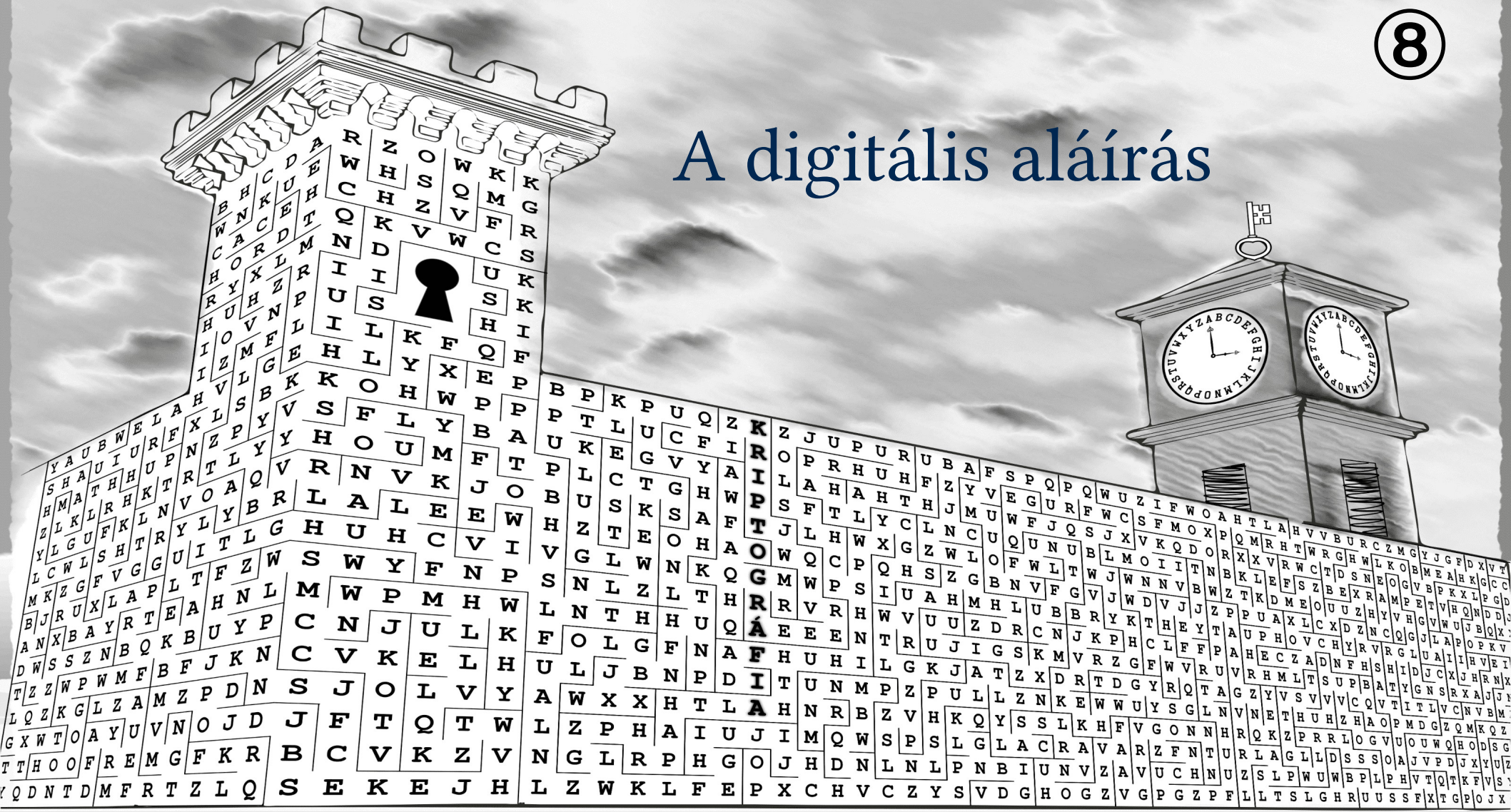
A digitális aláírás



A digitális aláírás

- az üzenethez csatolt, korlátozott hosszúságú adat
- segítségével ellenőrizhető:
  - a küldő fél (aláíró) identitása
  - az üzenet eredetisége, épsége (felismerhető az esetleges hamisítás)
- előállítható egy nyilvános kulcsú titkosítási rendszer és egy hash függvény használatával

