COSTRUIRE UN SISTEMA DI COMUNICAZIONE RSA USANDO I PRIMI $p = 47$ E $q = 83$.

INOLTRE CODIFICARE E DECODIFICARE UN MESSAGGIO

INNANZITUTTO CALCOLIAMO

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

POI CALCOLIAMO

$$\Phi(n) = (p-1)\cdot(q-1) = 46 \cdot 82 = 3772$$

TROVIAMO $e \in \mathbb{P} : MCD(e, 3772) = 1$, PER FARLO ANDIAMO A TENTATIVI. PER ESEMPIO 15 VA BENE. QUINDI

$$e = 15$$

ORA CALCOLIAMO L'INVERSA MOLTIPLICATIVA DI $[15]_{3772}$. INIZIAMO CON $MCD(3772, 15)$

$$3772 = 251 \cdot 15 + 7$$
$$15 = 2 \cdot 7 + 1$$
$$7 = 7 \cdot 1 + 0 = MCD(3772, 15)$$

ORA CALCOLIAMO L'IS DI BEZOUT

$$1 = 15(1) + 7(-2)$$
$$= 15(1) + (3742 + 15 \cdot (-251))(-2)$$
$$= 3742(-2) + 15(503)$$

QUINDI L'INVERSA MOLTIPLICATIVA DI

$$[15]_{3742} \text{ è } [d]_{\equiv_{CM}} = [503]_{3742}$$

PUBBLICHIAMO $m = 3901$ E $Q = 15$

INVECE TENIAMO PRIVATI

$$p = 47, \quad q = 83 \quad \text{E} \quad d = 503$$

ORA CODIFICHIAMO UN MESSAGGIO $1 \leq m \leq m$

TALE CHE $MCD(m, m) = 1$.

PRENDIAMO 3 PER ESEMPIO ($MCD(3, 3901) = 1 \rightarrow$ OK)

CALCOLIAMO

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

ABBIAMO CHE

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

Quindi

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

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

$$[3^8]_{3901} = ([81]_{3901})^2 = [6561]_{3901} =$$

$$= [2660]_{3901}$$

Per tanto

$$[3^{15}]_{3901} = [3]_{3901} \cdot [9]_{3901} \cdot [81]_{3901} \cdot [2660]_{3901} =$$

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

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

$$= [5917420]_{3901} =$$

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

Segue quindi il messaggio codificato

$$[1029]_{3901}$$

Decodifichiamo il messaggio calcolato:

$$[1029^{503}]_{3301}$$

Abbiamo che:

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

Calcoliamo

$$[1029^2]_{3301} = [1058841]_{3301} = [1670]_{3301}$$

$$[1029^4]_{3301} = \left([1670^2]_{3301}\right)^2 = [2788900]_{3301} =$$

$$= [3586]_{3301}$$

$$[1029^8]_{3301} = \left([3586]_{3301}\right)^2 = [12853396]_{3301} =$$

$$= [1400]_{3301}$$

$$[1029^{16}]_{3301} = \left([1400]_{3301}\right)^2 = [2830000]_{3301} =$$

$$= [3260]_{3301}$$

$$[1029^{32}]_{3301} = \left([3260]_{3301}\right)^2 = [10624600]_{3301} =$$

$$= [1246]_{3301}$$

$$[1023^{64}]_{3301} = \left([1246]_{3301}\right)^2 = [1628176]_{3301} =$$

$$= [1450]_{3301}$$

$$[1023^{128}]_{3301} = \left([1450]_{3301}\right)^2 = [2128681]_{3301} =$$

$$= [2063]_{3301}$$

$$[1023^{256}]_{3301} = \left([2063]_{3301}\right)^2 = [6978796]_{3301} =$$

$$= [815]_{3301}$$

Quindi

$$[1023^{503}]_{3301} = [3]_{3301}$$

AVETE 2 INTERLOCUTORI: A e B. LE CHIAVI PUBBLICHE SONO $n = 221$ ED $e = 11$ (A), $n = 391$ ED $e = 15$ (B).

LE VOSTRE CHIAVI SONO $n = 667$, $e = 39$

(PUBBLICHE) È $d = 79$ (PRIVATA).

VOLETE SPEDIRE IL MESSAGGIO 16 A B.

CODIFICATELO.

PRENDIAMO TALE MESSAGGIO $m = 16$

E CALCOLIAMO

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

QUINDI

$$[16^{15}]_{391}$$ MA

$15 = 8 + 4 + 2 + 1$

QUINDI

$$[16^2]_{391} = [256]_{391}$$

$$[16^4]_{391} = \left([256]_{391}\right)^2 = [256^2]_{391} =$$

$$= [65536]_{391} = [239]_{391}$$

$$[16^8]_{391} = \left([239]_{391}\right)^2 = [57121]_{391} =$$

$$= [35]_{391}$$

PERTANTO

$$[16^{15}]_{391} = [16]_{391} \cdot [256]_{391} \cdot [239]_{391} \cdot [35]_{391}$$

$$= [4096]_{391} \cdot [8365]_{391} =$$

$$= [186]_{391} \cdot [754]_{391} =$$

$$= [28644]_{391} = [101]_{391}$$

IN CONCLUSIONE IL MESSAGGIO CODIFICATO DA SPEDIRE AD B è $[101]_{391}$

AVETE 2 INTERLOCUTORI: A e B. LE CHIAVI PUBBLICHE SONO $n = 1037$ ED $e = 7$ (n

$n = 391$ ed $e = 9$ (B).

Le vostre chiavi sono $n = 391$, $e = 47$ (pubblica) e $d = 79$ (privata).

Ricevute il messaggio 3 da B, decifrate:

Per decifrare il messaggio 3 dobbiamo calcolare

$$[3^{79}]_{391}$$

ma

$$79 = 64 + 8 + 4 + 2 + 1$$

Quindi

$$[3^2]_{391} = [81]_{391}$$

$$[3^4]_{391} = \left([81]_{391}\right)^2 = [6561]_{391} =$$

$$= [305]_{391}$$

$$[9^8]_{391} = \left([305]_{391}\right)^2 = [93025]_{391} =$$

$$= [358]_{391}$$

$$[9^{16}]_{391} = \left([358]_{391}\right)^2 = [128164]_{391} =$$

$$= [304]_{391}$$

$$[9^{32}]_{391} = \left([304]_{391}\right)^2 = [92416]_{391} =$$

$$= [18]_{391}$$

$$[9^{64}]_{391} = \left([18]_{391}\right)^2 = [324]_{391}$$

QUINDI

$$[9^{79}]_{391} = [9]_{391} \cdot [81]_{391} \cdot [305]_{391} \cdot [358]_{391} \cdot$$

$$\cdot [324]_{391}$$

$$= [2916]_{391} \cdot [1405]_{391} \cdot [358]_{391} =$$

$$= [179]_{391} \cdot [72]_{391} \cdot [358]_{391} =$$

$$= [6139056]_{391} = [104]_{391}$$

Quindi il messaggio decodificato è 104.