



Data Security

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



Data Security: Concepts

1. Hozzáférésvédelem
2. Rejtjelezés
3. Azonosítás
4. Integritásvédelem
5. Kulcsgondozás

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: 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 a terminál bevonja a kártyát.

2.rendszer:

2 decimális karakter hosszú PIN kódot alkalmaz, és a PIN kód mindkét karaktere

beadaása után ellenőrzi és három egymás utáni hibás PIN-próbálkozás esetén nyeli el a kártyát.

Melyik a biztonságosabb rendszer?

Data Security: Access control

1.rendszer:

$$\frac{1}{10000} + 4 \cdot \left(\frac{9}{10}\right) \cdot \left(\frac{1}{9}\right) \cdot \left(\frac{1}{1000}\right) = 5 \cdot \left(\frac{1}{10000}\right) = 0.0005$$

2.rendszer:

$$1 - \left(\frac{99}{100}\right) \cdot \left(\frac{98}{99}\right) \cdot \left(\frac{97}{98}\right) = 1 - \frac{97}{100} = 0.003.$$

Tehát az első rendszer a biztonságosabb.

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

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

$C = M$

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

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

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

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

$c=mk$ (Hill rejtjelező)

$m^* = \text{fr id ay}$
 $c^* = \text{PQ CF KU}$

fr \rightarrow PQ : $E_{k(5,17)}=(15,16)$
id \rightarrow CF : $E_{k(8,3)}=(2,5)$
ay \rightarrow KU : $E_{k(0,24)}=(10,20)$

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

$$\det \begin{pmatrix} 5 & 17 \\ 8 & 3 \end{pmatrix} = 5*3 - 8*17 = -9 \pmod{26}$$

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 : $N \times N$ 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

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 mod 26 = I , N + B mod 26 = P , E + F 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

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

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

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.-től.

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

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

Data Security: Encryption

One Time Pad

Egy egy-bites x üzenetet rejtjelezve továbbítunk olyan módon, hogy pénzt dobunk fel, s ha fej az eredmény, akkor $r=1$ bitet, ha írás, akkor $r=0$ bitet adunk mod 2 az üzenethez, ahol $P(r=1)=1/3$, $P(r=0)=2/3$. Az x üzenet $1/2$ - $1/2$ valószínűséggel 0 illetve 1.

Q és R vitatkoznak: Q azt állítja, hogy mivel x véletlen, ezért úgy is tekinthető a kódolás, mint egy one time pad, ahol x a jó kulcs, így nem lehet sikeres (50%-nál nagyobb esélyű) a támadó döntése. R ezzel szemben azt állítja, hogy a véletlen találgatásnál van jobb döntés. (Feltételezhető, hogy a támadó is ismeri a pénz kimenetelek valószínűségeit és a továbbított értéket is képes lehallgatni.)

- Kinek van igaza, Q-nak vagy R-nek?
- Ennek megfelelően mi a legjobb döntés x értékére y ismeretében? Mekkora a döntés helyességének valószínűsége?

Data Security: Encryption

One Time Pad

$P(r=1)=1/3$, $P(r=0)=2/3$
 $P(x=1)=1/2$, $P(x=0)=1/2$

Találgatás a rejtett üzenetre

- R-nek van igaza, ugyanis, ha $x=0$, akkor $y=0$ a valószínűbb, ha $x=1$, akkor $y=1$ a valószínűbb megfigyelt érték.
- Legjobb döntés x értékére
 $y=0 \rightarrow x=0$ jó döntés valószínűsége: $2/3$
 $y=1 \rightarrow x=1$ jó döntés valószínűsége: $2/3$

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 \rightarrow B: $y_1 = E_A(x)$
2. B \rightarrow A: $y_2 = E_B(E_A(x)) (= E_A(E_B(x)))$
3. A \rightarrow 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?

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?

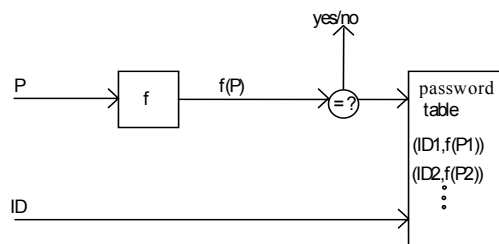
Készítsünk "biztonságos lenyomatot" a fájlról, hexadecimális ábrázolásban, s a fájl pl. email-ben történő elküldése után telefonon olvassuk fel a hexa sorozat néhány tagját a központban ülő ellenőrző személy számára (feltétel: központban ismert a telefonáló hangja)

"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

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 több, 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 elő 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 fél-bájt egyikébe. 25 db blokkot ilyen módon leképezve 100 db pénzfeldobás bitet kapunk.

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.)