Tema 4. Criptografie

1. Realizați o comparație între algoritmii de primalitate studiați la seminar.

2. Studiați algoritmul de factorizare rho al lui Pollard și aplicați-l pentru 10909

3. Implementați algoritmul de factorizare Fermat.

4. Implementați algoritmul de factorizare QS.

5. Pentru exercițiile următoare, rezolvați exercițiul folosind Fermat sau QS din cheptul numerelor din fișierul Excel

15. Descompuneți numărul 14783 în factorii săi primi.

---

3)
```
#include <iostream>
#include <cmath>
using namespace std;
long long gcd ( long long a, long long b) {
        if (b==0) return a;
        return gcd ( b, a%b);
}
long long fermat_factor ( long long n) {
        if (n%2==0) return 2;
        long long a = ceil (sqrt(n));
        long long b2= a*a - n;
        long long b = sqrt (b2);
        while (b*b != b2) {
                a++;
                b2 = a*a -n;
                b = sqrt (b2);
        }
        long long p = a-b;
        long long q = a+b;
        return (p==1 || q==1) ? n : p;
}
```

```
int main(){
    long long n;
    cout << "Introduceti numarul pentru factorizare: "; cin >> n;
    long long factor = fermat_factor(n);
    if (factor == n)
        cout << n << " este prim " << endl;
    else
        cout << "Factorii primi ai lui " << n << " sunt " << factor << " si " << n/factor << " . " << endl;
    return 0;
}
```

4)
```
#include <iostream>
#include <vector>
#include <cmath>
#include <algorithm>
using namespace std;
typedef long long ll;
// functia pentru a calcula cel mai mic divizor prim al unui numar
ll smallestPrimeDivision (ll n){
    if (n <= 1) return -1;
    if (n % 2 == 0) return 2;
    for (ll i = 3; i * i <= n; i += 2){
        if (n % i == 0) return i;
    } return n;
}
// functia pentru a calcula valoarea functiei legendre
ll legendreSymbol (ll a, ll p){
    ll ls = 1;
    a = a % p;
    if (a == 0) return 0;
    while (a != 0){
        while (a % 2 == 0){
            a /= 2;
            ll r = p % 8;
            if (r == 3 || r == 5) ls *= -1;
        }
```

```
        swap(a,p);
        if(a%4==3 && p%4==3) ls *= -1;
        a %= p;
    } return (p==1) ? ls : 0;
}
// functia pentru a calcula valoarea functiei f(x) = (x + sqrt(n))^2 - n
ll f(ll x, ll n){
    return (x*x - n);
}
// functia pentru a calcula valorile lui f(x) pentru un interval dat
vector<ll> calculateFunctionValues(ll n, ll start, ll end){
    vector<ll> values;
    for(ll i = start; i <= end; i++){
        values.push_back(f(i,n));
    } return values;
}
// functia pentru a gasi factorii primi ai unui numar compus folosind algoritmul QS
void quadricSieveFactorization(ll n){
    ll sqrt_n = sqrt(n);
    if(sqrt_n * sqrt_n == n){
        cout << "Numarul " << n << " este patrat perfect " << endl;
        return;
    }
    ll x = sqrt(n) + 1;
    vector<ll> primes;
    vector<ll> factors;
    while(true){
        ll p = smallPrimeDivisor(f(x,n));
        if(p != 1 && p != n){
            factors.push_back(p);
            if(factors.size() >= 2) break;
        } ++x;
    }
    if(factors.size() < 2){
        cout << "Algoritmul nu a putut gasi factorii " << endl;
        return;
    }
```

```
    ll a = factors[0];
    ll b = factors[1];
    ll p = a*b;
    ll q = n/p;
    cout << "Factorii primi ai lui: " << n << " sunt " << p << " si " << q << ". " << endl;
}
int main(){
    ll n; cout << "Introduceti numarul pt. factorizare: "; cin >> n;
    quadraticSieveFactorization(n);
    return 0;
}
```

5) $14783 = n$ Fermat

$\lceil \sqrt{n} \rceil = \sqrt{14783}$ | 133

1

$133 \cdot 1 = 39$

147

$263 \cdot 3 = 789$

39

883

789

94

$t = \lceil \sqrt{n} \rceil + 1 = 134$

$t^2 - n = 17956 - 14783 = 3173 \neq \square^2$

$t = 135$

$t^2 - n = 18225 - 14783 = 3442 \neq \square^2$

$t = 136$

$t^2 - n = 18496 - 14783 = 3713 \neq \square^2$

$t = 137 \quad t^2 - n = 18769 - 14783 = 3986 \neq \square^2$

$t = 138 \quad t^2 - n = 19044 - 14783 = 4261 \neq \square^2$

$t = 139 \quad t^2 - n = 19321 - 14783 = 4538 \neq \square^2$

QS: $n = 14783$

$\sqrt{n} = \sqrt{14783}$ | 133

94

$F(1) = 134^2 - 14783 = 3173$

$F(2) = 135^2 - 14783 = 3442$

$F(3) = 136^2 - 14783 = 3986$