Математические основы защиты информации и информационной безопасности. Отчет по лабораторной работе №7

Шифрование гаммированием

Терентьев Егор Дмитриевич 1132236902

Содержание

# 1 Цель работы

Освоить на практике дискретное логарифмирование в конечном поле.

# 2 Выполнение лабораторной работы

Требуется реализовать:

1. Алгоритм, реализующий p-метод Полларда для задач дискретного логарифмирования

## 2.1 p-метод Полларда

Основные шаги:

Вход: Простое число p, числа a порядка r по модулю p, целое число b, 1< b < p отображение f, обладающее сжимающими свойствами и сохраняющее вычислимость логарифма Выход: Показатель x, Для которого a^x Тождественно = b (mod p), если такой показатель существует 1. Выбрать произвольные числа u, v и положить c <- a^u \* b^v (mod p), d <- c 2. Выполнять c <- f(c)(mod p), d <- f(f(d))(mod p), вычисляя при этом логарифмы для c и d как линейные функции от x по модулю r, до получения равенства c тождественно = d(mod p) 3. Приравняв логарифмы для c и d, вычислить логарифм x решением сравнения по модулю r. Результат: x или “Решения нет”

Чтобы реализовать программу был написал след. код на python:

1. Функция, реализующая p-метод Полларда
2. Функция нахождения НОД
3. Расширенный алгоритм Евклида для вычисления модульного обратного элемента fig. 1.



Figure 1: main\_func

Выходные значения программы fig. 2.

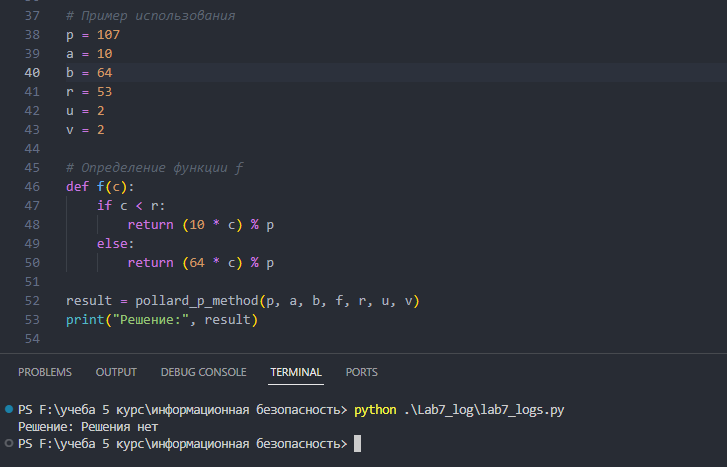


Figure 2: output

# 3 Выводы

В результате выполнения работы я освоил на практике дискретное логарифмирование в конечном поле.

# 4 Список литературы

1. Методические материалы курса