Математические основы защиты информации и информационной безопасности

Отчет по лабораторной работе № 7

Меньшов Иван Сергеевич НПМмд-02-21

Содержание

# Цель работы

Изучить алгоитм реализующий P-метод Полларда для задач дискретного логорифмирования.

# Теоретические сведения

## P-метод Полларда для задач дискретного логорифмирования

Вход: Простое число p, число а порядка r по модулю р, целое число b, 1 < b <p; отображение f, обладающее сжимающими свойствами и сохраняющее вычислимость логарифма.

Выход. Показатель x, для которого аx = b (mod p), если такой показатель существует.

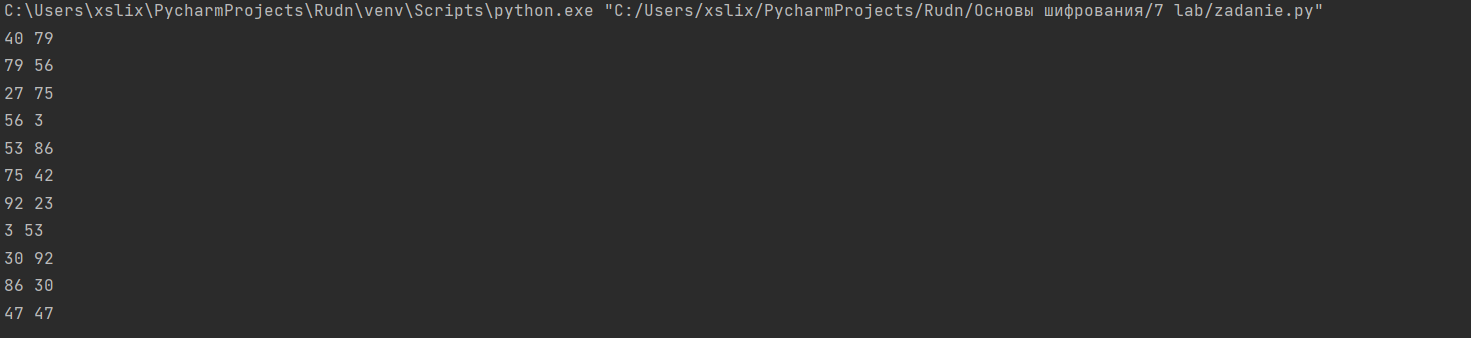
1. Выбрать произвольные целые числа u, v и положить с = аu bv (mod p), d = с.
2. Выполнять с = f(c)(mod p), d = f(f(d))(mod p), вычисляя при этом логарифмы для с и d как линейные функции от х по модулю r, до получения равенства с = d (mod p).
3. Приравняв логарифмы для c и d, вычислить логарифм х решением сравнения по модулю r. Результат: х или "Решений не

# Выполнение работы

## Реализация алгоритма на языке Python

a = 10  
b = 64  
p = 107  
u\_0 = 2  
v\_0 = 2  
  
  
def f(c, a, b, p):  
 if c < (p // 2):  
 return a \* c  
 else:  
 return b \* c  
  
  
c = (a \*\* u\_0 \* b \*\* v\_0) % p  
d = c  
  
while True:  
 c = f(c, a, b, p) % p  
 d = f(f(d, a, b, p) % p, a, b, p) % p  
 print(c, d)  
 if c == d % p:  
 break

## Контрольный пример



P-метод Полларда для задач дискретного логорифмирования

# Выводы

Мной было изучен алгоитм реализующий P-метод Полларда для задач дискретного логорифмирования. К сожаленю данный алгоритм нуждается в доработке - этот вывод был сделан преподавателем на семинаре.

# Список литературы

1. [Инструкция к лабораторной работе №7](https://esystem.rudn.ru/pluginfile.php/1283466/mod_folder/content/0/lab07.pdf?forcedownload=1)