Отчет по лабораторной работе № 6. Разложение чисел на множители

дисциплина: Математические основы защиты информации и информационной безопасности

Наливайко Сергей Максимович

Содержание

# Цель работы

Научиться реализовывать алгоритмы разложения чисел на множители.

# Задание

* Реализовать алгоритм, реализующий р-метод Полларда.

# Выполнение лабораторной работы

## Реализация алгоритма разложения чисел на множители

Реализуем алгоритм разложения чисел на множители на языке программирования C++.

Код функции разложения чисел на множители:

uint64\_t pollards\_method(uint64\_t n, uint64\_t c, uint64\_t (\*f)(uint64\_t)) {  
  
 uint64\_t a = c, b = 1, p = -1;  
  
 while (true) {  
 uint64\_t d;  
 b = f(b) % n;  
 a = f(f(a) % n) % n;  
 d = gcd(ABS(a, b), n);  
 if (d > 1 && d < n) {  
 p = d;  
 } else if (d == 1)  
 continue;  
 break;  
 }  
 return p;  
}

Полный листинг программного кода представлен в файле main.cpp (архив lab06, директория src).

Скомпилируем и запустим программу fig. 1.

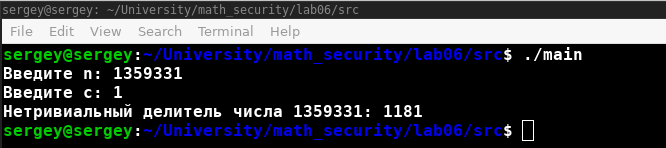


Figure 1: Разложение чисел на множители

# Выводы

В ходе лабораторной работы мы реализовывали алгоритмы разложения чисел на множители.