

# TITKOSÍRÁSOK

Waldhauser Tamás

SZTE Bolyai Intézet

# A titkosírás matematikai modellje

Az üzenetet darabokra bontjuk, és feltesszük, hogy minden egyes darab egy véges  $A$  halmaz eleme. Gyakran számokkal kódoljuk a darabokat:

$A = \{0, 1, \dots, m - 1\}$  vagy  $A = \mathbb{Z}_m$ .

## Példa

- betűk:  $A = \mathbb{Z}_{26}$  ( $A = 0, B = 1, \dots, Z = 25$ )
- ASCII kódok:  $A = \mathbb{Z}_{128}$  ( $A = 65, B = 66, \dots, Z = 90, [ = 91, \dots$ )
- betűhármások:  $A = \mathbb{Z}_{26}^3$  ( $AAA = 0, AAB = 1, \dots, ZZZ = 17575$ )

titkosítás (kódolás, sifírozás)

$T: A \rightarrow A$  bijekció

visszafejtés (dekódolás, desifírozás)

$T^{-1}: A \rightarrow A$

# Caesar-kód

- $A = \mathbb{Z}_{26}$  ( $A = 0, B = 1, \dots, Z = 25$ )
- kulcs:  $c \in \mathbb{Z}_{26}$
- $T: \mathbb{Z}_{26} \rightarrow \mathbb{Z}_{26}, x \mapsto x + c$
- $T^{-1}: \mathbb{Z}_{26} \rightarrow \mathbb{Z}_{26}, x \mapsto x - c$

## Példa

A  $c = 3$  kulcs esetén

titkosított üzenet:    N D O N X O X V

visszafejtett üzenet:    K A L K U L U S

# Vigenère-sifír

- $A = \mathbb{Z}_{26}^\ell$  ( $A \dots AA = 0$ ,  $A \dots AB = 1$ , ...,  $Z \dots ZZ = 26^\ell - 1$ )
- kulcs:  $c \in \mathbb{Z}_{26}^\ell$
- $T: \mathbb{Z}_{26}^\ell \rightarrow \mathbb{Z}_{26}^\ell, x \mapsto x + c$
- $T^{-1}: \mathbb{Z}_{26}^\ell \rightarrow \mathbb{Z}_{26}^\ell, x \mapsto x - c$

Lényegében a Vigenère-sifír egy változata a *one-time-pad*, ahol a kulcs hossza annyi, mint a küldendő (összes) üzenet(ek) hossza. Ha a kulcs teljesen véletlenszerű, akkor ez a titkosítás gyakorlatilag (sőt, elméletileg is!) feltörhetetlen. Problémát jelent azonban a kulcsok legyártása és szétosztása.

Ezt oldják meg a **nyilvános kulcsú titkosítások**, amelyeket még a kulcs ismeretében is nehéz feltörni, azaz a  $T$  kódolófüggvény ismeretében is nehéz meghatározni a  $T^{-1}$  dekódolófüggvényt (**csapóajtófüggvény**).



# Diffie–Hellman-kulcsváltás

## Tétel

Ha  $p$  prímszám, akkor létezik olyan  $\bar{g} \in \mathbb{Z}_p^*$  elem, amelyre  $o(\bar{g}) = p - 1$ .

Ha  $g$  egy ilyen **primitív gyök**, akkor  $\mathbb{Z}_p^*$  minden eleme előáll  $\bar{g}$  hatványaként:

$$\forall \bar{a} \in \mathbb{Z}_p^* \exists i \in \mathbb{Z}: \bar{g}^i = \bar{a}.$$

Az  $i$  kitevőt az  $\bar{a}$  maradékosztály **diszkrét logaritmusának** vagy **indexének** nevezzük (a  $p$  modulusra és a  $g$  primitív gyökre nézve).

Ha  $p$  elég nagy, akkor a diszkrét logaritmus kiszámítása nehéz(?) feladat, ezért használható arra, hogy Alice és Bob közös titkot hozhasson létre még akkor is, ha nem tudnak megbízható csatornán kommunikálni.

# Diffie–Hellman-kulcsváltás

- Alice és Bob megegyezik egy nagy  $p$  prímszámban és egy hozzá tartozó  $g$  primitív gyökben.
- Alice választ egy titkos  $a$  kitevőt, és a  $\bar{g}^a$  hatványt elküldi Bobnak.
- Bob választ egy titkos  $b$  kitevőt, és a  $\bar{g}^b$  hatványt elküldi Alice-nek.
- Alice ki tudja számolni a  $\bar{g}^{ab}$  hatványt így:  $\bar{g}^{ab} = (\bar{g}^b)^a$ .
- Bob ki tudja számolni a  $\bar{g}^{ab}$  hatványt így:  $\bar{g}^{ab} = (\bar{g}^a)^b$ .
- Az ellenség megtudhatja  $p$ ,  $g$ ,  $\bar{g}^a$ ,  $\bar{g}^b$  értékét, de ezekből nem tudja(?) kiszámítani  $\bar{g}^{ab}$  értékét.

A csak Alice és Bob által ismert  $\bar{g}^{ab}$  használható egy titkosírás kulcsaként.

