

Temă - seminar 1

26.02.2025

1. Exemple din literatura unde este descrisă criptare / decriptare:

- "Bruma din Rue Morgue" - Edgar Allan Poe

↳ În povestirea "The Gold Bug" apare un mesaj criptat a treburie decriptat pentru a găsi o comoară.

- "Codul lui Da Vinci" - Dan Brown.

↳ apar diverse tehnici de criptare

2. cmmdc al număratoarelor numere scrise în baza 2:

$$(101000110101)_{(2)}; (100001111011)_{(2)}$$

$$\begin{array}{cccccccc} 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 11 & 10 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 \end{array} (2) = 1 \cdot 2^0 + 1 \cdot 2^2 + 1 \cdot 2^4 + 1 \cdot 2^5 + 1 \cdot 2^9 + 1 \cdot 2^{11}$$

$$= 1 + 4 + 16 + 32 + 512 + 2048$$

$$= 1 + 20 + 2560 + 32$$

$$= 53 + 2560$$

$$= 2613_{(10)}$$

$$\begin{array}{cccccccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 11 & 10 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 \end{array} (2) = 1 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^2 + 1 \cdot 2^4 + 1 \cdot 2^5 + 1 \cdot 2^6 + 1 \cdot 2^{11}$$

$$= 1 + 2 + 8 + 16 + 32 + 64 + 2048$$

$$= 1 + 10 + 48 + 64 + 2048$$

$$= 11 + 112 + 2048$$

$$= 11 + 2160$$

$$= 2171_{(10)}$$

$$2171 = 13 \cdot 167$$

$$2613 = 3 \cdot 13 \cdot 67$$

$$\Rightarrow \text{cmmdc}(2613, 2171) = 13$$

$$13_{(10)} = 1101_{(2)}$$

5. Tehin bari di base:

$$\begin{aligned} 7. a) \quad 100101(2) &= 1 \cdot 2^0 + 1 \cdot 2^2 + 1 \cdot 2^5 \\ &= 1 + 4 + 32 \\ &= 37(10) \end{aligned}$$

$$\begin{aligned} b) \quad 4E(16) &= 4(14)(16) = 4 \cdot 16^1 + 14 \cdot 16^0 \\ &= 64 + 14 \\ &= 78(10) \end{aligned}$$

$$\begin{aligned} c) \quad 221(8) &= 1 \cdot 8^0 + 2 \cdot 8^1 + 2 \cdot 8^2 \\ &= 1 + 16 + 2 \cdot 64 \\ &= 14 + 128 \\ &= 142(10) \end{aligned}$$

$$d) \quad 41(5) + 12(5) = 103(5)$$

6. Exponentiere modular:

$$\begin{aligned} 7. \quad 6^{28} \pmod{29} &= (6^2)^{14} = 7^{14} = (7^2)^7 = 20^7 = 20 \cdot 20^6 = 20 \cdot (20^2)^3 \\ &= 20 \cdot 23^3 = 20 \cdot 23 \cdot 23^2 \\ &= 25 \cdot 7 \\ &= 1 \end{aligned}$$

$$\begin{array}{r} 400 : 29 = 13 \\ 29 \\ \underline{110} \\ 239 \\ \underline{23} \\ 232 \\ \underline{23} \\ 0 \end{array}$$

$$\begin{array}{r} 460 : 29 = 15 \\ 29 \\ \underline{170} \\ 145 \\ \underline{29} \\ 0 \end{array}$$

$$\begin{array}{r} 529 : 29 = 18 \\ 29 \\ \underline{239} \\ 232 \\ \underline{23} \\ 0 \end{array}$$

$$\begin{array}{r} 175 : 29 = 6 \\ 29 \\ \underline{174} \\ 1 \\ \underline{29} \\ 0 \end{array}$$

3. număr de k cifre în baza b:
 $k \cdot \log_b k$