A digitális aláírás

Ha az A felhasználó szeretne küldeni B-nek egy aláírt és titkosított P üzenetet, akkor a következőt küldheti el:

$$C = E_B(P \,||\, D_A(E_B(h(P)))),$$

ahol:

- E_B – a B felhasználó nyilvános kódoló eljárása
- D_A – az A felhasználó titkos dekódoló eljárása
- h – hash függvény

A digitális aláírás

A P üzenet után csatolt $D_A(E_B(h(P)))$ adat lesz az A felhasználónak a B felhasználó számára készített digitális aláírása, amire igaz, hogy:

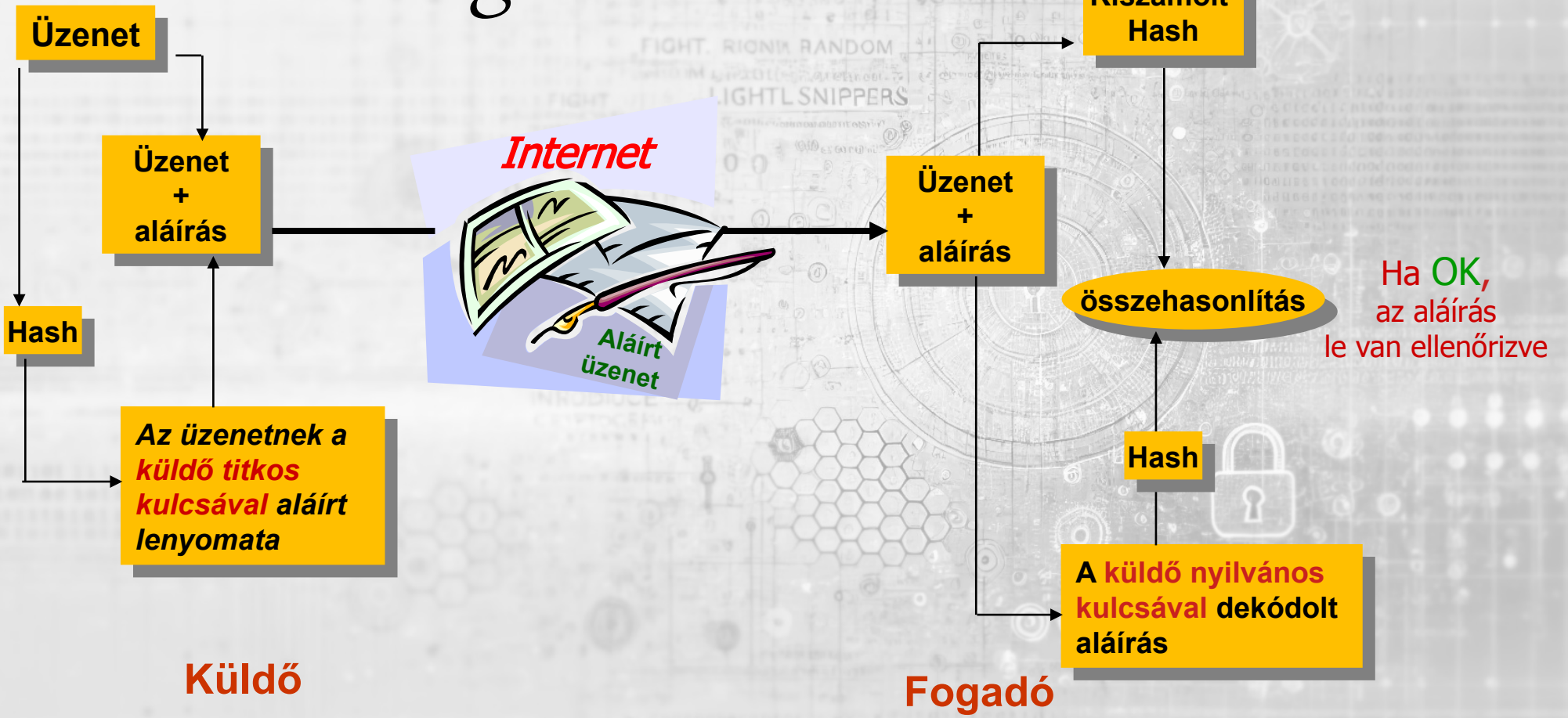
- más nem állíthatja elő, mert D_A titkos
- függ az üzenet tartalmától, de mivel csak egy kódolt lenyomatról van szó, a hossza nem túl nagy
- nem lehet ezt az aláírást egy másik üzenet esetén használni
- személyre szabott, csak B-nek szól (D_A használata miatt nem lehet $D_A(E_{B'}(h(P)))$ alakra átírni, ahol $B \neq B'$)

