



# Data Security

1. Concepts
2. Secret key methods
3. Public key methods
4. Protocols I.
5. Protocols II.



# Data Security: Concepts

1. Access control
2. Encryption
3. Identification
4. Integrity protection
5. Key management



# Data Security: Access Control

A Rossz talált egy bankkártyát, s szeretné a pénzt megszerezni. Tudja, hogy egy terminál  $K=3$  sikertelen PIN kísérlet után bevonja a kártyát.

$\text{PIN} \in \{1, \dots, 9999\}$ . Azonban hálózati problémák miatt 10 óra hosszat a 80 terminál off-line üzemel. Negyedóra kell, hogy a Rossz egyik termináltól a másikig érjen (beleértve a PIN próbálkozást).

Sikeres-e a Rossz?

(Sikeres, ha PIN megszerzésének valószínűsége a 0.01 értéket meghaladja)



# Data Security: Access control

Óvatos és csak 2 próbát végez.

Minden új próbálkozásnál új kombinációt próbál ki.

Összes kipróbálható kombináció =  $10 \cdot 4 \cdot 2 = 80$ .

$1 - P = (9999 - 80) / 9999 \rightarrow P \approx 0.008 < 0.01$

(A legutolsó terminálnál egy 3. próbálkozás is tehető, hiszen mivel úgysem teszünk további próbálkozásokat, nem számít, ha a terminál bevonja a kártyát.)



# Data Security: Access control

1.rendszer:

Egy bankkártya alkalmazásban 4 decimális karakter hosszú PIN kódot alkalmaznak.

A terminál egy karakter leütése után azonnal ellenőrzi azt.

A 4 karakterből összesen 1 egy karaktert téveszthet a támadó, s azt is csak egy alkalommal, utána bevonja a kártyát.

2.rendszer:

2 decimális karakter hosszú PIN kódot alkalmaz, és a PIN kód mindkét karaktere beadaása után ellenőríz és három egymás utáni hibás PIN-próbálkozás esetén nyeli el a kártyát.

Melyik a biztonságosabb rendszer?



# Data Security: Encryption

## Simple ciphers

$m$ : nyílt szöveg ( $m$  in  $M$ )

$c$ : rejtett szöveg ( $c$  in  $C$ )

$k$ : kulcs ( $k$  in  $K$ )

rejtjelező kódolás:

$$E_{k_1}(m) = c$$

rejtjelező dekódolás:

$$D_{k_2}(c) = m$$

$$D_{k_2}(E_{k_1}(m)) = m$$

szimmetrikus kulcs:  $k_1 = k_2$

aszimmetrikus kulcs:  $k_1 \neq k_2$

$(m \leftrightarrow x, c \leftrightarrow y)$



# Data Security: Encryption

## Simple ciphers

Betűnkénti lineáris rejtjelező

$M = \{26 \text{ betűs angol abc}\} = \{abcde fghij klmno pqrst uvwxy z\}$

$C = M$

$k = [a, b] \in M \times M$

$$c = a * m + b \text{ mod } 26$$

a) Adjuk meg a dekódoló transzformációt!

b) Sikerült két nyílt szöveg rejtett szöveg párt megismerni:

$m_1=4, c_1=14; m_2=10, c_2=10.$

Határozzuk meg a kulcsot!



# Data Security: Encryption

## Simple ciphers

a)  $m = (c - b) \cdot a^{-1}$ ,  $\text{Inko}(a, 26) = 1$

b)  $14 = 4a + b \pmod{26}$   
 $10 = 10a + b \pmod{26}$

$\rightarrow 6a = 22 \pmod{26} \rightarrow 3a = 11 \pmod{13} \rightarrow a = 8 \pmod{13}$

$\rightarrow a = 21 \pmod{26} \rightarrow b = 8 \pmod{26}$

$a = 21, b = 8$

# Data Security: Encryption

## Simple ciphers

$c=mk$  (Hill rejtjelező)

$m = \text{fr id ay}$

$c = \text{PQ CF KU}$

$\text{fr} \rightarrow \text{PQ} : \quad \text{Ek}(5,17)=(15,16)$

$\text{id} \rightarrow \text{CF} : \quad \text{Ek}(8,3)=(2,5)$

$\text{ay} \rightarrow \text{KU} : \quad \text{Ek}(0,24)=(10,20)$

$$\begin{pmatrix} 15 & 16 \\ 2 & 5 \end{pmatrix} = \begin{pmatrix} 5 & 17 \\ 8 & 3 \end{pmatrix} \begin{pmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{pmatrix} \rightarrow \begin{pmatrix} 5 & 17 \\ 8 & 3 \end{pmatrix}^{-1} = \begin{pmatrix} 9 & 1 \\ 2 & 15 \end{pmatrix} \rightarrow K = \begin{pmatrix} 9 & 1 \\ 2 & 15 \end{pmatrix} \begin{pmatrix} 15 & 16 \\ 2 & 5 \end{pmatrix} = \begin{pmatrix} 7 & 19 \\ 8 & 3 \end{pmatrix}$$



# Data Security: Encryption

## Simple ciphers

### Lineáris blokk rejtjelező

Tegyük fel, hogy  $y = Ax + b$  lineáris transzformációval rejtjelezünk, ahol  $A$   $n \times n$ -es bináris mátrix,  $x, y, b$   $n$  hosszú bináris (oszlop)vektorok, továbbá  $A$  és  $b$  a kulcs részei,  $x$  a nyílt szöveg,  $y$  a rejtett szöveg.

