PREPARAZIONE: B SCEGLIE 2 NUMERI PRIMI $p \neq q$, $p \neq q$ E CALCOLA

$$n \overset{def}{=} p \cdot q$$

POI CALCOLA

$$\Phi \overset{def}{=} (p-1)\cdot(q-1)$$

ALLORA CALCOLA $e \in \mathbb{P}$ TALE CHE

$$(e, \Phi) = 1$$

INFINE B CALCOLA L'INVERSA MOLTIPLICATIVA

$$[d]_\Phi \text{ DI } [e]_\Phi$$

QUINDI B PUBBLICA n E e E TIENE SEGRETI p, q, d

CODIFICA: A PRENDE UN MESSAGGIO m TALE CHE $(m, n) = 1$ E $1 \leq m \leq n$, E SPEDISCE $[m^e]_n$

$$\left[m\right]_n \overset{alt}{=} \left[m^2\right]_n$$

DECODIFICA: B RICEVE $\tilde{m}$ E LO DECODIFICA CALCOLANDO

$$\left[\tilde{m}^{d}\right]_n$$