(1)

KRIPTOLÓGIA: védett, ill. titkos kommunikáció tudománya.

- KRIPTOGRÁFIA tárgya: algoritmikus módszerek, melyek az üzenetek titkosságát, védettségét, hitelességét biztosítják
- KRIPTOANALÍZIS tárgya: a titok megfejtésére szolgáló algoritmusok, eljárások (illetéktelen is)

– titkosítás – történelem
- 70-es évektől egyre nagyobb arányú nyilvános kutatások

titkosítás
fizikai eljárások
ügyviteli eljárások } → információvédelem.

NYÍLT ADAT: a digitális forrás kimeneti adatfolyama

NYÍLT ÜZENET (PLAINTEXT): a nyílt adatból képzett blokkok:

$$\underline{b} = (b^{(1)}, b^{(2)}, \dots, b^{(M)})$$

TITKOSÍTÓ KÓDOLÓ: $E_{\underline{k}}: \mathcal{B}^M \to \mathcal{Y}^N$ egy-egyértelmű leképezés a nyílt adatból a tikosított üzenetbe, $\underline{k}$ paraméterrel.

TITKOSÍTOTT v. REJTETT ÜZENET (CIPHERTEXT): a titkosító kódoló kimenetén megjelenő, kódábécéből $(y_1, y_2, \dots, y_z)$ építkező N elemű sorozatok $\underline{y} = (y^{(1)}, y^{(2)}, \dots, y^{(N)})$.

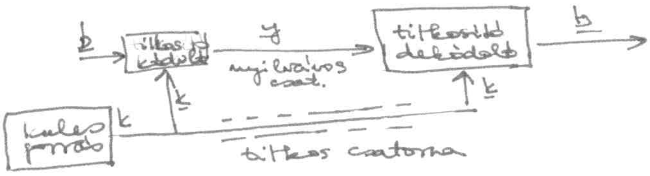
KULCS: az az információ mely egyértelműen megadja a titkosító transzformációt $\underline{k} = (k_1, \dots, k_K)$

TITKOSÍTÓ DEKÓDOLÓ: az $E_{\underline{k}}$ inverz transzformációja

$$\underline{y} = E_{\underline{k}}(\underline{b}) \text{ - hez} \qquad \underline{b} = D_{\underline{k}}(\underline{y})$$

- TITKOSÍTÓ ELJ. ABC → szó + ABC
- PERMUTÁCIÓS ELJ.: Blokk → Permutált blokk
- CAESAR - ELJ.: $y_i = b_i + k_i$ $\underline{k}$ kulcs, mod 26
- BINÁRIS VÉLETLEN ÁTKULCSOLÁS: $y_i^{bin} = b_i^{bin} + k_i^{bin}$ mod 2. (Vernam-féle)

EZEK: rejtett kulcsú v konvencionális v egykulcsos blokk-kódolások



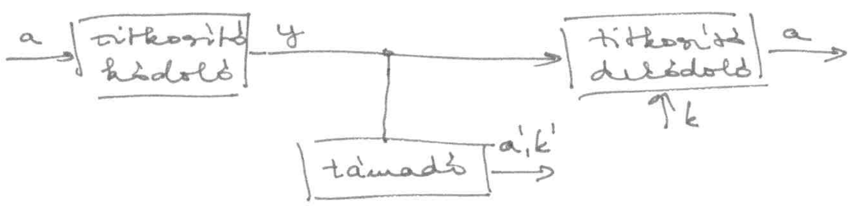
A támadó - célja: • $\underline{b}$ megszerzése
• $\underline{k}$ megszerzése
- ismer $\underline{k}$ kivételével mindent a titkosítási algoritmusból

- a kulcs gyorsan és gyakran cserélhető, a többi szelem változatlan.
- a rsz annyira védett, amennyire a kulcsa védett

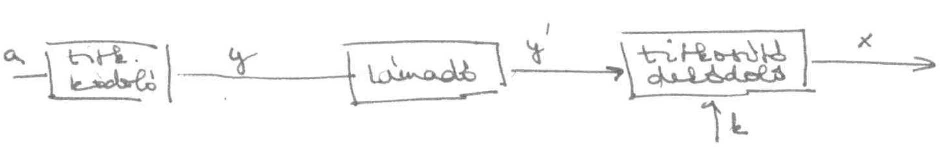
ALGORITMIKUS TÁMADÁSI MÓDSZEREK:

- PASSZÍV MÓDSZER: lehallgatás: a támadó a nyilvános csatornán hozzájut az üzenetekhez, az ezekből kinyert információkkal támadást indít a kulcs megszerzésére (→ kriptoanalízis)
  széleskörű háttérinformációk (nyelv, formátummegkötés, statisztikai tul., tipikus szavai, szófordulatai, fizikai támadások)

  TÍPUSAI növekvő veszélyességi sorrendben:
  - REJTETT SZÖVEGŰ TÁMADÁS (~~[illegible]~~ ciphertext only attack): a támadó ismer egy azonos kulccsal kódolt $E_{\underline{k}}(\underline{a}_1)\, E_{\underline{k}}(\underline{a}_2) \dots E_{\underline{k}}(\underline{a}_L)$ sorozatot, ebből próbál visszakövetkeztetni $\underline{k}$-ra
  - ISMERT NYÍLT SZÖVEGŰ TÁMADÁS (known plaintext attack): a támadó ismer egy nyílt szövegű szakaszt és annak kódolt változatát, az $(\underline{a}_1, E_{\underline{k}}(\underline{a}_1)), (\underline{a}_2, E_{\underline{k}}(\underline{a}_2)), \dots, (\underline{a}_L, E_{\underline{k}}(\underline{a}_L))$ párosokat
  - VÁLASZTHATÓ NYÍLT SZÖVEGŰ TÁMADÁS (chosen plain text attack): a támadó ismer egy általa választott nyílt szövegű szakaszt és annak kódolt változatát. (bank tranzakció)
  - VÁLASZTHATÓ SZÖVEGŰ TÁMADÁS (chosen text attack): a támadó szabadon megválaszthatja, akár a nyílt akár a rejtett szöveget, melynek a párját látni akarja.
- AKTÍV MÓDSZER: a rejtett üzenet csatornából való kivonása, cseréje, módosítása a támadó számára kedvező módon (ÜZENETMÓDOSÍTÁS) vagy valamely legális felhasználó szerepének eljátszása acélból, hogy információt csaljon ki egy másik, legális rendszerelemtől (MEGSZEMÉLYESÍTÉS)



PASSZÍV



TITKOS ÜZENET: csak legális (kívánatos) partner számára rekonstruálható az üzenet tartalma (PRIVACY) — tartalom

HITELES ÜZENET: csak olyan személy generálhata, aki az adott kulcs legális birtokosa (AUTHENTICITY) — személy

Egy támadó FELTÖRTE a titkosító algoritmust, ha egy lehallgatott üzenet nyílt tartalmát <u>gyorsan</u> meg tudja fejteni, függetlenül attól, melyik kulcsot használták.
Gyors a megfejtés akkor, ha azon az időintervallumon belül fejti meg, amin belül céljaira sikeresen fel tudja használni az üzenetet.

A TITKOSÍTÁSI ALGORITMUSOK CÉLJA a passzív támadások sikerességének akadályozása. Aktív támadás algoritmikusan nem akadályozható meg.

TITKOSÍTÁSI PROTOKOLLOK v. KRIPTOPROTOKOLLOK: előre meghatározott üzenetcsere folyamatok, melyet a partnerek együttműködve hajtanak végre valamely feladat végrehajtására.

<u>titkosítási algoritmus $\in$ kriptoprotokoll</u>

A kriptoprotokollok biztosítják a kapcsolat védett felépülését, az aktív támadások észlelését, garantálják a partnerek és üzeneteik hitelességét.

Vannak még:
- NYILVÁNOS KULCSÚ TITKOSÍTÁSI ALGORITMUSOK
- KULCSFOLYAMATOS TITKOSÍTÁS (stream cipher)

KONVENCIONÁLIS TITKOSÍTÓK

rejtett szövegű támadással szemben.

