Titkosírások

Nyilvános kulcsú titkosírások

Egy ü üzenetet titkosítunk a T titkosítófüggvénnyel.

- nyilvános rész: T és $T(\text{ü})$
- titkos rész: T^{-1} (és persze ü)

Olyan T függvényt kell választani, amelynek az inverzét nehéz kiszámítani.

Ötlet: könnyű összeszorozni két nagy (prím)számot, de nehéz (prím)tényezőkre bontani a szorzatot. (Jevons, 1874)

Konkrét megvalósítás: RSA (Cocks, 1973, és Rivest-Shamir-Adleman, 1977)

Az RSA-eljárás

Legyen $m = pq$, ahol p és q nagy prímszámok, és legyenek e, d olyan természetes számok, hogy $ed \equiv 1 \pmod{\varphi(m)}$. Ekkor az alábbi két függvény egymás inverze:

$$T : \mathbb{Z}_m \to \mathbb{Z}_m,\ \overline{x} \mapsto \overline{x}^e;$$
$$T^{-1} : \mathbb{Z}_m \to \mathbb{Z}_m,\ \overline{x} \mapsto \overline{x}^d.$$

Valóban, ha $x \perp m$, akkor az Euler–Fermat-tétel szerint x kitevője csak modulo $\varphi(m)$ „számít", azaz

$$(x^d)^e \equiv (x^e)^d \equiv x^{ed} \equiv x^1 \pmod{m}.$$

(HF: és ha x nem relatív prím m-hez?)

Ha ismert p és q, akkor $\varphi(m) = (p-1)(q-1)$ könnyen kiszámítható, és adott e kitevőhöz könnyen lehet megfelelő d párt találni (hogyan?).

Ha viszont csak m és e (azaz a T függvény) ismert, akkor nehéz(??) kiszámolni a d kitevőt (azaz a T^{-1} függvényt).

Az RSA-eljárás

Alice és Bob szeretne egymással üzenetet váltani. Alice választ p_A, q_A nagy prímeket és e_A, d_A kitevőket úgy, hogy $e_A \cdot d_A \equiv 1 \pmod{\varphi(p_A \cdot q_A)}$.

- nyilvános rész: $m_A = p_A q_A$ modulus, e_A nyilvános kitevő
- titkos rész: p_A, q_A prímek, d_A titkos kitevő

Ha Bob az ü üzenetet akarja küldeni Alice-nek (tfh. $1 \leq$ ü $\leq m_A$), akkor az ü^{e_A} hatvány modulo m_A maradékát küldi el, és azt Alice dekódolja a titkos kitevőjével: $(\text{ü}^{e_A})^{d_A} \equiv$ ü $\pmod{m_A}$.

Bob (és mindenki, aki részt akar venni a kommunikációban), szintén generál magának p_B, q_B prímeket és e_B, d_B kitevőket, és közli Alice-szel (vagy akár az egész világgal) az $m_B = p_B q_B$ modulust és e_B nyilvános kitevőt.

Ha Alice (vagy bárki más) üzenni akar Bobnak, akkor azt az ü$^{e_B} \bmod m_B$ titkosítással kódolja, amit csak Bob tud dekódolni (remélhetőleg).

Mindez használható az üzenet küldőjének azonosítására (hiteles aláírás), sőt telefonon keresztül történő pénzfeldobásra is!