

# Az informatikai biztonság alapjai

Pintér-Husztai Andrea

2022. november 1.

# Tartalom

- 1 Hash függvények, Digitális aláírások
  - Hash függvények
  - Digitális aláírási sémák

# Hash függvények

# Kriptográfiai hash függvények

## Definíció

*A  $H : \{0, 1\}^* \rightarrow \{0, 1\}^n$ ,  $n \in \mathbb{N}$  függvényt hash függvénynek nevezzük.*

Tetszőleges véges hosszú üzenethez  $n$  hosszú üzenetet rendelünk.

- kriptográfiai hash pl.: MD5, SHA-1, SHA-256, SHA-512, SHA-3(Keccak, 2015)
- adatintegritás ellenőrzése: Hash függvénnyel ellenőrizhetjük, hogy egy állomány változott -e vagy sem. Az állomány hash értéke szeparáltan tárolt. Kiszámítjuk az állomány hash értékét és összevetjük a tárolt hash értékkel. Ha különböznek, akkor az állomány módosult.
- A hash értéket lenyomatnak is hívjuk.
- **lavinahatás**: Egy bit változása az inputban, jelentős változást eredményez az outputban. (pl. az output fele)

# Elvárások

A hash függvények nem injektívek.

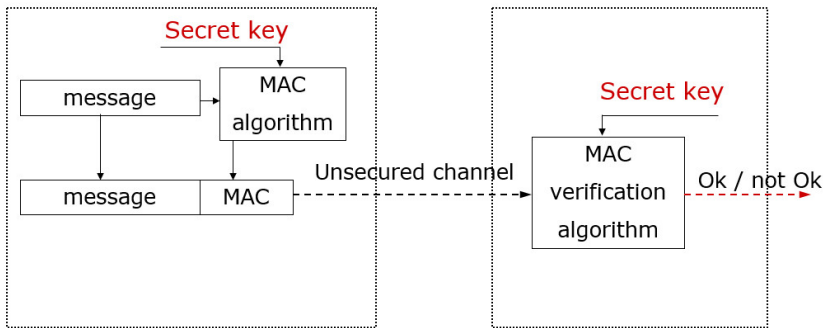
## Definíció

Az  $(x, x') \in \{0, 1\}^* \times \{0, 1\}^*$  a  $H$  hash függvény egy ütközése, ha  $x \neq x'$  és  $h(x) = h(x')$ .

Három jellemző:

- **Őskép ellenálló:** Adott  $y \in Y$  értékhez, nehéz olyan  $x \in X$  értéket megadni, hogy  $H(x) = y$ .
- **Második őskép ellenálló**(gyengén ütközésmentes): Adott  $x$  értékhez nehéz olyan  $x'$  értéket találni, hogy  $x \neq x'$  és  $H(x) = H(x')$ .
- **Ütközésmentes**(erősen ütközésmentes): Nehéz olyan  $x, x' \in X$  értékeket találni, hogy  $H(x) = H(x')$ .

# Üzenethitelesítés - Message Authentication Codes (MAC)



Jellemzők:

- Hitelesség (forrása az, amit megjelöltek, adatintegritás)

# Üzenethitelesítés

pl.:  $HMAC_K(m) = H((K' \oplus opad) || H((K' \oplus ipad) || m))$ , ahol

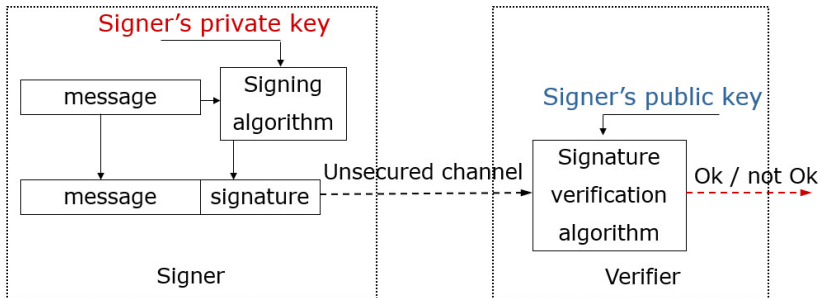
$H$ : hash függvény,  $m$ : üzenet,

$K$ : titkos kulcs,  $K'$ : másik titkos kulcs, mely  $K$ -ból származtatott

$||$ : konkatenáció jele,  $opad$ : külső konstans,  $ipad$ : belső konstans.

# Digitális aláírási sémák





Biztonsági jellemzők:

- Hitelesség (forrása az, amit megjelöltek, adatintegritás)
- letagadhatatlanság

# Formális definíció

## Definíció

A digitális aláírási séma egy  $DS = (Key, Sign, Ver)$  hármas, ahol

- *Key*: A *Key* kulcsgeneráló algoritmus a  $k$  biztonsági paraméterre kiszámítja a  $(PK, SK)$  kulcspárt, ahol  $PK$  nyilvános és  $SK$  titkos.
- *Sign*: A *Sign* aláíró algoritmus az  $SK$  titkos kulcshoz és az  $m \in \{0, 1\}^*$  üzenetre generál egy  $s = Sign_{SK}(m)$  aláírást.
- *Ver*: A *Ver* ellenőrző algoritmus a  $PK$  nyilvános kulcsra, az  $m$  üzenetre, és az  $s$  aláírásra IGAZ vagy HAMIS értéket ad vissza. IGAZ esetén az aláírás érvényes, HAMIS esetén érvénytelen.