Legyen $\underline{B}$ és $\underline{K}$ az üzenet és a kód vv. vált. FÜGGETLEN

$\underline{b}$ és $\underline{k}$ az realizáltoló üzenet és kód

$\underline{Y} = E_{\underline{K}}(\underline{B})$ az titkosított üzenet vv. valt.

TÖKÉLETES TITKOSÍTÁS: ha $I(\underline{B}, \underline{Y}) = 0$, azaz, ha a nyílt és a rejtett üzenet kölcsönös információtartalma 0. $\rightarrow \underline{B}, \underline{Y}$ ftl (mintha a támadó egy $C=0$ csatorna kimenetét látná)

TÉTEL: Létezik tökéletes titkosítás:

Bizonyítás: pl. bináris véletlen átkulcsolás: $\underline{Y} = \underline{B} + \underline{K}$

$\underline{Y} = (Y^{(1)}, Y^{(2)}, \ldots, Y^{(N)})$, $\underline{B} = (B^{(1)}, B^{(2)}, \ldots, B^{(N)})$, $\underline{K} = (K^{(1)}, K^{(2)}, \ldots, K^{(N)})$ bináris vektorokkal.

Legyen $\underline{K}$ egyenletes eloszlású a bin. N-dim. vektorokon:

$$P(\underline{Y}=y \mid \underline{B}=\underline{b}) = P(\underline{B}+\underline{K}=y \mid \underline{B}=\underline{b}) = P(\underline{K}=y-\underline{b} \mid \underline{B}=\underline{b}) \underset{\text{független } K \text{ és } B}{=}$$

$$= P(\underline{K}=y-\underline{b}) \underset{\text{egyenl. eloszl.}}{=} \frac{1}{2^N}$$

$$\longrightarrow P(\underline{Y}=y) = \sum_{\underline{b}} \overbrace{\underbrace{p(\underline{Y}=y \mid \underline{B}=\underline{b}_i)}_{\frac{1}{2^N}} \cdot P(\underline{B}=\underline{b})}^{1} =$$

QED

$$= \frac{1}{2^N} = P(\underline{Y}=y \mid \underline{B}=\underline{b}) \longrightarrow \underline{Y} \text{ és } \underline{B} \text{ függetlenek}$$

- $\underline{B}$ eloszlásától függetlenül: független $\underline{Y}$ és $\underline{B}$
  $\underline{Y}$ egyenletes eloszl

de ehhez $\forall$ üzenet kódolásához új kulcs kell $\rightarrow$ az adási és vételi oldalon ∞ sok kulcsot kell tárolni v. védett csatornán annyi kulcsbitet átvinni, ahány bitet nyílt csatornán.

TÉTEL: $\forall$ tökéletes titkosító algoritmusra $\underline{\underline{H(\underline{K}) \geq H(\underline{B})}}$

Bizonyítás: $I(\underline{B}, \underline{Y}) = 0 \longrightarrow$

$$H(\underline{B}) = H(\underline{B} \mid \underline{Y}) + I(\underline{B}, \underline{Y}) = H(\underline{B} \mid \underline{Y})$$

$$H(B \mid Y) \leq H(\underline{B}, \underline{K} \mid \underline{Y})$$

kevesebb átl. inf.
ui B és $K \mid Y$ a kóddal kötött egymáshoz.

$$H(\underline{B}|\underline{Y}) \leq H(\underline{B},\underline{K}|\underline{Y}) = H(\underline{K}|\underline{Y}) + H(\underline{B}|\underline{Y},\underline{K}) = H(\underline{K}|\underline{Y}) \leq H(\underline{K})$$

$\underline{B} = D_{\underline{K}}(\underline{Y})$

$\rightarrow H(X|Y,K) = 0$

QED

Bináris esetben $H(\underline{B}) \leq H(\underline{K}) = H(K^{(1)},\ldots,K^{(N)}) = \#\underline{K}$ $\longrightarrow$ legalább annyi bináris számot kell tartalmaznia a kulcsnak, amennyi információt hordoz az ugyilt üzenet

MINIMÁLIS TÖKÉLETES TITKOSÍTÓ ELJÁRÁS, ha $\#K = \lceil H(\underline{B}) \rceil$.

