

Bil 663

CIA Triad

Protection of Data and Systems

Bilgi Güvenliğinin üç ölçütleri → Sifreleme / Erisim Kontrolü / Saldirı Tespit

Mesajın
istediği
cevap
şekli

Sifreleme bilgilerin gizliliğinin ve bütünlüğünün sağlanması amacıyla
korunmasıdır

Erisim Kontrolü

Saldirı Tespitİ ve Önleme Stratejileri (IDS/IPS)

Non Chalant

Bilgi Güvenliğinin Önemi:

Bilgi Güvenliği Uygulamaları ve Sağlama Yöntemleri:

Tekrar edilen
kısım

Bilgi Güvenliği: Bilginin korunması için uygulamalı önlemler
dizisidir.

Bilginin gizliliğini bütünlüğünü ve erişilebilirliğini sağlama sürecidir.

CIA Triad → Gizlilik / Bütünlük / Erişebilirlik

↳ Bütünlük sağlanması
güvenlik olarak dirençli hale getirir.
↓
Dijital imzalar
↓
Yedekleme Sistemleri

Doğrulama Yöntemleri (Örnek)

Yetkilendirme → Banka çalışanının sade kendi departmanına erişmesi;

Sorumluluk ve izlenebilirlik.

Risk Yönetimi → Uygun güvenlik önlemlerinin alınma sürecidir.

Veri ve sistemlerin korunması → Hem Fiziksel hem Digital olarak korunması
Hastane Örneği:

Yasal Düzenlegici Uyumluluk → KVK

2. hafta
Cesar Sifreleme, Afi → (Simetrik şifrelemeye gider)

Plaintext

Chiper test

Key

Encryption

Decryption

Simetrik Sifreleme (Aynı anahtar?) ibilitaraf

DES bluefish twofish

Anahtar Yönetimi

Asimetrik Sifreleme

RSA ECC ECA

Faik anahtar
özel anahtar

Avantaj / Dezavantaj

Aşırı Sifreleme

Simetrik Sifreleme : Veriyi şifrelerek ve gizlemek için kullanılır
Sifreyi çözmek için

Asimetrik : Anahtarları dağıtmak ve paylaşmak için

Desavantajı : Hesaplama maliyeti (İstemci)
Karmaşıklık

Anahtar üretimi ve Sifreleme . Sifre Gözme

(Fikri)

$p = 61$, $q = 53$ message: MUHENDISLIK
 $m = 11$

$$n = p \times q = 3233$$

$$\phi(n) = (p-1) \times (q-1) = 60 \times 52 = 3120$$

$$c = 11^3 \bmod 3233 = 1331 \bmod 3233$$

$$= 1331 //$$

$$\begin{array}{l} p = 61 \quad q = 53 \\ n = p \times q = 3233 \\ \phi(n) = (p-1)(q-1) = 3120 \end{array}$$

$$n = 61 \times 53 = 3233$$

$$\phi(n) = (61-1)(53-1) = 3120$$

$$\gcd(e, \phi(n))$$

$\hookrightarrow e = 3$ kullanılır.

$$c = 3^3 \bmod 3233 = 27 \bmod 3233$$

RSA

iki asal sayı p ve q

2) $n = p \times q$ $m = \text{Mesajdaki harf sayısı, (?)}$

3) $\phi(n) = (p-1) \times (q-1)$

4) $e > 1$: bul

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

ECC (Eliptik Eğri Kar...)

Anahtar uzunluğu: 256 bit ve üzeri

Mobil cihazlar, gövde ve taranıcıları

Eliptik eğri seçimi

Öldü: Anahtar seçimi $> G$ noktası seçilir ve hesaplanmadan kullanılabilecektir.
Aralık anahtar hesaplaması başlangıç noktasıdır.

DSA Digital Signature Algorithm

Anahtar uzunluğu: 1024

Dijital uygulama, doğrulama

Anahtar içimi:

- Aşamalar: özel anahtarlar, rastgele seçim, ortak anahtarlar, imza oluşturma, imza doğrulama.

