Livello di segretezza e sicurezza dei cifrari

Distinguiamo cifrari ad uso:

ristretto la sicurezza dipende dalla segretezza delle funzioni di cifratura e decifrazione (e.g. cifrario di Cesare);

generale solo la chiave è segreta:

$$c = C(m, k) \qquad m = D(c, k)$$

dove k è una chiave segreta diversa per ogni coppia di utenti, che deve essere necessaria per la decifrazione del messaggio. Il numero delle chiavi deve essere sufficientemente elevato da scongiurare attacchi esaurienti (brute force).

La sicurezza di un cifrario può essere:

incondizionata nasconde l'informazione con certezza assoluta;

computazionale nasconde l'informazione solo se il crittoanalista ha accesso a risorse computazionali limitate.

Un cifrario ha sicurezza di b bit se il costo del miglior attacco è di ordine $\mathrm{O}(2^b)$ operazioni di decifrazione. Se il miglior attacco è un brute force puro, allora b è la dimensione della chiave.

Un cifrario è sicuro se non ci sono attacchi più efficienti del forza bruta.