Teorema 2.10: Se (Gen, Enc, Dec) è uno schema di cifratura perfettamente segreto con spazio dei messaggi $\mathcal{M}$ e spazio delle chiavi K, allora

$$|K| \geq |\mathcal{M}|$$

Dimostrazione: Mostreremo che se $|K| < |\mathcal{M}|$, lo schema Π non è perfettamente segreto.

IPOTESI

hp.1 sia $|K| < |\mathcal{M}|$

hp.2 $Pr[C = c] > 0$

hp.3 prob. unif. di scegliere un certo $m \in \mathcal{M}$

DEFINIZIONI:

$$\mathcal{M}(c) = \{m \mid m := Dec_K(c), \text{ per qualche } K \in K\}$$

chiaramente $|\mathcal{M}(c)| \leq |K|$ perché in $\mathcal{M}(c)$ ci sono tanti elementi tante quante sono le chiavi che andiamo ad usare per tentare di decifrare m.

per hp. 1

$$|K| < |M| \Rightarrow |M(c)| \leq |K| < |M| \Rightarrow |M(c)| < |M|$$

cioè $\exists\, m' \in M$ t.c. $m' \notin M(c)$, allora:

$$Pr[M = m' \mid C = c] = 0 \neq Pr[M = m']$$

cioè, la probabilità che venga scelto un certo messaggio $m' \in M$ conoscendo un certo cifrato $c \in C$ è 0 che è diversa dalla probabilità che venga scelto il messaggio $m' \in M$. Cioè lo schema non è perf. segreto. Noi però vogliamo che:

$$Pr[M = m' \mid C = c] = Pr[M = m']$$

che è la nostra def. di segretezza perfetta. Questo implica dunque che per essere

$$|K| \geq |M|$$