

PREPARATION: B SCEGLIE 2 NUMERI

Primi  $p$  e  $q$ ,  $p \neq q$  e CALCOLA

$$n \stackrel{\text{def}}{=} p \cdot q$$

Poi CALCOLA

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

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

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

INFINE B CALCOLA L'INVERSA  
MULTPLICATIVA

$$[d]_{\Phi} \text{ s.t. } [e]_{\Phi}$$

Quindi B PUBBLICA  $n$  e  $e$   
e TIENE SEGRETO  $p, q, d$

CODIFICA: A PRENDE UN MESSAGGIO

$m$  TALE CHE  $(m, n) = 1$  e  $1 \leq m \leq n$ ,

e SPEDISCE  $[m]_n$  a B

$$[m]_n \stackrel{\text{def}}{=} [m^e]_n$$

DECODIFICA:  $\mathcal{B}$  RICEVE  $\tilde{m}$  E

LO DECODIFICA CALCOLANDO

$$[\tilde{m}^{\text{ol}}]_n$$

