Nichita Bogdan Valentin

M531

TEMA 1

1. Identificați alte exemple din literatură unde este descrisă criptare/decriptare.

“Codul lui Da Vinci” – Dan Brown

(Se uită înăuntru. Era gol, cu excepţia cîtorva cioburi de sticlă. Nici urmă de papirus — fie el dizolvat sau nu. Rostogolindu-se, privi în sus, către Langdon. Sophie stătea alături, cu revolverul îndreptat spre el. Perplex, privi din nou criptex-ul şi abia atunci observă. Discurile nu mai erau aranjate la întîmplare. Pe cilindru se formase un cuvînt din cinci litere: "MĂRUL".)

"Cryptonomicon" – Neal Stephenson

2. Determinați cmmdc al următoarelor numere scrise în baza 2:

$(101000110101)_2$; $(100001111011)_2$. Verificați egalitatea în baza 10.

$(101000110101)_2 = 1 \cdot 2^{11} + 1 \cdot 2^9 + 1 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^2 + 1 \cdot 2^0 = 2613$

$(100001111011)_2 = 1 \cdot 2^{11} + 1 \cdot 2^9 + 1 \cdot 2^6 + 1 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^1 + 1 \cdot 2^0 = 2171$

$2613 - 2171 \cdot 1 = 442$

$2171 - 442 \cdot 4 = 2171 - 1768 = 403$

$442 - 403 \cdot 1 = 39$

$403 - 39 \cdot 10 = 403 - 390 = 13$

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

$CMMDC = 13 = 1 \cdot 2^3 + 1 \cdot 2^1 + 1 \cdot 2^0 = (1011)_2$

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

- trecerea unui număr de k biți în baza 10

$$n = \sum_{i=0}^{k-1} a_i 2^i \ , a_i \in \{0, 1\}, \forall i \ \in \overline{1, k-1}$$

Complexitate: **O(k)**

-trecerea unui număr din baza 10 în baza 2

$k = [\log_2 n] + 1$

Dacă numărul are m cifre => $n < 10^m$ deci $k \approx [\log_2 10^m] + 1 = m \cdot [\log_2 \ 10] + 1$

Complexitate: $O(m \cdot [\log_2 \ 10])$ = **O(k)**

-trecerea unui număr de k biți în baza b

trebuie să facem mai întai trecerea în baza 10, apoi împartim numarul obtinut la b păna când obținem câtul 0.

$n \leq \ 2^k - 1$

$$\log_b n + 1 \leq \log_b \left(2^k - 1\right) + 1 = \log_b 2^k + 1 = k \cdot \log_b 2 + 1 = \frac{k \cdot \log_2 2}{\log_2 b} + 1 = \frac{k}{\log_2 b} + 1$$

Complexitate: $O(k + k / \log_2 b)$= **O(k)**

-trecerea unui număr din baza b în baza 2

Dacă numărul are in baza b are m cifre atunci:

$$n = \sum_{i=0}^{m-1} a_i b^i \ , a_i \in \overline{0, b-1}, \forall i \ \in \overline{1, m-1}$$

Deci trecerea de la baza b în baza 10 are complexitatea O(m) = $O(k / \log_2 b)$

Trecerea de la baza 10 în baza 2 are complexitatea O(k)

Complexitate: $O(k / \log_2 b + k)$ = **O(k)**

5. Schimbări de baze Baza 16: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A (10), B (11) , C (12), D (13), E(14), F(15)

23. a) Convertiți numărul 101100 din baza 2 în baza 10.

$(101100)_2 = 1 \cdot 2^5 + 1 \cdot 2^3 + 1 \cdot 2^2 = 32 + 8 + 4 = 44$

b) Convertiți numărul 2D din baza 16 în baza 10.

$(2D)_{16} = 2 \cdot 16^1 + 13 \cdot 16^0 = 32 + 13 = 45$

c) Convertiți numărul 232 din baza 6 în baza 3.

$(232)_6 = 2 \cdot 6^2 + 3 \cdot 6^1 + 2 \cdot 6^0 = 72 + 18 + 2 = 92$

$92 = 30 \cdot 3 + 2$

$30 = 10 \cdot 3 + 0$

$10 = 3 \cdot 3 + 1$

$3 = 1 \cdot 3 + 0$

$1 = 0 \cdot 3 + 1$

$(232)_6 = (10102)_3$

d) Înmulțiți numerele 36 și 12 în baza 8.

$(36)_8 \cdot (12)_8 = (74+360)_8 = (454)_8$

6. Exponențiere modular

Calculați, folosind metoda de ridicare la putere prin pătrate succesive.

23. $4^{28} \pmod{19} \equiv 16^{14} \pmod{19} \equiv (-3)^{14} \pmod{19} \equiv 9^7 \pmod{19} \equiv 9 \cdot 81^3 \pmod{19} \equiv$
$\equiv 9 \cdot 5^3 \pmod{19} \equiv 9 \cdot 5 \cdot 5^2 \pmod{19} \equiv 45 \cdot 5^2 \pmod{19} \equiv 7 \cdot 5^2 \pmod{19} \equiv$
$\equiv 7 \cdot 25 \pmod{19} \equiv 7 \cdot 6 \pmod{19} \equiv 42 \pmod{19} \equiv 4 \pmod{19}$