Teorema di Shannon

In un cifrario perfetto il numero delle chiavi deve essere maggiore o uguale al numero dei messaggi possibili ($m \in \text{MSG}$ è possibile se $P(M = m) > 0$).

Condizione necessaria ma non sufficiente.

Dimostrazione

$N_k = \#\text{chiavi}$, $N_m = \#\text{messaggi possibili}$.
Per assurdo sia $N_k < N_m$.

Dato $c \in \text{CRITTO}$, posso provare a decifrare c con tutte le chiavi. Alcune chiavi possono dare lo stesso messaggio decifrato, perciò indichiamo:

$$s = \#\text{messaggi possibili che possono corrispondere a } c.$$

Vale:

$$s \leq N_k < N_m,$$

perciò esiste un messaggio possibile m' che non può corrispondere a c, quindi

$$P(M = m' \mid C = c) = 0,$$

ma $P(M = m') = p > 0$ perché m' è possibile, e questo è in contraddizione con la proprietà dei cifrari perfetti ($P(M = m \mid C = c) = P(M = m)$).