

# Criptografie - Tema 1

Popescu Paul - Constantin

Facultatea de Matematică

1. Identificați alte exemple din literatură unde sunt descrise procesele de criptare/decriptare.

Un exemplu ar fi romanul "Enigma" de Robert Harris, care urmărește încercările de a sparge cifrul Enigma folosit de naziști în Al Doilea Război Mondial. Un alt roman care detaliază procesul de decriptare a mesajelor codificate în timpul celui de-al Doilea Război Mondial este "Cryptonomicon" de Neal Stephenson.

2. Determinați cmmdc al următoarelor numere scrise în baza 2:  $101000110101_{(2)}$  și  $100001111011_{(2)}$ . Verificați egalitatea în baza 10.

$$101000110101_{(2)} = 1 \cdot 2^0 + 1 \cdot 2^2 + 1 \cdot 2^4 + 1 \cdot 2^5 + 1 \cdot 2^9 + 1 \cdot 2^{11} = 2613_{(10)}$$

$$100001111011_{(2)} = 1 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^3 + 1 \cdot 2^4 + 1 \cdot 2^5 + 1 \cdot 2^6 + 1 \cdot 2^{11} = 2171_{(10)}$$

$$2613 = 2171 \cdot 1 + 442$$

$$2171 = 442 \cdot 4 + 403$$

$$442 = 403 \cdot 1 + 39$$

$$403 = 39 \cdot 10 + 13$$

$$39 = 13 \cdot 3 + 0$$

$$13 = 1 \cdot 13 + 0$$

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

3. Estimați complexitatea pentru conversia unui număr de  $k$  biți în baza 10/într-o bază oarecare  $b$  și invers.

Conversia unui număr de  $k$  biți din baza 10 într-o bază oarecare  $b$ :

Pentru un număr  $N$  în baza 10, care poate fi descompus astfel:

$$N = q_0 b^0 + q_1 b^1 + \dots + q_m b^m$$

unde  $m$  reprezintă numărul de cifre în baza  $b$ , determinat prin relația:

$$m = \lfloor \log_b N \rfloor + 1$$

Dacă  $N$  este un număr reprezentat cu  $k$  biți, atunci valoarea sa maximă este aproximativ:  $N_{\max} \approx 10^k$ , astfel încât, înlocuind  $N$  cu  $10^k$ , obținem

$$m = \lfloor \log_b(10^k) \rfloor + 1 = \lfloor k \log_b 10 \rfloor + 1 \Rightarrow O(k \log_b 10) \text{ ceea ce duce la o complexitate liniară } O(k)$$

Conversia unui număr de  $k$  biți dintr-o bază oarecare  $b$  în baza 10:

Pentru această conversie,  $N$  poate fi scris ca

$$N = d_0 + d_1 \cdot b + d_2 \cdot b^2 + \dots + d_n \cdot b^n$$

Operațiile folosite sunt operații elementare, adunări și înmulțiri, ceea ce duce la concluzia că un număr de  $k$  biți în baza  $b$  conține aproximativ  $O(k)$  cifre.

4. Scrieți un cod care să realizeze conversia unui număr din baza  $b_1$  în baza  $b_2$  (unde  $b_1$  și  $b_2$  pot fi până la baza 26).

```
1      #include <iostream>
2      #include <string>
3      #include <cmath>
4      using namespace std;
5
6      int ConvertireInBaza10(string numar, int baza) {
7          int numarFinal = 0, putere = 1, cifra = 0;
8          for (int i = numar.size() - 1; i >= 0; i--) {
9              cifra = isdigit(numar[i]) ? numar[i] - '0' : numar[i] - 'A' + 10;
10             numarFinal += cifra * putere;
11             putere *= baza;
12         }
13         return numarFinal;
14     }
15
16     string ConvertireDinBaza10(int numar, int baza) {
17         string rezultat = "";
18         while (numar > 0) {
19             int cifra = numar % baza;
20             rezultat = (cifra < 10 ? char(cifra + '0') : char(cifra - 10 + 'A')) + rezultat;
21             numar /= baza;
22         }
23         if (rezultat.empty()) return "0";
24         else return rezultat;
25     }
26
27     int main() {
28         string numar;
29         int baza1, baza2;
30
31         cout << "Introduce, pe rand, un numar, prima baza si a doua baza:";
32         cin >> numar >> baza1 >> baza2;
33
34         if (baza1 < 2 || baza1 > 26 || baza2 < 2 || baza2 > 26) {
35             cout << "Eroare: Bazele trebuie sa fie intre 2 si 26!" << endl;
36             return 1;
37         }
38
39         int numarBazaB1 = ConvertireInBaza10(numar, baza1);
40         string numarBazaB2 = ConvertireDinBaza10(numarBazaB1, baza2);
41
42         cout << "Numar final: " << numarBazaB2 << endl;
43         return 0;
44     }
```

**Program:** Codul este inclus in folder-ul cu tema, numit `schimbari_de_baze.cpp`

**5. Schimbări de baze:**

1. Converteți numărul 100110 din baza 2 în baza 10.

$$100110_{(2)} = 0 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^2 + 0 \cdot 2^3 + 0 \cdot 2^4 + 1 \cdot 2^5 = 38_{(10)}$$

2. Converteți numărul 3D din baza 16 în baza 10.

$$3D_{(16)} = D \cdot 16^0 + 3 \cdot 16^1 = (13) \cdot 16^0 + 3 \cdot 16^1 = 61_{(10)}$$

3. Converteți numărul 201 din baza 6 în baza 4.

$$201_{(6)} = 1 \cdot 6^0 + 0 \cdot 6^1 + 2 \cdot 6^2 = 73_{(10)}$$

$$73 = 18 \cdot 4 + 1$$

$$18 = 4 \cdot 4 + 2$$

$$4 = 4 \cdot 1 + 0$$

$$1 = 4 \cdot 0 + 1$$

$$\Rightarrow 201_{(6)} = 73_{(10)} = 1021_{(4)}$$

4. Adunați numerele 54 și 13 în baza 7.

$$\begin{array}{r} 1 \\ 5 \quad 4_7 \\ + \quad 1 \quad 3_7 \\ \hline 1 \quad 0 \quad 0_7 \end{array}$$

$$\Rightarrow 54_{(7)} + 13_{(7)} = 100_{(7)}$$

- 6.** Calculați, folosind metoda de ridicare la putere prin pătrate succesive:  $12^{46} \bmod 47$

$$\begin{aligned} 12^{46} \bmod 47 &= (12^2)^{23} \bmod 47 = 144^{23} \bmod 47 = 3^{23} \bmod 47 = 3 \cdot 3^{22} \bmod 47 = \\ &= 3 \cdot (3^2)^{11} \bmod 47 = 3 \cdot 9^{11} \bmod 47 = 3 \cdot 9 \cdot 9^{10} \bmod 47 = 27 \cdot 9^{10} \bmod 47 = \\ &= 27 \cdot (9^2)^5 \bmod 47 = 27 \cdot 81^5 \bmod 47 = 27 \cdot 34^5 \bmod 47 = 27 \cdot 34 \cdot 34^4 \bmod 47 = \\ &= 918 \cdot 34^4 \bmod 47 = 25 \cdot 34^4 \bmod 47 = 25 \cdot (34^2)^2 \bmod 47 = 25 \cdot 1156^2 \bmod 47 = \\ &= 25 \cdot 28^2 \bmod 47 = 25 \cdot 784 \bmod 47 = 19600 \bmod 47 = 1 \end{aligned}$$