# RSA-eljárás

## Tétel

Legyen  $p$  és  $q$  két különböző prímszám, és legyenek  $e, d$  olyan egész számok, melyekre  $ed \equiv 1 \pmod{(p-1)(q-1)}$ . Ekkor az alábbi két leképezés egymás inverze:

$$T: \mathbb{Z}_{pq} \rightarrow \mathbb{Z}_{pq}, x \mapsto x^e;$$

$$T^{-1}: \mathbb{Z}_{pq} \rightarrow \mathbb{Z}_{pq}, x \mapsto x^d.$$

## Bizonyítás.

Legyen  $m = pq$ , ekkor  $\varphi(m) = (p-1)(q-1)$ . Mivel  $ed \equiv 1 \pmod{\varphi(m)}$ , alkalmas  $k$  egész számmal felírható  $ed = 1 + k \cdot \varphi(m)$  alakban.

Használjuk az Euler–Fermat-tételt:

$$\begin{aligned} T(T^{-1}(x)) &= T^{-1}(T(x)) = x^{ed} = x^{1+k \cdot \varphi(m)} = \\ &= x \cdot (x^{\varphi(m)})^k \equiv x \cdot 1^k \equiv x \pmod{m}. \quad \checkmark \end{aligned}$$

Hol a hiba a bizonyításban?

# RSA-eljárás

## Tétel (zanzásítva)

$$ed = 1 + k \cdot (p - 1)(q - 1) \implies x^{ed} \equiv x \pmod{pq}$$

## Bizonyítás (folyt.)

Az Euler–Fermat-tétel csak akkor alkalmazható, ha  $\text{Inko}(x, pq) = 1$ . Ha ez nem teljesül, akkor három eset lehetséges.

1.  $p \nmid x$  és  $q \mid x$ : Ekkor modulo  $p$  alkalmazhatjuk az Euler–Fermat-tételt:

$$x^{ed} = x^{1+k \cdot (p-1)(q-1)} = x \cdot (x^{\varphi(p)})^{(q-1)k} \equiv x \cdot 1^{(q-1)k} \equiv x \pmod{p}.$$

Modulo  $q$  pedig triviális a dolog:

$$q \mid x \implies x \equiv 0 \pmod{q} \implies x^{ed} \equiv 0 \pmod{q}.$$

Beláttuk, hogy  $x^{ed} \equiv x \pmod{p}$  és  $x^{ed} \equiv x \pmod{q}$ , és ebből már következik, hogy  $x^{ed} \equiv x \pmod{pq}$ . ✓



# RSA-eljárás

## Tétel (zanzásítva)

$$ed = 1 + k \cdot (p - 1)(q - 1) \implies x^{ed} \equiv x \pmod{pq}$$

## Bizonyítás (folyt.)

Az Euler–Fermat-tétel csak akkor alkalmazható, ha  $\text{Inko}(x, pq) = 1$ . Ha ez nem teljesül, akkor három eset lehetséges.

2.  $p \mid x$  és  $q \nmid x$ : Hasonló az előző esethez.
3.  $p \mid x$  és  $q \mid x$ : Triviális ( $x \equiv 0 \pmod{pq}$ ).



# RSA-eljárás

- Alice titokban választ nagy  $p$  és  $q$  prímszámokat és kiszámítja  $\varphi(pq) = (p-1)(q-1)$  értékét.
- Alice választ egy olyan  $e$  kitevőt, melyre  $\text{Inko}(e, (p-1)(q-1)) = 1$ .
- Ekkor létezik olyan  $d$ , amelyre  $ed \equiv 1 \pmod{(p-1)(q-1)}$ , és Alice ezt könnyen ki tudja számítani euklideszi algoritmussal.
- Így Alice megkapja a kódoló és dekódoló függvényt:

$$T_A: \mathbb{Z}_{pq} \rightarrow \mathbb{Z}_{pq}, x \mapsto x^e; \quad T_A^{-1}: \mathbb{Z}_{pq} \rightarrow \mathbb{Z}_{pq}, x \mapsto x^d.$$

- Alice elküldi Bobnak (vagy akár az egész világnak) a  $pq$  és  $e$  számokat.
- Ha Bob (vagy bárki más) az  $x$  üzenetet akarja küldeni Alice-nek, akkor a  $T_A(x)$  értéket küldi el, amit Alice a  $T_A^{-1}$  függvény birtokában vissza tud fejteni.
- Az ellenség nem tudja(?) kiszámítani  $d$  értékét (a  $T_A^{-1}$  függvényt), mert ehhez a  $pq$  számot faktorizálnia kellene(?).

# Kronológia

- 1874 - W. S. Jevons: „*Can the reader say what two numbers multiplied together will produce the number 8 616 460 799? I think it is unlikely that any one but myself will ever know. . .*”  
(1889 C. J. Busk:  $96\,079 \times 89\,684$ .)
- 1970 - J. H. Ellis: a nyilvános kulcs (csapóajtófüggvény) ötlete
- 1973 - C. Cocks: RSA
- 1974 - M. J. Williamson: D–H-kulcsváltás
- 1976 - W. Diffie, M. Hellman: D–H-kulcsváltás
- 1977 - R. Rivest, A. Shamir, L. Adleman: RSA  
(RSA-129 feltörve 1994-ben)
- 1997 - A GCHQ nyilvánosságra hozza a történetet.