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

Шифрование гаммированием

Серенко Данил Сергеевич 1132236895

Содержание

# Цель работы

Освоить на практике дискретное логарифмирование в конечном поле.

# Выполнение лабораторной работы

Требуется реализовать:

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

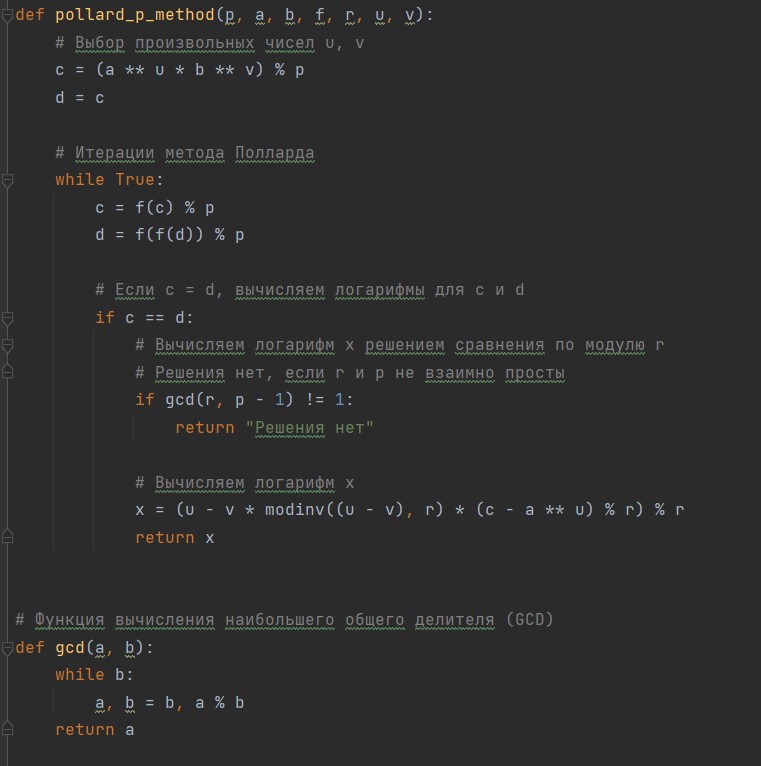
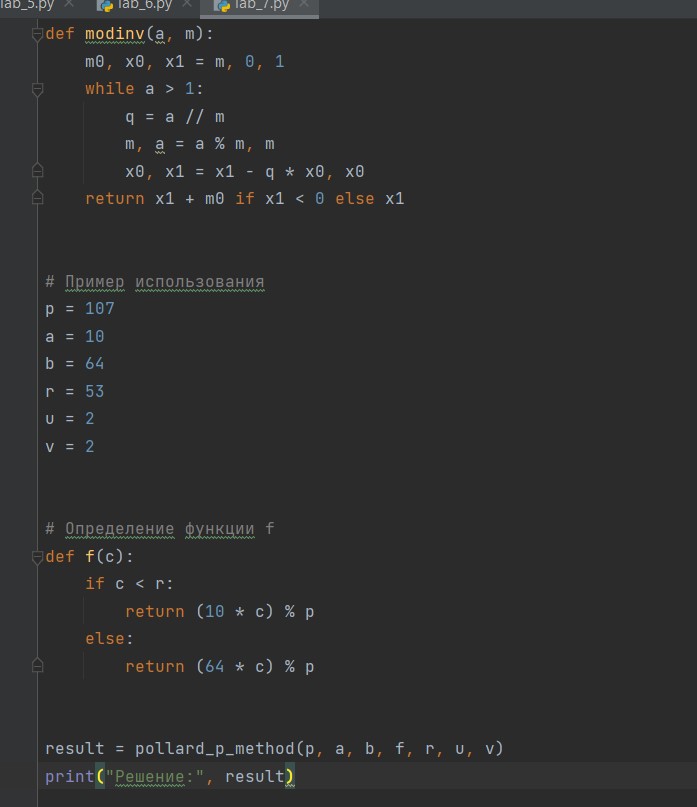
## p-метод Полларда

Основные шаги:

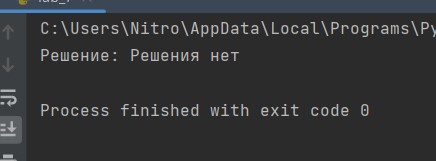
Вход: Простое число p, числа a порядка r по модулю p, целое число b, 1< b < p отображение f, обладающее сжимающими свойствами и сохраняющее вычислимость логарифма Выход: Показатель x, Для которого a^x Тождественно = b (mod p), если такой показатель существует 1. Выбрать произвольные числа u, v и положить 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.

Выходные значения программы.



output

# Выводы

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

# Список литературы

1. Методические материалы курса