RSA (definizione e correttezza)

Rivest, Shamir, Adleman. Funzione one-way trap-door: moltiplicazione (inversa fattorizzazione è difficile anche se non è dimostrato che sia NP-hard).

Creazione delle chiavi

- si generano (Miller-Rabin) due primi p e q grandi (prodotto di 2048 bit fino al 2030, poi 3072);
- si calcola $n = pq$, $\phi(n) = (p-1)(q-1)$;
- si sceglie $e < \phi(n)$ tale che $(e, \phi(n)) = 1$;
- si trova $d = e^{-1} \bmod \phi(n)$.

$$k_{\text{pub}} = (n, e) \qquad k_{\text{priv}} = d$$

Tutte le operazioni sono eseguite in tempo polinomiale.

Cifratura e decifrazione

Il messaggio m interpretato come intero deve essere $< n$ per garantire l'iniettività. Se non lo è, si divide in blocchi di $b = \lfloor \log_2 n \rfloor$. In pratica si fissa un limite b comune, per cui:

$$m < 2^b < n$$

Data la chiave pubblica (n, e) e quella privata d,

$$C(m, k_{\text{pub}}) = m^e \bmod n \qquad D(c, k_{\text{priv}}) = c^d \bmod n.$$

Entrambe le operazioni richiedono tempo polinomiale con quadrature successive.

Correttezza

Mostriamo che $D(C(m)) = m$, ovvero:

$$m^{ed} \bmod n = m$$

$(m, n) \notin \{1, p, q\}$**:** impossibile, significa che $m \geq n$;

$(m, n) = 1$**:**

$$\begin{aligned} m^{ed} \bmod n &= (m^{\phi(n)})^k m \bmod n && ed = k\phi(n) + 1 \\ &= m \bmod n \\ &= m && m < n \end{aligned}$$

$(m, n) = p$**:**

$$m^{ed} \equiv m \mod n \overset{\text{TCR}}{\iff} \begin{cases} m^{ed} \equiv m \mod p \\ m^{ed} \equiv m \mod q \end{cases}$$

La prima equazione è soddisfatta perché

$$p \mid m \implies m^{ed} \equiv m \equiv 0 \mod p,$$

e visto che $q \nmid m$ (altrimenti $(m, n) = pq$), analogamente al caso precedente,

$$m^{ed} \equiv m^{k\phi(n)+1} \equiv m(m^{q-1})^{k(p-1)} \equiv m \mod q;$$

$(m, n) = q$**:** come sopra.