A digitális aláírás

B a köv. módon tudja ellenőrizni A aláírását:

- kiszámolja $D_B(C) = (P' \,||\, S)$-t, ahol D_B a titkos dekódolási eljárása és S a digitális aláírás, aminek a hossza ismert (rögzített)
- leellenőrzi a $h(P') = D_B(E_A(S))$ egyenlőséget, ahol E_A az A nyilvános kódoló eljárása:
  - ha egyenlőség van, akkor $P = P'$
  - ellenkező esetben az üzenet sérült, vagy akarattal módosították

A digitális aláírás



A digitális aláíró algoritmus (DSA)

- DSA – Digital Signature Algorithm
- 1993-tól NIST szabvány, a DSS (Digital Signature Standard) része
- szerzője David W. Kravitz (volt NSA alkalmazott)
- tervben van a fokozatos kivezetése 2025-től kezdődően (a 160 bites kulcs és az SHA-1 használata miatt)

A digitális aláíró algoritmus (DSA)

1. **A kulcsok generálása** (ezt a lépést a rendszer összes felhasználója elvégzi)

   - Válassz egy 160 bites prímszámot, legyen ez q.
   - Válassz egy L bites p prímszámot úgy, hogy $p = 1 \bmod q$, $512 \leq L \leq 1024$ és L osztható 64-gyel.
   - Válassz egy $h \in \mathbb{N}$ értéket úgy, hogy $1 < h < p-1$ és $1 < g = h^{\frac{p-1}{q}} \bmod p$.
   - Válassz véletlenszerűen egy $x \in \mathbb{N}$ értéket, ahol $0 < x < q$.
   - Számítsd ki $y = g^x \bmod p$-t.
   - A nyilvános kulcs (p, q, g, y), a titkos kulcs pedig x. Vegyük észre, hogy a (p, q, g) számhármast a rendszer több felhasználója is használhatja.

A digitális aláíró algoritmus (DSA)

2. **Az üzenetek aláírása**

- Minden egyes üzenet esetében válassz egy egyszer használatos véletlenszerű k számot, ahol $0 < k < q$.
- Számítsd ki $r = (g^k \bmod p) \bmod q$-t.
- Számítsd ki $s = (k^{-1}(h(M) + xr)) \bmod q$-t, ahol $h(M)$ az M üzenet SHA-1 lenyomata.
- Generálj másik k értéket, és végezd el újra az előbbi két műveletet abban az esetben, ha $r = 0$ vagy $s = 0$ (ennek a valószínűsége elég kicsi).
- Az aláírás az (r, s) pár lesz.

