Tema1_Criptografie

Ioana Ilie

21 February 2026

1 Exercițiul 1

a) Convertiți numărul 101100_2 în baza 10.

$$101100_2 = 1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0$$

$$= 32 + 0 + 8 + 4 + 0 + 0 = 44_{10}$$

b) Convertiți numărul $2D_{16}$ în baza 10.
(În baza 16, $D = 13$)

$$2D_{16} = 2 \cdot 16^1 + 13 \cdot 16^0$$

$$= 32 + 13 = 45_{10}$$

c) Convertiți numărul MAD_{26} în baza 10.
(În baza 26: $A = 0, B = 1, ..., Z = 25$)

$$M = 12, \quad A = 0, \quad D = 3$$

$$MAD_{26} = 12 \cdot 26^2 + 0 \cdot 26^1 + 3 \cdot 26^0$$

$$= 12 \cdot 676 + 0 + 3$$

$$= 8112 + 3 = 8115_{10}$$

d) Convertiți numărul 324_{10} în baza 26.
Împărțim succesiv la 26:

$$324 : 26 = 12 \text{ rest } 12$$

$$12 : 26 = 0 \text{ rest } 12$$

Deci cifrele sunt 12 și 12.

$$12 = M$$

$$324_{10} = MM_{26}$$

e) Înmulțiți numărul COD_{26} cu C_{26}.

$$\begin{array}{r} COD\times \\ \quad C \\ \hline FCG \end{array}$$

$$\begin{array}{r} (2)(14)(3)\times \\ \quad (2) \\ \hline (5)(2)(6) \end{array}$$

Verificare:

$$C = 2, \quad O = 14, \quad D = 3$$

$$COD_{26} = 2 \cdot 26^2 + 14 \cdot 26 + 3$$

$$= 2 \cdot 676 + 364 + 3$$

$$= 1352 + 364 + 3 = 1719_{10}$$

$$C_{26} = 2_{10}$$

$$1719 \cdot 2 = 3438_{10}$$

Acum convertim 3438 în baza 26:

$$3438 : 26 = 132 \text{ rest } 6$$

$$132 : 26 = 5 \text{ rest } 2$$

$$5 : 26 = 0 \text{ rest } 5$$

Deci obținem cifrele: $5, 2, 6$.

$$5 = F, \quad 2 = C, \quad 6 = G$$

$$COD \cdot C = FCG_{26}$$

2 Exercițiul 2

Calculați 9^{70} *mod* 71

Metoda pătratelor succesive ne dă următorul șir de egalități:

$$9^{70} = (9^{35})^2 = ((9^{17})^2 \cdot 9)^2 = (((9^8)^2 \cdot 9)^2 \cdot 9)^2 = ((((9^4)^2)^2 \cdot 9)^2 \cdot 9)^2 = (((((9^2)^2)^2)^2 \cdot 9)^2 \cdot 9)^2.$$

Deoarece facem calculele modulo 71, reducem la fiecare pas:

$$9^2 \equiv 10 \pmod{71}$$

$$9^4 \equiv 10^2 \equiv 29 \pmod{71}$$

$$9^8 \equiv 29^2 \equiv 60 \pmod{71}$$

$$9^{16} \equiv 60^2 \equiv 49 \pmod{71}$$

$$9^{32} \equiv 49^2 \equiv 56 \pmod{71}$$

$$9^{64} \equiv 56^2 \equiv 1 \pmod{71}.$$

Cum $70 = 64 + 4 + 2$, rezultă:

$$9^{70} \equiv 9^{64} \cdot 9^4 \cdot 9^2 \equiv 1 \cdot 29 \cdot 10 \equiv 290 \equiv 6 \pmod{71}.$$

$$\boxed{9^{70} \equiv 6 \pmod{71}}$$