Tema 2. Criptografie

(1) Scrieți un program care să convertească un număr din baza b_1 în baza b_2 și să permită baze de la 2 la 16.

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

(3) Schimbări de bază

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

15. (a) Convertiți numărul ~~1100~~ 10010 în baza 2 în baza 10

(b) Convertiți numărul 4A din baza 16 în baza 10.

(c) Convertiți numărul 125 din baza 7 în baza 4.

(d) Scădeți numerele 17 și 13 în baza 8.

(4) Exponențiere modulară

15. Calculează 55^{113} în mod 117.

1.

```
#include <iostream>
#include <string>
#include <algorithm>
#include <cmath>
using namespace std;

// funcția pentru a converti un caracter într-o valoare numerică
int charToValue (char c) {
    if (c >= '0' && c <= '9') return c - '0';
    if (c >= 'A' && c <= 'Z') return c - 'A' + 10;
    return -1;
}

// funcția pentru a converti o valoare numerică într-un caracter
char valueToChar (int value) {
    if (value >= 0 && value <= 9) return value + '0';
    if (value >= 10 && value <= 35) return value - 10 + 'A';
    return '?';
}
```

Scanat cu CamScanner

```
// funcție pentru a converti un număr dintr-o bază în baza 10
long long baseToDecimal (const string& num, int base){
    long long decimal = 0;
    for (char c: num){
        decimal = decimal * base + charToValue (c);
    } return decimal;
}
// funcția pentru a converti un număr din baza 10 într-o altă bază
string decimalToBase (long long decimal, int base){
    string result;
    while (decimal > 0){
        result. push_back (valueToChar (decimal % base));
        decimal /= base;
    } reverse (result. begin (), result. end ());
    return result;
}
// funcția principală pentru conversia din baza b1 în baza b2
string base b1 To Base b2 (const string & num, int b1, int b2){
    ~~throw invalid_argument ("Baza trebuie să fie între 2 și 26.");~~
    if (b1 < 2 || b1 > 26 || b2 < 2 || b2 > 26){
        throw invalid_argument ("Baza trebuie să fie între 2 și 26.");
    }
    long long decimal = baseToDecimal (num, b1);
    return decimalToBase (decimal, b2);
}
int main (){
    string num;
    int b1, b2;
    cout << "Introduceți numărul: "; cin >> num;
    cout << "Introduceți baza b1: "; cin >> b1;
    cout << "Introduceți baza b2: "; cin >> b2;
```

Scanat cu CamScanner

```
try {
    string result = baseB1ToBaseB2(num, b1, b2);
    cout << "Numarul " << num << " in baza " << b1 << " este " << result <<
" in baza " << b2 << endl;
} catch (const invalid_argument& e) {
    cout << e.what() << endl;
}
return 0;
}
```

3) a) $10010_2 = X_{10}$

$= 2^3 + 2^0 = 8 + 1 = 9_{10}$

b) $4A_{16} = X_{10}$

$4 \cdot 16^1 + 0 \cdot 16^0 = 64_{10}$

c) $125_7 = X_4$

$125_7 = X_{10}$

$= 5 \cdot 7^2 + 2 \cdot 7^1 + 1 \cdot 7^0 = 5 \cdot 49 + 2 \cdot 7 + 1 = 245 + 14 + 1 = 260_{10}$

$260_{10} = X_4$

$260 = 65 \cdot 4 + 0$

$65 = 16 \cdot 4 + 1$

$16 = 4 \cdot 4 + 0$

$4 = 4 \cdot 1 + 0$

$1 = 0 \cdot 4 + 1$

$X_4 = 10010$

d) $27_{10} = X_8 = 33_8$

$27 = 3 \cdot 8 + 3$

$3 = 0 \cdot 8 + 3$

$33 - 15 = 16_8$

$13_{10} = X_8 = 15_8$

$13 = 1 \cdot 8 + 5$

$1 = 0 \cdot 8 + 1$

Scanat cu CamScanner

4) 127 este număr prim

Th Fermat $\Rightarrow 53^{126} \equiv 1 \pmod{127}$

$53^{113} = 53^{126 \times k + r} = (53^{126})^k \cdot 53^r \equiv 1^k \cdot 53^r \equiv 53^r \pmod{127}$

$113 = 126 \cdot 0 + 113 \Rightarrow k = 0, r = 113$

$53^{113} \bmod 127$

$53^{163} \bmod 127$

127 -> prim => Th. Fermat $53^{126} \equiv 1 \pmod{127}$

$53^{113} = 53^{126 - 13} \bmod 127 = 53^{126} \cdot 53^{-13} \bmod 127$

$= 53^{-13} \bmod 127$

$(53^{-1})^{13} \bmod 127 \equiv 12^{13} \bmod 127$ ⊛

$1 = (53, 127) \Rightarrow 1 = u53 + v127 \Rightarrow 1 \bmod 127 = u53 \bmod 127$

$\Rightarrow u \equiv 53^{-1}$

$127 = 53 \cdot 2 + 21$

$53 = 21 \cdot 2 + 11$

$21 = 11 \cdot 1 + 10$

$11 = 10 \cdot 1 + 1$

$10 = 1 \cdot 10 + 0$

$\Rightarrow 1 = 11 - 10 = 11 - (21 - 11) =$

$= (53 - 2 \cdot 21) - (21 - (53 - 2 \cdot 21))$

$= 53 - 2 \cdot 21 - 21 + 53 - 2 \cdot 21$

$= 2 \cdot 53 - 5 \cdot 21$

$= 2 \cdot 53 - (127 - 2 \cdot 53) \cdot 5$

$= -5 \cdot 127 + 12 \cdot 53$

⊛ $12^{13} \bmod 127 \equiv 12^{12} \cdot 12 \bmod 127 \equiv (12^2)^6 \cdot 12 \bmod 127$

$\equiv (144)^6 \cdot 12 \bmod 127 \equiv 17^6 \cdot 12 \bmod 127 \equiv$

$\equiv (17^2)^3 \cdot 12 \bmod 127 \equiv 289^3 \cdot 12 \bmod 127 \equiv 35^3 \cdot 12 \bmod 127$

$\equiv 35^2 \cdot 35 \cdot 12 \bmod 127 \equiv 35^2 \cdot 420 \bmod 127 \equiv 35^2 \cdot 39 \bmod 127$

$\equiv 1225 \cdot 39 \bmod 127 \equiv 82 \cdot 39 \bmod 127 \equiv 3198 \bmod 127 \equiv 23 \bmod 127$

Scanat cu CamScanner