23.04.24

Elem TN 9_3 11

RSA (Ron RIVEST, Adi SHAMIR, Leonard ADELMAN)

elemente de text ↔ valori numerice

RSA constă în prelucrarea respectivelor valori numerice de următoarea manieră:

Considerăm două numere prime distincte $p \neq$ „mari", $p \neq q$.

Considerăm și un număr e (cu proprietatea

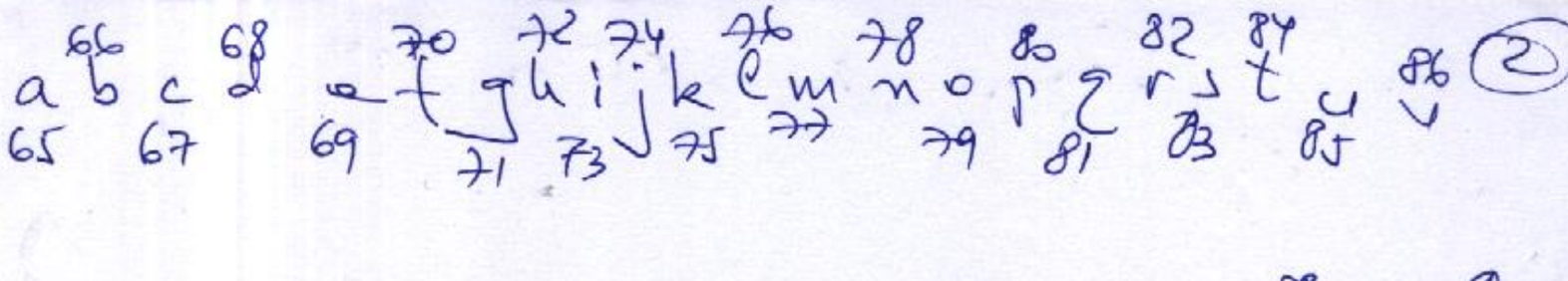
$(e, (p-1)(q-1)) = 1$ — $\varphi(pq)$

Și fiecare din respectivele valori V_i, calculăm $C_i \overset{not}{=} V_i^e \pmod{pq}$

Mesajul cifrat constă în succesiunea $C_1, C_2, C_3, \ldots$

ex: Să cifrăm textul „mi folosind criptosistemul RSA cu cheia de cifrare $pq = 6767$, $e = 7$ (folosind codul ASCII).

Sol:



Toate caracterele de mai jos sunt (mod 6767)

$f \longleftrightarrow 70$

$70^2 = 4900$

$70^4 = 4900^2 \equiv 684,$

deci

$70^7 \equiv 684 \cdot 4900 \cdot 70 \equiv 684 \cdot 4650 \equiv 110$

Deci valoarea cifrată corespunzătoare lui f e 110.

$m \longleftrightarrow 77$

$77^2 = 5929$

$77^4 = 5929^2 \equiv 5243,$

deci

$77^7 \equiv 5243 \cdot 5929 \cdot 77 \equiv 4916 \cdot 77 \equiv 6347.$

Deci, val. cifrată corresp. lui m e 6347

$i \longleftrightarrow 73$

$73^2 = 5329$

$73^4 = 5329^2 \equiv 3909,$

deci

$73^7 \equiv 3909 \cdot 5329 \cdot 73 \equiv 2235 \cdot 73 \equiv 747.$

Ca urmare, textul cifrat e

110 6347 747.

Cum decifrăm?

Știm $(e, (p-1)(q-1))$.

Atunci $e \in U(Z_{(p-1)(q-1)})$.

Fie f inversul lui e $(\mod (p-1)(q-1))$

Atunci $V \overset{n}{\equiv} V^{1+k(p-1)(q-1)} \overset{n}{\equiv} V^{ef} \overset{n}{\equiv} C^f$.

Ca urmare, pentru a decifra mesajul e suficient să calculăm C la puterea f inversul lui e $(\mod (p-1)(q-1))$

$$\frac{6600}{7} = 942 + \frac{6}{7} = 942 + \frac{1}{1+\frac{1}{6}}.$$

$R_1 = 942 + \frac{1}{1} = 943$.

Deci, inversul lui $7 \pmod{6600 = (67-1)(101-1)}$ este 943.

$943 = 512 + 256 + 128 + 32 + 8 + 4 + 2 + 1$

$110^2 = 12100 \equiv 5333$

$110^4 \equiv 5333^2 \equiv 5955$

$110^8 \equiv 5955^2 \equiv 2945$

$110^{16} \equiv 2945^2 \equiv 4498$

$110^{32} \equiv 4498^2 \equiv 5441$

$110^{64} \equiv 5441^2 \equiv 5623$

$110^{128} \equiv 5623^2 \equiv 2705$

$110^{256} \equiv 2705^2 \equiv 1898$

$110^{512} \equiv 1898^2 \equiv 2360.$

Deci, $110^{943} \equiv 110^{512} \cdot 110^{256} \cdot 110^{128} \cdot 110^{32} \cdot 110^{8} \cdot 110^{4} \cdot 110^{2} \cdot 110 \equiv$

$\equiv 2360 \cdot 1898 \cdot 2705 \cdot 5441 \cdot 2945 \cdot 5955 \cdot 5333 \cdot 110$

$\equiv 3560 \cdot 2145, 4668 \equiv 70 \overset{\text{ASCII}}{\longleftrightarrow} f$