Crittografia a chiave pubblica

Chiave pubblica

Crittografia asimmetrica: ogni utente ha una coppia di chiavi, pubblica per cifrare e privata per decifrare.

$$c = C(m, k_{\text{pub}}) \qquad m = D(c, k_{\text{priv}})$$

La funzione di cifratura è *one-way trap-door*:

one-way cifratura facile, decifrazione difficile;

trap-door a meno che non si possegga la trap-door (chiave privata),

per esempio:

prodotto/fattorizzazione calcolare $n = pq$ è facile, ma trovare p e q a partire da n no (non si conosce un algoritmo polinomiale, ma non è stato dimostrato che è NP-hard) se non si conosce uno dei fattori (chiave segreta);

esponenziazione/radice in modulo $y = x^k \bmod n$ si calcola velocemente con quadrature successive, ma trovare $x = \sqrt[k]{y} \bmod n$ se n è composto richiede tempo esponenziale;

esponenziazione/logaritmo in modulo $y = a^x \bmod n$ si calcola con QS, ma l'inverso (logaritmo discreto) è difficile tanto quanto la fattorizzazione.

Vantaggi:

- molti a uno: per n utenti servono $2n$ chiavi anziché $n(n-1)/2$;
- non è richiesto scambio segreto di chiavi

Svantaggi:

- molto più lenti dei cifrari simmetrici;
- esposti per costruzione ad attacchi di tipo *chosen plain-text*: il crittoanalista può determinare se un dato messaggio è stato mandato perché può cifrare messaggi arbitrari;
- vulnerabili ad attacchi man-in-the-middle (intercettazione e modifica della chiave pubblica).