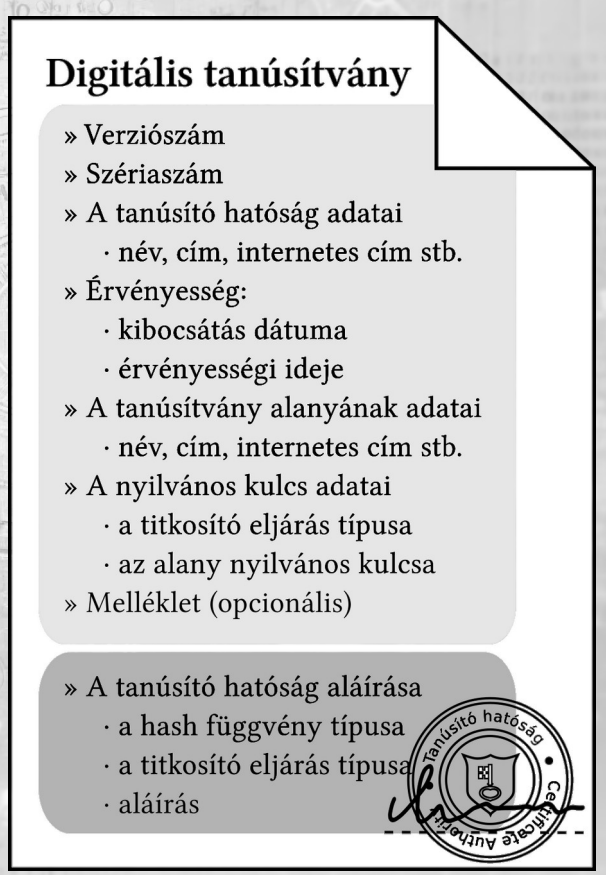
A digitális aláíró algoritmus (DSA)

3. **Az aláírás ellenőrzése**

- Az aláírás hiteltelen, ha a $0 < r < q$ valamint $0 < s < q$ egyenlőtlenségek nem teljesülnek.
- Számítsd ki $w = s^{-1} \bmod q$-t.
- Számítsd ki $u_1 = (h(M)w) \bmod q$-t.
- Számítsd ki $u_2 = rw \bmod q$-t.
- Számítsd ki $v = ((g^{u_1} y^{u_2}) \bmod p) \bmod q$-t.
- Az aláírás akkor valódi, ha $v = r$.

A digitális tanúsítvány

- az aláíró elektronikus „személyi igazolványa”, mely az aláíróról hiteles és pontos adatokat szolgáltat
- egy tanúsító hatóság (angolul Certificate Authority, rövidítve CA) adja ki, amiben a rendszer összes felhasználója feltétlenül megbízik
- fontos szerepük van az internetes alkalmazások biztonságában



Nyilvános kulcsú infrastruktúra

- public key infrastructure – PKI
- szerepek, irányelvek, eljárások sorozata, amely ahhoz szükséges, hogy létrehozzunk, kezeljünk, terjesszünk, használjunk, tároljunk és visszavonjunk digitális tanúsítványokat, illetve kezeljük a nyílt kulcsú titkosításokat.

Nyilvános kulcsú infrastruktúra

A PKI felépítése:

- **azonosító hatóság** (CA, certificate authority), amely tárolja, kiosztja és megjelöli a digitális tanúsítványokat
- **regisztrációs hatóság** (RA, registration authority), amely az azonosító hatóságnál tárolt digitális tanúsítványok alapján az egységek beazonosítását igazolja
- **központi könyvtár** (central directory), ahol biztonságos módon tárolják és jelölik a kulcsokat
- **tanúsításirányítási rendszer** (certificate management system), amely a tárolt tanúsítványok hozzáférését irányítja, illetve a tanúsítványokat elosztja,
- **tanúsítási irányelvek** (certificate policy), melyek leírják a PKI-rendszer folyamataival szemben támasztott követelményeket azzal a céllal, hogy a PKI-rendszer megbízhatóságával kapcsolatos külső személyek számára lehetővé tegyék annak elemzését.

Nyilvános kulcsú infrastruktúra