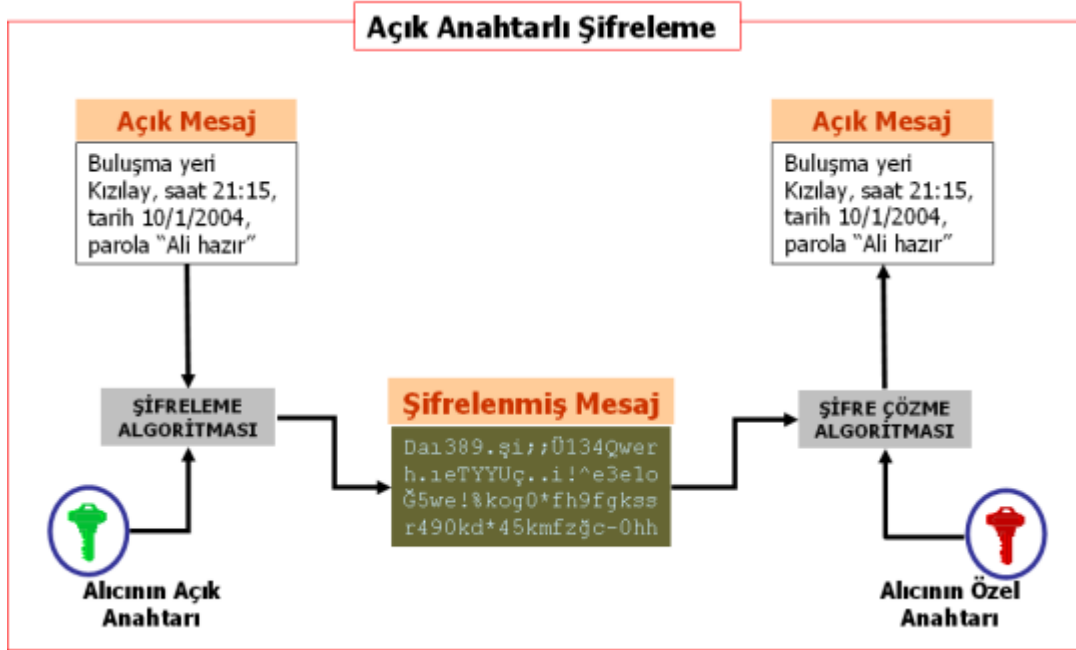


Asimetrik Kriptografi nedir?

Asimetrik kriptografide, şifreleme ve şifre çözme işlemi farklı anahtarlar ile yapılır. Bu anahtar çiftini oluşturan anahtarlara açık ve özel anahtar adı verilir. Bu kriptografi yönteminde özel anahtar gizli tutulmalıdır fakat açık anahtar gerekli kişilere verilebilir ve başka kişilerle paylaşılabilir. Bu özelliğinden dolayı asimetrik kriptografi, açık anahtarlı şifreleme adıyla da anılır.

Bu sistemi kullanarak haberleşen taraflar:

- Aynı şifreleme algoritmasını kullanırlar
- Birbiriyle uyumlu gerçeklemler kullanırlar
- Gerekli anahtarlara erişebilirler



Asimetrik kriptografi için anahtar yönetimi simetrik kriptografiye göre daha kolaydır çünkü bir kullanıcıyla şifreli haberleşmek isteyen kişi karşı tarafın açık anahtarına ihtiyaç duyar. Bu açık anahtar kamuya açık olarak yayınlandığı için sisteme giren bir kişi için sadece bir anahtar çifti üretmek yeterli olmaktadır.

Kullanıcı Sayısı	Anahtar Çifti Sayısı
3	3
10	10
100	100
1,000	1,000
10,000	10,000
n	n

Asimetrik Kriptografik yöntemleri

Başlıca asimetrik kriptografi algoritmaları

- RSA
- Eliptik Eğri Sistemleri
- El Gamal
- Diffie-Hellman

olarak sıralanabilir. Asimetrik kriptografi algoritmaları, simetrik algoritmalarından farklı olarak çözülmesi zor olan matematiksel problemlere dayanmasıdır.