RSA örneği

$$p = 5, q = 11 \quad \text{KUTUP} \quad m = 5$$

$$n = p \times q = 5 \times 11 = 55$$

$$\phi(n) = (p-1) \times (q-1) = (5-1) \times (11-1) = 40$$

$$\begin{array}{l} c = m^e \bmod n \quad e = 3 \text{ kullanılır} \\ 5^3 \bmod 55 \\ 125 \bmod 55 = 15 \end{array}$$

RSA Sifreleme Çözümü:

$$\gcd(e, \phi(n))$$

Aralarında asal iki sayı p, q

$$n = p \times q$$

$m = \text{Mesajdaki harf sayısı}$

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

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

örnek: MUHENDISLIK

$$p = 61, q = 53$$

$$m = 11$$

$$n = p \times q = 61 \times 53 = 3233$$

$$\phi(n) = (61-1)(53-1) = 60 \times 52 = 3120$$

$$\gcd(e, \phi(n)) = \gcd(3, 3120) = 1 \text{ uygun}$$

$e = 3$

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

$$11^3 \bmod 3233$$

$$1331 \bmod 3233$$

$$= 1331 //$$

Örneğ: $p=11, q=17$ D^EFTER

$$n = p \times q = 11 \times 17 = 187$$

$$\varphi(n) = (p-1) \times (q-1) = (11-1) \times (17-1) = 10 \cdot 16 = 160$$

$$\gcd(e, \varphi(n)) = \gcd(3, 160) = 1 \text{ uygun}$$

$$e=3$$

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

$$m=6$$

$$\begin{array}{r} 36 \\ - 187 \\ \hline 216 \end{array}$$

$$\begin{array}{r} 216 \\ - 187 \\ \hline 29 \end{array}$$

$$6^3 \bmod 187 = 216 \bmod 187 = 29$$

Örneğ: $p=5, q=11$ KUTUP

$$m=5$$

$$n = p \times q$$

$$5 \times 11 = n = 55$$

$$\varphi(n) = (5-1) \times (11-1) = 4 \times 10 = 40 = \varphi(n)$$

$$\gcd(e, \varphi(n)) = \gcd(3, 40) = 1 \text{ uygundur}$$

$$e=3$$

$$c: m^e \bmod n \rightarrow 5^3 \bmod 55 = 125 \bmod 55 = 15$$

→ Sifreleme sistemlerinde Uygulama Adımları.

1 * Anahtar Üretimi

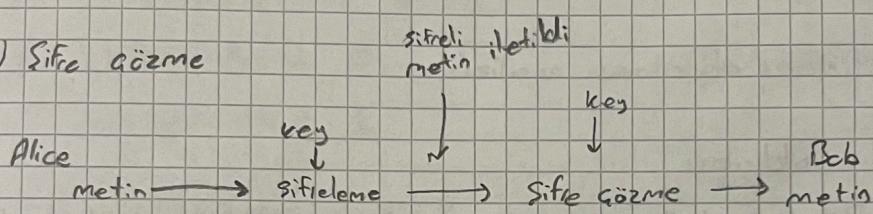
Simetrik tek anahtar

2 * Sifreleme (Encryption)

Asimetrik

3 Anahtar Dağıtımlı

4) Sifre Gözme



1) Kablosuz Saldırısı.

Olası tüm paroları föz dener -----

Örnek 8 bit bir anahtar için 256 kombinasyon denebilir

2) Sözlük Saldırısı.

İşte) Yüzbin olarak kullanılan paroların listesi ile hash değerlerini karşılaştırır.

3) Bilinen Diz metin saldırısı. (enigma'da kullandıklar

Sifreleme

4) Sembol Pazar metin saldırısı.

Sifreleme yapısının zayıflıklarını belirler

RSA sifreleme yöntemine yönelik saldırılardır.

5) Sıfırı Sıfırı Metin Saldırısı

Satırının seçtiği sıfırı metinden düz metine çevirmesi

örn RSA, OAEP

6) Diferansiyel Kripto Analiz

Sıfırlama algoritmasındaki kütüphane deşifreleri metindeki etkilerini inceler

örn DES sıfırlama algoritması analizi

7) Yarı Karal Saldırıları

Fiziksel Bilgileri kullanarak şifre gözmeye yetenik saldıruları
örn Güç yönetimi analizi

8) İstatistiksel Analiz

Vigenere şifrelenmesinin frekans analizi

10) Zayıf Anahtar Saldırıları

En zayıf anahtarı bulur.

DES algoritmasındaki zayıf anahtarlar.

the üçüncü yana en zayıf

the 2'se " "

$e \rightarrow$ kaçıncı (frekans analizi)

$t \rightarrow$ "

$c \rightarrow$ "

Xre

exC

abedc eFg h i j k m n o p q r s t u v w x y z

Sezar Sifrelemesi

fsfo gwdj

bseb ewhe ewhe

- a) klohexy 1 en zayıf
 b) eee kxz 2
 c) eebyw f 4
 d) cphilno 5 en zor
 e) eezy w~~c~~ 3

permelin en kolay çözülebilir oburlar

- a) k x b + k x b y z b 3
 b) + tabackeln 4
 c) bababa baba 2
 d) xxxxxxxx - 1

Owctskweldmxjzr

gagtsrweldmxjer

$\sum f_{\text{freq}}$

$k=3$ dosfin

K0KXASSEH2D6XJZRW

ilovemydewartsmens

ed

I LOVE MY DEPARTMENT

Bilinmesi ~~tezin~~
 Kriptografi ~~tez~~ nedir? Verilerin gizliliğini ve bütünlüğünü ve doğrulamasını saglamak amacıyla verileri sifreleme ve çözme teknikleri bilinir.

