Отчет по лабораторной работе № 7. Дискретное логарифмирование в конечном поле

дисциплина: Математические основы защиты информации и информационной безопасности

Наливайко Сергей Максимович

Содержание

1 Цель работы

Познакомиться с дискретным логарифмированием в конечном поле и реализовать алгоритм, реализующий p-метод Полларда.

2 Задание

- Реализовать алгоритм, реализующий p-метод Полларда для задач дискретного логарифмирования.

3 Выполнение лабораторной работы

3.1 Реализация алгоритма дискретного логарифмирования

Реализуем алгоритм, реализующий p-метод Полларда для задач дискретного логарифмирования на языке программирования C++.

Код функций данного алгоритма:

```
long long f(long long x, long long& a, long long& b,
    long long alpha, long long beta, long long N, long long r) {
    if (x < r) {
        x = alpha * x % N;
        a = (a + 1) % r;
    } else {
        x = beta * x % N;
        b = (b + 1) % r;
    }
    return x;
}

long long pollard_method(long long p, long long alpha, long long beta, lo
    long long a1, b1, a2, b2, c = 4, d = 4;
    a1 = b1 = b2 = a2 = 2;
    cout << "i" << setw(6) << "c" << setw(6) << "a1" << setw(6) << "b1"
         << setw(6) << "d" << setw(6) << "a2" << setw(6) << "b2" << "\n";
```

```
    for(int i = 1; i < p - 1; ++i) {
        c = f(c, a1, b1, alpha, beta, p, r);
        d = f(f(d, a2, b2, alpha, beta, p, r), a2, b2, alpha, beta, p, r)
        cout << i << setw(6) << c << setw(6) << a1 << setw(6) << b1
             << setw(6) << d << setw(6) << a2 << setw(6) << b2 << "\n";
        if(c == d){
            for(long long j = 1; j < p; ++j) {
                long long tmp = (a1 + b1 * j - a2 - b2 * j) % r;
                if(tmp == 0) {
                    cout << "Уравнение: " << a1 << " + " << b1 << "x" <<
                         << a2 << " + " << b2 << "x (mod " << r << ")\n";
                    return j;
                }
            }
        }
    }
    return 0;
}
```

Полный листинг программного кода представлен в файле main.cpp (архив lab07, директория src).

Скомпилируем и запустим программу fig. 3.1.

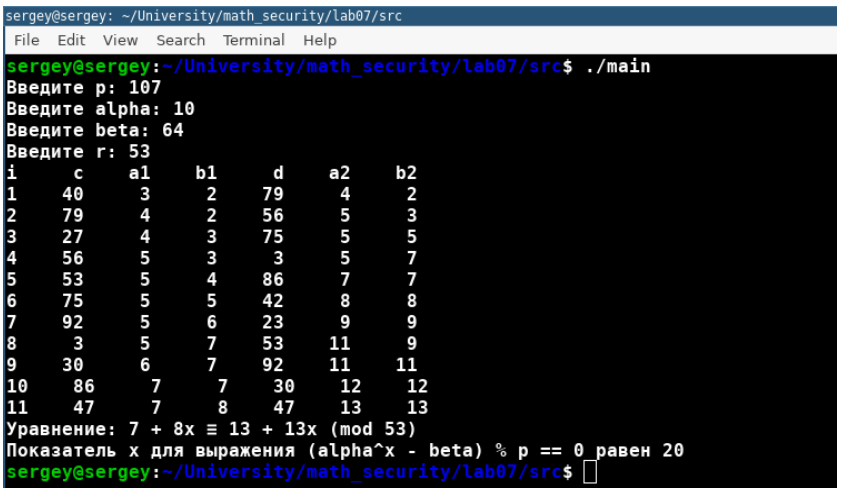

Figure 3.1: Дискретное логарифмирование в конечном поле

4 Выводы

В ходе работы мы познакомились с дискретным логарифмированием в конечном поле и реализовали алгоритм, реализующий p-метод Полларда.