$\longrightarrow$ A kulcsméret csökkentéséhez tömöríteni kell:

$H(\underline{B})$ fix $\rightarrow (\#K)_{min}$ fix $\longrightarrow$ az egy szimbólumra jutó kulcsmennyiség $\frac{H(B)}{M} \approx 1$ -gyel kell csökkenteni

ideális tömörítés + Vernam-titkosítás: $\#K = M = N \simeq H(\underline{B})$

GYAKORLATI TITKOSSÁGOT NYÚJTÓ titkosítási algoritmus, ha feltöréséhez irreálisan nagy számítási v. tárolási kapacitás szükséges.

FELTÉTEL NÉLKÜLI TITKOSSÁG: a megszerezhető információ mennyisége elvileg sem elegendő a kód feltöréséhez, bármekkora számítási és tárolási kapacitás áll rendelkezésre.
A tökéletes titkosító eljárások feltétel nélküli titkosságot biztosítanak.

A nyilvános kulcsú titkosítási eljárások csak gyakorlati titkosságra törekszenek.

NYILVÁNOS KULCSÚ TITKOSÍTÁS

gyakorlati titkosság anélkül, hogy a felek előzetesen, titkosan bármiféle kulcsot cseréltek volna

Két kulccsal dolgozik

- $\underline{k}_A^p$ nyilvános
- $\underline{k}_A^s$ titkos

$y = E_{\underline{k}_A^p}(\underline{b})$ könnyű fv.

$\underline{x} = D_{\underline{k}_A^s}(\underline{y})$ $\underline{k}_A^s$ nélkül nagyon nehéz

A, B, C ... felhasználók

$\underline{k}_A^p, \underline{k}_B^p, \underline{k}_C^p, \ldots$ nyilvános kulcsok kulcstárban, bárki által <u>olvasható</u>

- helyben generálhatók a $(\underline{k}_x^p, \underline{k}_x^s)$ párok, melyből $\underline{k}_x^p$ nyilvánosságra hozható
- hitelesség biztosítandó.
- $y = E_B(\underbrace{D_A(\underline{a})}_{\text{hitelesítés}})$ – digitális aláírás

<u>Shamir-eljárás:</u> • ha a behatoló csak lehallgatásra képes

– $\forall$ felhasználónak van egy titkos kulcsa

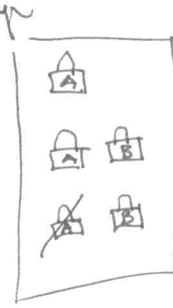
– legyen a kódoló kommutatív: $E_{k_A}(E_{k_B}(\underline{b})) = E_{k_B}(E_{k_A}(\underline{b}))$

– A → B titkos kommunikáció a következőképp

1.) A → B $y_1 = E_{k_A}(\underline{b})$

2.) B → A $y_2 = E_{k_B}(E_{k_A}(\underline{b}))$ $\left(= E_{k_A}(E_{k_B}(\underline{b}))\right)$

3.) A → B $y_3 = D_{k_A}(E_{k_B}(E_{k_A}(\underline{b}))) = E_{k_B}(\underline{b})$



ládák

- Ki van téve aktív támadásoknak (postás saját lakat)

kommutatív $E_{\underline{k}}(\underline{b}) = \underline{b} + \underline{k}$ mod 2

$(\underline{b} + \underline{k}_A) + \underline{k}_B = (\underline{b} + \underline{k}_B + \underline{k}_A)$ mod 2

→ a rejtett szövegre épülő támadásnak sem áll ellen

$y_1 = \underline{b} + \underline{k}_A$ $y_2 = \underline{b} + \underline{k}_A + \underline{k}_B$ $y_3 = \underline{b} + \underline{k}_B$ → $y_1 + y_2 + y_3 = \underline{b}$

kommutatív még: $x^e \bmod n$ $\quad x, e, n \in \mathbb{N}$

$$\left(x^{e_1}\right)^{e_2} = \left(x^{e_2}\right)^{e_1} \bmod n \longrightarrow$$ RSA
Rivest
Shamir
Adleman