Sifreleme nedir? Verilerin güvenliği için belirli algoritmalarla anlaşılmaz formata dönüşür.

Diz metin uygulaması örneği metini olduğu gibi göndermek hello → hello

// Hibrit sistemler iki yöntemin avantajlarını birleştirerek daha esnek ve güvenli bir sifreleme çözümü sunar //

// Kriptografi sifreleme algoritmalarının zayıflıkları tespit edip bunları sifre kırmak için kullanır //

Simetrik Sifreleme ve Çözme için aynı anahtarı kullanır.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	

Simetrik Asimetrik Farkı "C = (P + k) mod n" Sezar Sifreleme formülü

HELLO

7 4 11 11 14

6 1 11 1

11 8 15 15 18

5 1 11 1

L I P P S

"C = (P + k) mod n" DESifreleme

A b c d e f g h i j k l m n o p q r s t u v

w x y z

Sezar
Sifreleme

C = (P + k) mod n

harf numarası
Atlamalı
Değeri

Sezar
Desifreleme

C = (P - k) mod n

26 Alfabe
harf sayısı

Affine Sifreleme

$$E(x) = (ax + b) \bmod n$$

$$\text{deşifreleme } D(x) = a^{-1}(x - b) \bmod n$$

Affine Sifreleme

$\gcd(a, n)$ asallık

" $E(x) = (ax + b) \bmod n$ " ~~Sifreleme~~

$$D(x) = a^{-1}(x - b) \bmod n \quad \text{DÜ sifreleme}$$

$\gcd(a, n)$ asallık

~~örnek~~

$$\text{Key} = 4x + 3 \quad \text{Yani: } a = 4, b = 3$$

Affine - ?

$$w \rightarrow 4(22) + 3 \bmod 26$$

(WORLD)

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
a b c d e f g h i j k l m n o p q r s t u v w x y z

örnek:

$$\text{HELLO } a = 5, b = 8, n = 26$$

$$H = 7 \rightarrow (5 \cdot 7 + 8) \bmod 26$$

$$= 43 \bmod 26 = 17 = F$$

$$E(x) = (ax + b) \bmod n$$

$$E = G \rightarrow (5 \cdot 4 + 8) \bmod 26 = 2 = C$$

HELLO
rclla

$$L = 13 \rightarrow (5 \cdot 13 + 8) \bmod 26 =$$

$$63 \bmod 26 = 11 = L$$

$$O = 14 \rightarrow (5 \cdot 14 + 8) \bmod 26$$

$$78 \bmod 26 = 0 = O$$

desifreleme

$$D(x) = a^{-1}(x - b) \bmod n$$

$$D(x) = a^{-1}(x-b) \bmod 26$$

Hello

$$a=5, b=8$$

$$a^{-1} \cdot a \equiv 1 \pmod{n}$$

$c \parallel a$

$$a^{-1}(x-b) \bmod 26$$

$$\hookrightarrow 17 \rightarrow 21 (17-8) \bmod 26 = 21 \cdot 9 \bmod 26 = 7 \text{ H}$$

$$\begin{aligned} a^{-1} &= 21 \\ b &= 8 \end{aligned}$$

$$\begin{array}{r} 189 \mid 26 \\ -182 \\ \hline 7 \end{array}$$

$$c=2 \rightarrow 21 (2-8) \bmod 26 = 21 (-6) \bmod 26$$

$$= 21 \cdot 20 \bmod 26 = 420 \bmod 26 = 4 = e$$

$$l=11 \rightarrow 21 (11-8) \bmod 26 = 21 \cdot 3 \bmod 26$$

$$= 63 \bmod 26 = 11 = l$$

$$A=0 \rightarrow 21 (0-8) \bmod 26$$

$$21 \cdot 18 \bmod 26 = 14 = 0$$

$$\begin{array}{r} 21 \\ \times 18 \\ \hline 168 \\ 21 \\ \hline 378 \\ -26 \\ \hline 118 \\ -104 \\ \hline 14 = \end{array}$$