DECODIFICHIAMO IL MESSAGGIO CRIPTATO

$[\tilde{m}]_n = [1029]_{3901}$. DOBBIAMO CALCOLARE

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

ABBIAMO CHE

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

CALCOLIAMO

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

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

$$= \left[3586\right]_{3901}$$

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

$$= \left[1285^{5}9396 \right]_{3901} = \left[1700 \right]_{3901}$$

$$* \left[1029^{16} \right]_{3901} = \left(\left[1029^{8} \right]_{3901} \right)^{2} = \left[1700^{2} \right]_{3901} = \left[3260 \right]_{3901}$$

$$\left[1029^{32} \right]_{3901} = \left(\left[1029^{16} \right]_{3901} \right)^{2} = \left[3260^{2} \right]_{3901} =$$

$$= \left[1276 \right]_{3901}$$

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

$$= \left[1459\right]_{3901}$$

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

$$= \left[2636\right]_{3901}$$

$$\left[1029^{256}\right]_{3901} = \left(\left[1029^{128}\right]_{3901}\right)^2 = \left(\left[2636\right]_{3901}\right)^2$$

$$= \left[815\right]_{3901}$$

PERTANTO

$$\left[1029^{503}\right]_{3901} = \left[1029^{256}\right]_{3901} \cdot \left[1029^{128}\right]_{3901} \cdot$$

$$\cdot \left[1029^{64}\right]_{3901} \cdot \left[1029^{32}\right]_{3901} \cdot \left[1029^{16}\right]_{3901} \cdot \left[1029^{4}\right]_{3901}$$

$$\cdot \left[1029^{2}\right]_{3901} \cdot \left[1029\right]_{3901} =$$

$$= \left[815\right]_{3901} \cdot \left[2636\right]_{3901} \cdot \left[1459\right]_{3901} \cdot \left[1276\right]_{3901} \cdot$$

$$\cdot \left[3260\right]_{3901} \cdot \left[3586\right]_{3901} \cdot \left[1670\right]_{3901} \cdot \left[1029\right]_{3901} =$$

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

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

PERTANTO IL MESSAGGIO ORIGINALE ERA

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

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

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

CHE $(m, n) > 1$?

QUESTA PROBABILITÀ È

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

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

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

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

$$= 0,\underbrace{000 \ldots\ldots 000}_{1000}2 .$$