ES.: COSTRUIRE UN SISTEMA DI COMUNICAZIONE RSA USANDO i PRIMI $p=47$ E $q=83$. INOLTRE CODIFICARE E DECODIFICARE UN MESSAGGIO.

CALCOLIAMO

$$m = p \cdot q = 47 \cdot 83 = 3901$$

QUINDI

$$\varphi(m) = (p-1)\cdot(q-1) = 46 \cdot 82 = 3772$$

TROVIAMO $e \in \mathbb{P}$ TALE CHE $(e, (p-1)\cdot(q-1)) = 1$.
DOBBIAMO AVERE $(e, 3772) = 1$. PROCEDIAMO
PER TENTATIVI, $e = 15$ FUNZIONA. TROVIA-
MO L'INVERSA MOLTIPLICATIVA $[\alpha]_{(p-1)(q-1)}$
DI $[e]_{(p-1)(q-1)} = [15]_{3772}$. CALCOLIAMO A.E.:

$$3772 = (200+40+10+1)\cdot 15 + 7$$

$$15 = 2\cdot 7 + \boxed{1}, \quad 7 = 7\cdot 1 + 0$$

CALCOLIAMO L'ID. DI BEZOUT:

$$1 = 15 + 7 \cdot (-2)$$

$$= 15 + \left(3772 + 15 \cdot (-251)\right) \cdot (-2)$$

$$= 15 \cdot (503) + 3772 \cdot (-2)$$

QUINDI L'ID. DI BEZOUT È

$$1 = 15 \cdot (503) + 3772 \cdot (-2)$$

PERTANTO $[d]_{(p-1)\cdot(q-1)} = [503]_{3772}$.

PUBBLICHIAMO

$$m = 3901 \quad , \quad e = 15$$

TENIAMO PRIVATI

$$p = 47 \quad , \quad q = 83 \quad , \quad d = 503 \, .$$

CODIFICHIAMO UN MESSAGGIO $1 \leq m \leq n$ TALE CHE $(m, n) = 1$. PRENDIAMO $m = 3$ ($(3, 3901) = 1 \Rightarrow$ o.k.). CODIFICHIAMO. DOBBIAMO CALCOLARE

$$[m^e]_n = [3^{15}]_{3901}.$$

ABBIAMO CHE

$$15 = 8 + 4 + 2 + 1$$

QUINDI

$$[3^2]_{3901} = [9]_{3901}$$

$$[3^4]_{3901} = \left([3^2]_{3901}\right)^2 = \left([9]_{3901}\right)^2 = [81]_{3901}$$

$$[3^8]_{3901} = \left([3^4]_{3901}\right)^2 = \left([81]_{3901}\right)^2 =$$

$$= \left[81^2 \right]_{3901} = \left[6561 \right]_{3901} = \left[2660 \right]_{3901}$$

$$\left(3901 + 2660 \right)$$

PERTANTO

$$\left[3^{15} \right]_{3901} = \left[3^8 \right]_{3901} \cdot \left[3^4 \right]_{3901} \cdot \left[3^2 \right]_{3901} \cdot \left[3 \right]_{3901}$$

$$= \left[2660 \right]_{3901} \cdot \left[81 \right]_{3901} \cdot \left[9 \right]_{3901} \cdot \left[3 \right]_{3901}$$

$$= \left[2660 \right]_{3901} \cdot \left[81 \right]_{3901} \cdot \left[27 \right]_{3901}$$

$$= [2660]_{3901} \cdot [8\ 2187]_{3901}$$

$$= [5817420]_{3901}$$

$$= [1029]_{3901}$$

SPEDIAMO QUINDI IL MESSAGGIO CODIFICATO CHE È

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

SONDAGGIO: SIANO $a, b \in \mathbb{P}$ TALI CHE $(a,b)=1$. ALLORA:

(53)

a) $(2a, 2b) = 2$ 72% ✓

b) $(2a, 2b) = 1$ 15%

c) $(2a, b) = 2$ 6%

d) $(a, 2b) = 1$ 7%

e) NDQ. 0%