A támadó célja a kulcselemek meghatározása.

A támadás  $(x_0, y_0), (x_1, y_1) \dots$  ismert nyílt-rejtett szöveg párok alapján történik.

- a.) Adja meg a támadás algoritmusát!
- b.) Korlátozhatjuk-e a támadás sikerét azzal, hogy maximáljuk egy kulcs felhasználásának számát?

# Data Security: Encryption

## Simple ciphers

$$y = Ax + b$$

$$K = [A, b]$$

A :  $N \times N$  méretű, invertálható bináris mátrix

b :  $N$  méretű bináris vektor

ismert nyílt szövegű támadás:  $Q = \{(x_0, y_0), (x_1, y_1), \dots, (x_N, y_N)\}$

$$y_1 - y_0 = A(x_1 - x_0)$$

$$y_2 - y_0 = A(x_2 - x_0)$$

...

→

$$Y = AX$$

$$X = (x_1 - x_0, x_2 - x_0, \dots, x_N - x_0) \rightarrow A = YX^{-1}, \text{ ha } \exists X^{-1}$$

$$Y = (y_1 - y_0, y_2 - y_0, \dots, y_N - y_0)$$

$$y_N - y_0 = A(x_N - x_0)$$

# Data Security: Encryption

## Statistical analysis

$$E_k(x) = ax + b \pmod{26}$$

*Letter probability distribution in English texts*

letter	prob.	letter	prob.
A	.082	N	.067
B	.015	O	.075
C	.028	P	.019
D	.043	Q	.001
E	<b>.127</b>	R	.060
F	.022	S	.063
G	.020	<b>T</b>	<b>.091</b>
H	.061	U	.028
I	.070	V	.010
J	.002	W	.023
K	.008	X	.001
L	.040	Y	.020
M	.024	Z	.001

*Letter frequency in ciphertext y*

letter	freq.	letter	freq.
A	2	N	1
B	1	O	1
C	0	P	2
D	7	Q	0
E	5	R	8
F	4	S	3
G	0	T	0
H	5	U	2
I	0	V	4
J	0	W	0
K	5	X	2
L	2	Y	1
M	2	Z	0

FMXVEDKAPHFERBNDKRXRSREFMORUDSDKDVSHVUF  
EDKAPRKDLYEVLRRHRH

# Data Security: Encryption

## Statistical analysis

The most frequent letters: R(8); D(7); E,H,K(5); F,V(4)

*guess 1:* R → e, D → t

$$E_k(4)=17 \quad 1. 4a+b=17 \pmod{26}$$

$$\rightarrow \rightarrow a=6, b=19 \quad (2.-1.: 15a=-14=12, 15-1=7, a=7 \cdot 12=6 \pmod{26})$$

$$E_k(19)=3 \quad 2. 19a+b=3 \pmod{26}$$

→  $\gcd(a,26)=2 > 1$  incorrect guess

*guess 2:* R → e, E → t

→ a=13 incorrect

*guess 3:* R → e, H → t

→ a=8 incorrect

*guess 4:* R → e, K → t

→ a=3, b=5 legal key

*decryption trial* (check if we get meaningful decrypted text):  $D_k(y)=3^{-1}(y-5)=9y-19 \pmod{26}$

algorithms are quite general definitions of arithmetic processes

algorithms are quite general definitions of arithmetic processes



# Data Security: Encryption

## One Time Pad

x = 01001101 01011101 ...

k = 11010000 11101011 ...

-----

y = 10011101 10110110 ...

$y = x + k$  ,  $x = y - k = y + k = (x + k) + k = x + (k + k) = x$  , + : mod 2 addition (XOR)

x= ONETIMEPAD

k= TBFrgFARFM

-----

y= IPKLPSFHGQ

$O + T \text{ mod } 26 = I$  ,  $N + B \text{ mod } 26 = P$  ,  $E + F \text{ mod } 26 = K$  . . .



