



# Data Security

1. Alapelvek
2. Titkos kulcsú rejtjelezés
3. Nyilvános kulcsú rejtjelezés
4. Kriptográfiai alapprotokollok I.
5. Kriptográfiai alapprotokollok II.

# Data Security: Access Control

A Rossz talált egy bankkártyát, s szeretné a pénzt megszerezni. Egy terminál  $K=3$  sikertelen PIN kísérlet után bevonja a kártyát. 4 decimális karakter hosszú PIN kódot alkalmaznak. 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  $P$  valószínűsége a 0.01 értéket meghaladja)

# Data Security: Access control

Óvatos és csak 2 próbát végez terminálonként.

Minden új próbálkozásnál új kombinációt próbál ki.

Összes kipróbálható kombináció =  $10 * 4 * 2 = 80$ .

$1 - P = (10000 - 80) / 10000 \rightarrow P = 0.008 < 0.01$

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

# Data Security: 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

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

$C = M$

$k = [a, b] \in \mathbb{M}_M$

$c = a * m + b \text{ mod } 26, \quad k = [a, b] \in \mathbb{M}_M$

a) Adjuk meg a dekódoló transzformációt! Milyen megszorítást kell tenni "a" kulcselemre?

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)  $m=(c-b)*a^{-1}$  ,  $\gcd(a,26)=1$ , ( $a \neq 13$  ,  $2*i$  ,  $i=0 \dots 12$ )

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

### 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)vektor, 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 : NxN 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 of simple ciphers

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

*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  
EDKAPRKDLYEVLRRHHRH

# Data Security: Encryption

## Statistical analysis of simple ciphers

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

*guess 1:* R → e, D → t

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

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

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

→  $\gcd(a,26)=2 > 1$  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

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.

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

# 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

- Mekkora annak valószínűsége, hogy a 3 rejtett szöveg kerül továbbításra?
- A lehallgatott rejtett szöveg 3. Mekkora annak valószínűsége, hogy e volt a nyílt szöveg?
- 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	$C = \{1, 2, 3, 4\}$

$$\begin{aligned} \text{a.) } P(3) = 1/4 : \quad P(3) &= P(3|e)P(e) + P(3|f)P(f) \\ &= P(k3)P(e) + P(k2)P(f) \\ &= 1/16 + 3/16 = 1/4 \end{aligned}$$

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

$$\text{c.) Nem: } P(e | 1) = 1.$$

# Data Security: Protokollok

## 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.)

# Data Security: Kriptoprotokoll

Shamir háromlépéses protokollja:

Titok rejtett továbbítása előzetes kulcsmegegyezés nélkül?

A, B felhasználók

x üzenet

feltétel:

1. kommutatív tulajdonságú rejtjelezés  $E_B(E_A(x)) = E_A(E_B(x))$
2. lehallgató típusú támadó

1. A → B:  $y_1 = E_A(x)$

2. B → A:  $y_2 = E_B(E_A(x)) (= E_A(E_B(x)))$

3. A → B:  $y_3 = D_A(y_2) = E_B(x)$

# 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 rejtjelezzük.

Támadható a megoldás?

# 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?

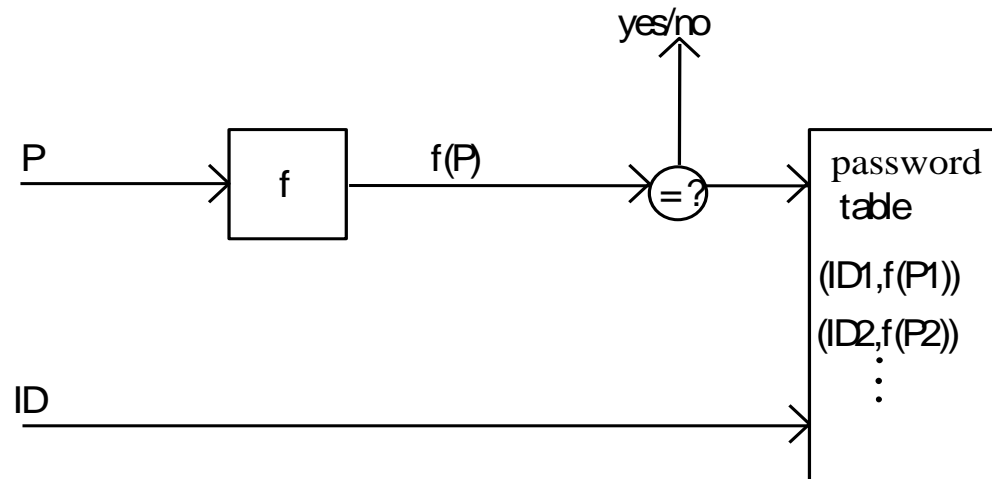
Készítsünk “biztonságos lenyomatot” a fájlról, hexadecimális ábrázolásban, s a fájl pl. email-ben történő elküldése után telefonon olvassuk fel a hexa sorozat néhány tagját a központban ülő ellenőrző személy számára (feltétel: központban ismert a telefonáló hangja)

“biztonságos lenyomatot” megvalósítása: kriptográfiai hash függvény

# Data Security: Kriptoprotokoll

## Identification

### Jelszó alapú azonosítás



Egyirányú leképezés

# Data Security: Kriptoprotokoll

## Key management

Egy kriptográfiát használó rendszerben a biztonság szintje nem haladja meg a kulcsgondozása biztonsági szintjét!

Kulcsgondozás alapfeladatok:

kulcs-

- generálás
- tárolás
- szétosztás (csere, megegyezés)
- frissítés
- visszavonás