Cifrari perfetti

Intuitivamente: la sicurezza è garantita qualunque sia l'informazione catturata dal crittoanalista sul canale. Agli occhi del crittoanalista il crittogramma è una sequenza casuale priva di significato.

Formalmente, definendo:

- MSG spazio dei messaggi;
- CRITTO spazio dei crittogrammi;
- M variabile aleatoria che descrive il comportamento del mittente, e assume i valori in MSG;
- C variabile aleatoria che descrive la comunicazione sul canale, e assume valori in CRITTO;
- $P(M = m)$ probabilità che il mittente voglia inviare $m \in$ MSG;
- $P(M = m \mid C = c)$ probabilità condizionale che il messaggio inviato sia $m \in$ MSG, posto che sul canale transita il crittogramma $c \in$ CRITTO,

un cifrario è perfetto se:

$$\forall m \in \text{MSG}, c \in \text{CRITTO} \quad . \quad P(M = m \mid C = c) = P(M = m).$$

Scenario: il crittoanalista conosce

- distribuzione di probabilità con cui il mittente sceglie i messaggi;
- cifrario utilizzato;
- spazio delle chiavi.

Svantaggio: per il teorema di Shannon richiede almeno tante chiavi quanti sono i messaggi possibili.

Esempi

Casi estremi di cifrari *non* perfetti:

- $P(M = \overline{m}) = p > 0 \implies \exists \overline{c} \,.\, P(M = \overline{m} \mid C = \overline{c}) = 1$
- $P(M = \overline{m}) = p > 0 \implies \exists \overline{c} \,.\, P(M = \overline{m} \mid C = \overline{c}) = 0$