Tema 4 Criptografie

2. Algoritmul rho al lui Pollard este un algoritm de factorizare utilizat pentru a găsi factorii primi ai unui număr întreg compus. Acesta este un algoritm euristic, adică nu garantează întotdeauna găsirea factorilor într-un timp rezonabil, dar în general are o performanță bună pentru numere medii și mari.

Pașii de funcționare:

1. Se alege o funcție $f(x)$ cu valori întregi aleatoare sau pseudoaleatoare, care poate fi exprimată matematic sub formă de funcție modulară, cum ar fi: $f(x) = x^2 + c \pmod n$, c - constantă.
2. Se aleg două valori x_1 și x_2.
3. Se calculează secvența de valori $x_1, x_2, x_3, \ldots$ folosind funcția $f(x)$.
4. Calculăm c.m.m.d.c, d

$$d = \gcd(|x_i - x_j|, n)$$

5. $d \neq 1$, $d \neq n$ $\Rightarrow$ d - factor al lui n

Pentru 10909

1. $f(x) = x^2 + 1 \pmod n$
2. $x_1 = 2 \quad x_2 = 2$
3. secvența de valori: 2, 5, 26, 677, ...

4. c.m.m.d.c

$x_1 = f(x_1) = 2^2 + 1 \mod 10909 = 5$

$x_2 = f(x_2) = 5^2 + 1 \mod 10909 = 26$

$x_3 = f(x_3) = 26^2 + 1 \mod 10909 = 677$

$x_4 = f(x_4) = 677^2 + 1 \mod 10909 = 8635$

$10909 : d = \gcd(|x_i - x_j|, 10909)$

$i = 1 \quad j = 2 \Rightarrow |5 - 26| = 21$

$\gcd(21, 10909) = 1$

⋮ continuăm până găsim $\neq 1$ sau 10909

3. Fermat.cpp 4. QS.cpp

5. (20)

Pentru a descompune numărul 15823 în factori primi, vom folosi alg. Fermat. Acest algoritm se bazează pe faptul că fiecare număr intreg pozitiv poate fi exprimat ca diferența dintre două pp consecutive.

Pas 1: Calculăm pătratul numărului și păstrăm rezultatul într-o variabilă "square_number", care va reprezenta baza pentru căutarea diferenței de pătrate perfecte.

Pas 2: Inițializăm a variabilă "root" la valoarea radicalului pătratului numărului. "Anunțăm" partea fracționară și

adăugăm 1 dacă radicalul este nr întreg

Pas 3: Într-o buclă, vom incrementa "naat" și vom verifica dacă diferența dintre pătratul lui "naat" și "square_number" este un pătrat perf. Dacă este, vom opri bucla și vom considera că am găsit factorii primi ai numărului.

Numărul nostru este prim.