

DECODIFICHIAMO IL MESSAGGIO CRIPTATO

$$[\tilde{m}]_m = [1029]_{3901} \quad \text{DOBBIAMO CALCOLARE}$$

$$[\tilde{m}^d]_m = [1029^{503}]_{3901}$$

ABBIAMO CHE

$$503 = 256 + 128 + 64 + 32 + 16 + 4 + 2 + 1$$

CALCOLIAMO

$$[1029^2]_{3901} = [1058841]_{3901} = [1670]_{3901}$$

$$[1029^4]_{3901} = \left( [1029^2]_{3901} \right)^2 = [1670^2]_{3901} = [2788900]_{3901}$$

$$= [3586]_{3901}$$

$$[1029^8]_{3901} = \left( [1029^4]_{3901} \right)^2 = [3586^2]_{3901}$$

$$= \begin{bmatrix} 128 & 89 & 396 \end{bmatrix}_{3901}^{10501} = \begin{bmatrix} 1700 \end{bmatrix}_{3901}^{10501}$$

$$\star \begin{bmatrix} 1029 & 16 \end{bmatrix}_{3901}^{10501} = \left( \begin{bmatrix} 1029 & 8 \end{bmatrix}_{3901}^{10501} \right)^2 = \begin{bmatrix} 1700^2 \end{bmatrix}_{3901}^{10501} = \begin{bmatrix} 3260 \end{bmatrix}_{3901}^{10501}$$

$$\begin{bmatrix} 1029 & 32 \end{bmatrix}_{3901}^{10501} = \left( \begin{bmatrix} 1029 & 16 \end{bmatrix}_{3901}^{10501} \right)^2 = \begin{bmatrix} 3260^2 \end{bmatrix}_{3901}^{10501} =$$

$$= \begin{bmatrix} 1276 \end{bmatrix}_{3901}^{10501}$$

$$[1029^{64}]_{3901} = \left( [1029^{32}]_{3901} \right)^2 = [1276^2]_{3901} =$$

$$= [1459]_{3901}$$

$$[1029^{128}]_{3901} = \left( [1029^{64}]_{3901} \right)^2 = [1459^2]_{3901} =$$

$$= [2636]_{3901}$$

$$\begin{bmatrix} 1029 & 256 \end{bmatrix}_{3901} = \left( \begin{bmatrix} 1029 & 128 \end{bmatrix}_{3901} \right)^2 = \left( \begin{bmatrix} 2636 \end{bmatrix}_{3901} \right)^2$$

$$= \begin{bmatrix} 815 \end{bmatrix}_{3901}$$

PERTANTO

$$\begin{bmatrix} 1029 & 503 \end{bmatrix}_{3901} = \begin{bmatrix} 1029 & 256 \end{bmatrix}_{3901} \cdot \begin{bmatrix} 1029 & 128 \end{bmatrix}_{3901}$$

$$\begin{aligned}
 & \cdot \left[ \begin{matrix} 1029 \\ 64 \end{matrix} \right]_{3901} \cdot \left[ \begin{matrix} 1029 \\ 32 \end{matrix} \right]_{3901} \cdot \left[ \begin{matrix} 1029 \\ 16 \end{matrix} \right]_{3901} \cdot \left[ \begin{matrix} 1029 \\ 4 \end{matrix} \right]_{3901} \\
 & \cdot \left[ \begin{matrix} 1029 \\ 2 \end{matrix} \right]_{3901} \cdot \left[ \begin{matrix} 1029 \\ 1 \end{matrix} \right]_{3901} =
 \end{aligned}$$

$$\begin{aligned}
 & \cdot \left[ \begin{matrix} 1029 \\ 2 \end{matrix} \right]_{3901} \cdot \left[ \begin{matrix} 1029 \\ 1 \end{matrix} \right]_{3901} =
 \end{aligned}$$

$$\begin{aligned}
 & = \left[ \begin{matrix} 815 \\ 3901 \end{matrix} \right] \cdot \left[ \begin{matrix} 2636 \\ 3901 \end{matrix} \right] \cdot \left[ \begin{matrix} 1459 \\ 3901 \end{matrix} \right] \cdot \left[ \begin{matrix} 1276 \\ 3901 \end{matrix} \right] \cdot
 \end{aligned}$$

$$\begin{aligned}
 & \cdot \left[ \begin{matrix} 3260 \\ 3901 \end{matrix} \right] \cdot \left[ \begin{matrix} 3586 \\ 3901 \end{matrix} \right] \cdot \left[ \begin{matrix} 1670 \\ 3901 \end{matrix} \right] \cdot \left[ \begin{matrix} 1029 \\ 3901 \end{matrix} \right] =
 \end{aligned}$$

$$= [2790]_{3901} \cdot [907]_{3901} \cdot [2964]_{3901} \cdot [1990]_{3901}$$

$$= [3]_{3901}$$

PERTANTO IL MESSAGGIO ORIGINALE

ERA

$$[m]_n = [\hat{m}^d]_n = [1029^{503}]_{3901} = [3]_{3901}$$

ES.: SIANO  $p, q, n, e, d$  COME IN RSA.

SIA  $1 \leq m \leq n$ . QUAL'È LA PROBABILITÀ

CHE  $(m, n) > 1$  ?

QUESTA PROBABILITÀ È

$$\frac{n - \Phi(n)}{n} = \frac{p \cdot q - p \cdot \left(1 - \frac{1}{p}\right) \left(1 - \frac{1}{q}\right)}{p \cdot q}$$

$$= 1 - \left(1 - \frac{1}{p}\right) \cdot \left(1 - \frac{1}{q}\right) = \frac{1}{p} + \frac{1}{q} - \frac{1}{p \cdot q}$$



$$SE \quad p, q \approx 10^{1000} \Rightarrow \frac{1}{p}, \frac{1}{q} \approx 10^{-1000}, \quad \frac{1}{p \cdot q} \approx 10^{-2000}$$

$$\Rightarrow \frac{1}{p} + \frac{1}{q} - \frac{1}{p \cdot q} \approx 2 \cdot 10^{-1000} =$$

$$= 0,000 \dots \dots \dots 0002.$$

1000