# Data Security: Encryption

## One Time Pad

### Probabilistic model (C. Shannon)

X, Y, K random variable

K has uniform distribution (coin flipping sequence)

X and K are independent

**Perfect encryption:**  $I(X,Y)=0$ .

**Theorem:** Perfect encryption exists.

Proof: One time pad

$$Y=X+K \quad (+ = \oplus)$$

$$P(Y=y|X=x) = P(X+K=y|X=x) = P(K=y-x|X=x) = P(K=y-x) = 2^{-N}$$

(X and K are independent)

$$P(Y=y) = \sum_x P(X+K=y|X=x)P(X=x) = 2^{-N} = P(Y=y|X=x) \blacklozenge$$



# Data Security: Encryption

## One Time Pad

A nyílt szövegek, a rejtett szövegek halmaza, illetve a kulcsok halmaza rendre  $\{A,B\}$ ,  $\{a,b,c\}$ , illetve  $\{1,2,3,4\}$ . A kulcsokat egyenletesen véletlenül sorsoljuk. A kódolás az alábbi táblázat szerinti:

k	$E_k(A)$	$E_k(B)$
1	a	c
2	c	b
3	c	a
4	b	c

A nyílt szöveg tetszőleges, rögzített bináris eloszlással sorsolt.

Tökéletes-e a rejtjelezés?



# Data Security: Encryption

## One Time Pad

k	$E_k(A)$	$E_k(B)$
1	a	c
2	c	b
3	c	a
4	b	c

Igen.

A rejtett szöveg v.v. független a nyílt szöveg v.v.-tól.

- $P(y=a \mid x=A) = P(y=a \mid x=B) = 1/4$
- $P(y=c \mid x=A) = P(y=c \mid x=B) = 1/4$
- $P(y=b \mid x=A) = P(y=b \mid x=B) = 1/2$



# Data Security: Encryption

## One Time Pad

$M = \{e, f\}$  ,  $P(e)=1/4$  ,  $P(f)=3/4$

$K = \{k1, k2, k3\}$  ,  $P(k1)=1/2$  ,  $P(k2)=1/4$  ,  $P(k3)=1/4$

$C = \{1, 2, 3, 4\}$

	e	f
k1	1	2
k2	2	3
k3	3	4

- a.) Mekkora annak valószínűsége, hogy a 3 rejtett szöveg kerül továbbításra?
- b.) A lehallgatott rejtett szöveg 3. Mekkora annak valószínűsége, hogy e volt a nyílt szöveg?
- c.) Tökéletes-e a rejtjelező?

# Data Security: Encryption

## One Time Pad

	e	f	$M = \{e, f\}, P(e)=1/4, P(f)=3/4$
k1	1	2	$K = \{k1, k2, k3\}, P(k1)=1/2, P(k2)=1/4,$
k2	2	3	$P(k3)=1/4$
k3	3	4	$C = \{1, 2, 3, 4\}$

a.)  $P(3) = 1/4$  :  $P(3) = P(3|e)P(e) + P(3|f)P(f)$   
 $= P(k3)P(e) + P(k2)P(f)$   
 $= 1/16 + 3/16 = 1/4$

b.)  $P(e | 3) = 1/4$  ( $= P(3 | e)P(e) / P(3) = P(k3)P(e) / P(3) = 1/4 \times 1/4 / (1/4) = 1/4$ )

c.) Nem. Pl. b.) szerint  $P(f | 3) = 3/4$ , tehát a 3 rejtett szöveg esetén valószínűbb, hogy f volt a nyílt szöveg.



# Data Security: Kriptoprotokoll

Shamir háromlépéses protokollja:

Titok rejtett továbbítása előzetes kulcsmegegyezés nélkül?

A, B felhasználók  
x üzenet

feltétel:

1. kommutatív tulajdonságú rejtjelezés  $EB(EA(x)) = EA(EB(x))$
2. lehallgató típusú támadó

1.  $A \rightarrow B$ :  $y_1 = EA(x)$
2.  $B \rightarrow A$ :  $y_2 = EB(EA(x)) (= EA(EB(x)))$
3.  $A \rightarrow B$ :  $y_3 = DA(y_2) = EB(x)$



# Data Security: Kriptoprotokoll

## Integrity protection

$m$  számú blokkból álló üzenetünket rejtjelezve és integritásvédelemmel szeretnénk továbbítani. Integritásvédelemül a következő módszert választjuk:

Az  $m$  darab üzenetblokkot mod 2 összegezzük, s így egy ellenőrző összeg blokkot nyerünk (azaz az ellenőrző összeg blokk  $i$ -edik bitje az üzenetblokkok  $i$ -edik bitjeinek a mod 2 összege). Ezután az  $m+1$  darab blokkot blokkonként ECB módban rejtjelezzük.

Támadható a megoldás?

És ha CRC-t alkalmazunk az üzenetblokkok fenti összegzése helyett?



