Лабораторная работа №7

Математические основы защиты информации и информационной безопасности

Полиенко Анастасия Николаевна

26 сентября 2023

Российский университет дружбы народов, Москва, Россия

НПМмд-02-23

Дискретное логарифмирование в конечном поле

Цель лабораторной работы

Изучить дискретное логарифмирование в конечном поле.

Задачи лабораторной работы

Реализовать алгоритм p-метода Полларда.

Ход лабораторной работы

Код

Реализуем алгоритм алгоритм p-метода Полларда.

```
def f(x, u, v):
    if x < 53:
        return (10 * x) % 107, u + 1, v
    return (64 * x) % 107, u, v + 1

p = 107
a = 10
b = 64
r = 53
u = 2; v = 2
u_c = 2; v_c = 2
u_d = 2; v_d = 2

c = ((a ** u) * (b ** v)) % p
d = c

c, u_c, v_c = f(c, u_c, v_c)
d, u_d, v_d = f(f(d, u_d, v_d)[0], f(d, u_d, v_d)[1], f(d, u_d, v_d)[2])

while c % p != d % p:
    c, u_c, v_c = f(c, u_c, v_c)
    d, u_d, v_d = f(f(d, u_d, v_d)[0], f(d, u_d, v_d)[1], f(d, u_d, v_d)[2])
    print(c, u_c, v_c, d, u_d, v_d)

x = 1
while (u_c + v_c * x) % r != (u_d + v_d * x) % r:
    x += 1

print("x =", x)
```

```
79 4 2 56 5 3
27 4 3 75 5 5
56 5 3 3 5 7
53 5 4 86 7 7
75 5 5 42 8 8
92 5 6 23 9 9
```

Выводы

Изучила дискретное логарифмирование в конечном поле.