

Математические основы защиты информации и информационной безопасности

Отчет по лабораторной работе № 7

Меньшов Иван Сергеевич НПМмд-02-21

Содержание

1	Цель работы	4
2	Теоретические сведения	5
2.1	Р-метод Полларда для задач дискретного логорифмирования . .	5
3	Выполнение работы	6
3.1	Реализация алгоритма на языке Python	6
3.2	Контрольный пример	7
4	Выводы	8
	Список литературы	9

List of Figures

3.1	Р-метод Полларда для задач дискретного логорифмирования . .	7
-----	---	---

1 Цель работы

Изучить алгоритм реализующий Р-метод Полларда для задач дискретного логарифмирования.

2 Теоретические сведения

2.1 Р-метод Полларда для задач дискретного логорифмирования

Вход: Простое число p , число 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 $a^x = b \pmod{p}$, если такой показатель существует.

1. Выбрать произвольные целые числа u, v и положить $c = a^u b^v \pmod{p}$, $d = c$.
2. Выполнять $c = f(c) \pmod{p}$, $d = f(f(d)) \pmod{p}$, вычисляя при этом логарифмы для c и d как линейные функции от x по модулю r , до получения равенства $c = d \pmod{p}$.
3. Приравняв логарифмы для c и d , вычислить логарифм x решением сравнения по модулю r . Результат: x или "Решений не

3 Выполнение работы

3.1 Реализация алгоритма на языке Python

```
a = 10
b = 64
p = 107
u_0 = 2
v_0 = 2

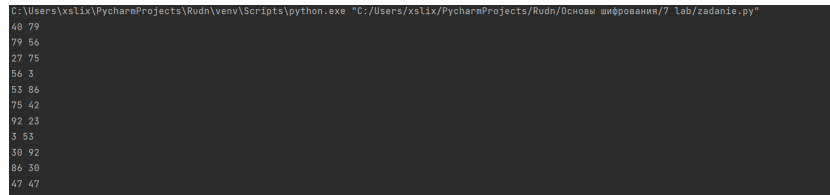
def f(c, a, b, p):
    if c < (p // 2):
        return a * c
    else:
        return b * c

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
```

3.2 Контрольный пример



```
C:\Users\xsl1x\PycharmProjects\Rudn\venv\Scripts\python.exe "C:/Users/xsl1x/PycharmProjects/Rudn/Основы шифрования/7_lab/zadanie.py"
40 79
79 56
27 75
56 3
53 86
75 42
92 23
3 53
30 92
86 30
47 47
```

Figure 3.1: Р-метод Полларда для задач дискретного логорифмирования

4 Выводы

Мной было изучен алгоритм реализующий Р-метод Полларда для задач дискретного логарифмирования. К сожалению данный алгоритм нуждается в доработке - этот вывод был сделан преподавателем на семинаре.

Список литературы

1. Инструкция к лабораторной работе №7