# Data Security: Kriptoprotokoll

## Integrity protection

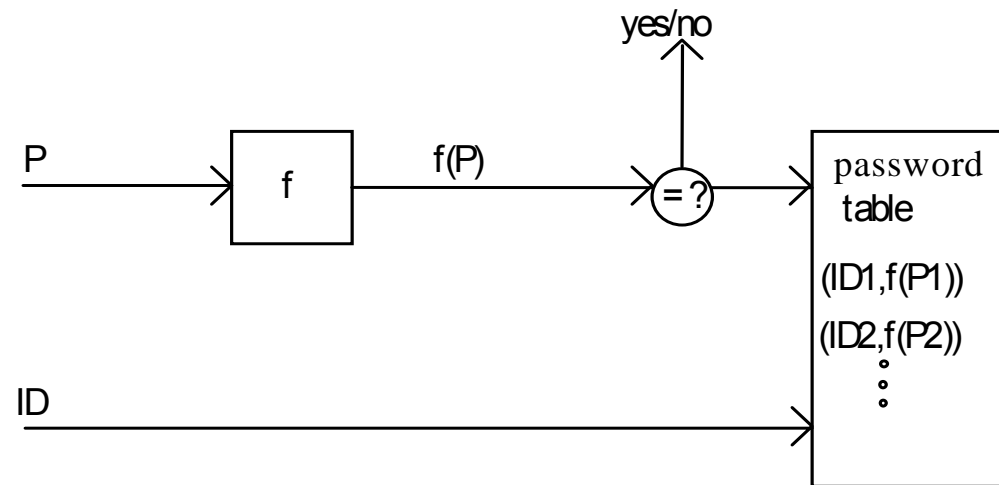
Egy cég informatikai központja szoftverek egy-egy példányát szétosztja távoli egységei informatikai részlegeinek. Szeretné a fájlok sértetlenségét biztosítani, s alkalmanként (például hetente) szeretné ellenőrizni azok helyességét, amely feladat megoldásához azonban nem kíván titkos kulcshoz kapcsolódó eljárásokat alkalmazni, például azért, mert a korrekt kulcsgondozás költséges feladat, s erre nem kíván erőforrásokat lekötöni. Lehetséges-e megoldás ilyen feltételek mellett?

Készítsünk “biztonságos lenyomatot” a fájlról, hexadecimális ábrázolásban, s a fájl pl. email-ben történő elküldése után telefonon olvassuk fel a hexa sorozat néhány tagját a központban ülő ellenőrző személy számára.

“biztonságos lenyomatot” megvalósítása: kriptográfiai hash függvény

# Data Security: Kriptoprotokoll

## Identification





# Data Security: Kriptoprotokoll

## Key management

The level of security in a system using cryptography cannot be higher than the security of its key management.

Basic tasks of key management:  
key-

- generation
- storage
- distribution (exchange, agreement)
- updating (freshing)
- revoking



# Data Security: Kriptoprotokoll

## Key management

Egy kriptorendszer kulcshossza 100 bit. A kulcsot olyan generátorból nyerjük, amely 5 bites blokkokat állít elő. Ezen blokkokból azonos valószínűséggel olyanokat generál, amelyekben az 1 bitek darabszáma mindig kevesebb, mint a 0 bitek darabszáma. Az egymás utáni blokkok függetlenek. 20 db blokkot használunk kulcsként.

- a.) Mennyi a tényleges kulcshossz, azaz mennyi az így generált kulcs entrópiája?
- b.) Lehetséges-e, hogy 100 bit entrópiájú kulcsot állítsunk előállítani az adott generátorra támaszkodva?

# Data Security: Kriptoprotokoll

## Key management

a.)

<u>blokkfajta:</u>	<u>db</u>
3db 1bit    2db 0 bit	→ 10
4db 1bit    1db 0 bit	→ 5
5db 1bit    0db 0 bit	→ 1

Összesen: 16 –féle blokk →  $\log_2 16 = 4$  bit /blokk →  
 $100/5 \cdot 4 = 80$  bit

b.) A 16 lehetséges blokkot egyértelműen leképezzük a 0000,.....,1111 16 db féljbájt egykébe. 25 db blokkot ilyen módon leképezve 100 db pénzfeldobás bitet kapunk.



# Data Security: Kriptoprotokoll

## Digital signature

Internetes verseny feladat megoldását ( $x$ ) rejtjelezve és a küldő fél aláírásával hitelesítve kell beküldeni. Mi tervezzük az algoritmust, melyiket válasszuk az alábbiak közül?

a.)  $A \rightarrow B: E_B(D_A(X))$

b.)  $A \rightarrow B: D_A(E_B(X))$

ahol publikus kulcsú technológiát (pl. RSA) alkalmazunk.

Melyik megoldást válasszuk?

(Feltehetjük, hogy  $X$  egy blokk méretű, továbbá, hogy blokkméret gond nem merül fel annak kapcsán, hogy  $A$  és  $B$  más modulust használ.)