RSA Algoritması

En yaygın olarak kullanılan asimetrik algoritmadır. R. Rivest, A. Shamir, L. Adleman tarafından 1977 yılında bulunmuş ve 1978 yılında yayınlanmıştır. Adını mucitlerinin isimlerinin ilk harflerinden almıştır.

- Açık anahtar kriptografik sistemi ve sayısal imzalama yöntemi olarak kullanılır.
- Çarpanlarına ayırma problemi üzerine inşa edilmiştir.
- Bileşik tam sayı olan n 'i oluşturan, asal sayılar p ve q bulunur, öyleki $n=pq$ 'dir.
- Yeterince büyük bir n için kırılması çok zordur.
- Ayrıca kök bulma problemine de dayanır.
- Çok güvenlidir fakat fazla hızlı değildir.

Algoritmanın kullandığı parametreler

Açık anahtar: n, e

Özel anahtar: d

n bileşik bir tamsayıdır ("modulus")

e bir tamsayıdır ("açık üs ifadesi")

d bir tamsayıdır ("gizli üs ifadesi")

bu parametrelerle:

$$ed \equiv 1 \pmod{(p-1)(q-1)}$$

ve p, q sayıları n 'nin asal çarpanlarıdır.

Algoritmanın kullanımı

Ayşe, Bora'ya m mesajını şifreli göndermek için:

m 'nin e 'inci üssünü alır, yani m 'yi Bora'nın açık anahtarı ile şifreler:

$$c = m^e \bmod n$$

c ("şifreli mesajı")'yi Bora'ya gönderir

Bora c sayısının d 'nci üssünü alır, yani c 'nin şifresini kendi özel anahtarını kullanarak çözer:

$$m = c^d \bmod n$$

Algoritmanın Kriptoanalizi

- Şifreleyenin işi kolaydır, sadece iki tane modüler çarpma işlemi yapar.
- Şifre açanın işi kolaydır, $1.5 \log n$ tane modüler çarpma yapar.
- Eğer asal sayılar p, q bilinirse işlem daha hızlı yapılabilir.
- Düşmanın işi zordur çünkü kök bulma ya da çarpanlarına ayırma problemini çözmelidir.
- Etkili bir çözümü bulunmamıştır.
- Modulus n sayısı arttıkça algoritmanın güvenliği artar.

Kripto Sistemlerini Karşılaştırılması

Simetrik kriptografinin kuvvetli yönleri:

Algoritmalar hızlıdır

Algoritmaların donanımla gerçekleştirilmesi kolaydır

"Gizlilik" güvenlik hizmetini yerine getirir

Simetrik kriptografinin zayıf yönleri:

Ölçeklenebilir değil

Emniyetli anahtar dağıtımı zor

"Bütünlük" ve "Kimlik Doğrulama" güvenlik hizmetlerini gerçekleştirmek zor

Asimetrik kriptografinin kuvvetli yönleri:

Anahtar yönetimi ölçeklenebilir

Kripto-analize karşı dirençli (Kırılması zor)

Bütünlük, kimlik doğrulama ve inkâr edememezlik güvenlik hizmetleri sağlanabilir.

Asimetrik kriptografinin zayıf yönleri:

Algoritmalar genel olarak yavaş çalışırlar. Simetrik kriptografi algoritmalarına göre yaklaşık 1500 kat daha yavaştır.

Anahtar uzunluğu bazı durumlar için kullanışlı değildir. Mobil cihazlar için klasik algoritma anahtar uzunlukları sorunlu olabilir.

Konu	Simetrik Kriptografi	Asimetrik Kriptografi
Gizlilik	Sağlar	Sağlar
Bütünlük	--	Sağlar
Kimlik doğrulama	--	Sağlar
İnkâr Edememezlik	--	Sağlar
Performans	Hızlı	Yavaş
Güvenlik	Anahtar uzunluğuna bağlı	Anahtar uzunluğuna bağlı