$\mathcal{M}$ : üzenetek halmaza

$\mathcal{S}$ : aláírások halmaza

# Támadó célja

- **Teljes feltörés:** A támadó ki tudja számolni az aláíró fél titkos kulcsát.
- **Univerzális hamisítás:** A támadó bármilyen üzenethez képes érvényes aláírást generálni.
- **Szelektív hamisítás:** A támadó képes egy általa választott üzenethez aláírást generálni.
- **Egzisztenciális hamisítás:** A támadó képes egy aláírt üzenetet generálni.

# Támadási módok

- **Csak a nyilvános kulcs ismert (Key-only attack):** A támadó csak a nyilvános kulcsot ismeri.
- **Ismert üzenet alapú támadás (Known message attack):** A támadó ismer egy ugyanazon kulccsal aláírt üzenetlistát.
- **Választott üzenet alapú támadás (Chosen message attack):** A támadó rendelkezésére áll egy általa választott üzenetek és a hozzájuk tartozó aláírások listája.
- **Adaptívan választott üzenet alapú támadás (Adaptive chosen message attack):** A támadó rendelkezésére áll egy általa választott üzenetek és a hozzájuk tartozó aláírások listája, ahol az üzenetet a korábban megkapott aláírások alapján választja ki.

# RSA aláírási séma

$$DS = (Key, Sign, Ver)$$

- *Key*:

- 1 Véletlenül választunk két nagy prímet:  $p, q$ .
- 2 Kiszámítjuk az RSA modulust:  $n = p \cdot q$ .
- 3 Kiszámítjuk  $n$  Euler-féle  $\phi$  függvény értékét:  

$$\phi(n) = (p - 1)(q - 1).$$
- 4 Véletlenül választunk egy  $e$  egészt, ahol  $1 < e < \phi(n)$  és  
 $(e, \phi(n)) = 1$ .
- 5 Kiszámítjuk:  $d$ :  $1 < d < \phi(n)$ , ahol  $ed \equiv 1 \pmod{\phi(n)}$ .

$PK = (n, e)$ ,  $SK = d$  és  $\phi(n)$ ,  $p, q$  titkos paraméterek

$$\mathcal{M} = \mathcal{S} = \mathbb{Z}_n$$

- $Sign_{SK}(m) = m^d \pmod{n} \quad \forall m \in \mathcal{M}$ , ahol  $SK = d$ .
- $Ver_{PK}(m, s) = \begin{cases} TRUE, & s^e \equiv m \pmod{n}; \\ FALSE, & \text{egyébként.} \end{cases}$   
 $\forall (m, s) \in \mathcal{M} \times \mathcal{S}$ , ahol  $PK = (n, e)$ .

# A tankönyvi RSA aláírással szembeni támadások

- Az RSA univerzálisan hamisítható a választott üzenet alapú támadás mellett.

Input: tetszőleges  $m, PK = (n, e)$ ,  $s'$  egy adott  $m'$  üzenetre

Output:  $s$

Algoritmus:

- 1 Véletlenül választunk  $r \in \mathcal{M}$
  - 2 Kiszámítjuk:  $r' \equiv r^e \pmod{n}$
  - 3 Kérjük az  $m' \equiv m \cdot r' \pmod{n}$  aláírását, megkapjuk  $s'$ -t.
  - 4 Kiszámítjuk  $s \equiv s' \cdot r^{-1} \pmod{n}$
- Az RSA egzisztenciálisan hamisítható a csak nyilvános kulcs ismert támadás mellett.

Input:  $PK = (n, e)$

Output:  $(m, s) \in \mathcal{M} \times \mathcal{S}$

Algoritmus:

- 1 Véletlenül választjuk:  $s \in \mathcal{S}$
- 2 Kiszámítjuk:  $m \equiv s^e \pmod{n}$

# RSA-FDH (Full Domain Hash) aláírási séma

$DS = (Key, Sign, Ver)$

- *Key:*

- 1 Véletlenül választunk két nagy prímet:  $p, q$ .
- 2 Kiszámítjuk az RSA modulust:  $n = p \cdot q$ .
- 3 Kiszámítjuk  $n$  Euler-féle  $\phi$  függvény értékét:  
 $\phi(n) = (p - 1)(q - 1)$ .
- 4 Véletlenül választunk egy  $e$  egészt, ahol  $1 < e < \phi(n)$  és  $(e, \phi(n)) = 1$ .
- 5 Kiszámítjuk:  $d$ :  $1 < d < \phi(n)$ , ahol  $ed \equiv 1 \pmod{\phi(n)}$ .

$PK = (n, e)$ ,  $SK = d$  és  $\phi(n)$ ,  $p, q$  titkos paraméterek

$\mathcal{M} = \{0, 1\}^*$ ,  $\mathcal{S} = \mathbb{Z}_n$

- $Sign_{SK}(m) = H(m)^d \pmod{n} \forall m \in \mathcal{M}$ , ahol  $SK = d$ ,  
 $H : \{0, 1\}^* \rightarrow \mathbb{Z}_n$  hash függvény.

- $Ver_{PK}(m, s) = \begin{cases} TRUE, & s^e \equiv H(m) \pmod{n}; \\ FALSE, & \text{egyébként.} \end{cases}$

$\forall (m, s) \in \mathcal{M} \times \mathcal{S}$ , ahol  $PK = (n, e)$ .