Bejan-Topîrceanu Lucian-Cosmin @ Cripto - temă

Ex. 85072 28652 36131 22033 76275 - mesajul criptat.

Avem m_j, cu $j = \overline{1,5}$ necunoscute.

cheia publică: (86609, 65777)

Deci $\begin{cases} n = 86609 \\ e = 65777 \end{cases} \Leftrightarrow n = p \cdot q \Leftrightarrow n = 257 \cdot 337 \Rightarrow \varphi(n) = \varphi(p) \cdot \varphi(q) = 256 \cdot 336 = 86016$

Se observă că $\gcd(e, \varphi(n)) = 1$.

Luăm astfel $d = e^{-1} \pmod{\varphi(n)}$, adică $d = 65777^{-1} \pmod{86016} = 17$.

$\boxed{d = 17}$.

~~De demonstrat~~

Deci avem - cheie publică $(n, e) = (86609, 65777)$.
- cheie privată $d = 17$.

Pentru a decripta fiecare m_j, $j = \overline{1,5}$ vom aplica $m = c^d \pmod{n}$

Astfel:

- $m_1 = c_1^d \pmod{n} = 85072^{17} \pmod{86609} = 3181$.
- $m_2 = c_2^d \pmod{n} = 28652^{17} \pmod{86609} = 3921$
- $m_3 = c_3^d \pmod{n} = 36131^{17} \pmod{86609} = 1465$.
- $m_4 = c_4^d \pmod{n} = 22033^{17} \pmod{86609} = 1893$
- $m_5 = c_5^d \pmod{n} = 76275^{17} \pmod{86609} = 920$.

Concatenând obținem: 3181 3921 1465 1893 920

Vom presupune că numerele reprezintă indexii literelor alfabetului cu A=1, B=2 etc...

3181 3921 1465 1893 920.

I CAHA CIBA ADȚEAHIC IT

II. CRA CIBA ADȚE. RIC LI

III CRA CIU N FERIC IT - multumim, la fel.