Отчёт по лабораторной работе №7
Дискретное логарифмирование в конечном поле

Дисциплина: Математические основы защиты информации и информационной безопасности

Студент: Агеева Анастасия Сергеевна, 1032212304
Группа: НФИмд-02-21
Преподаватель: д-р.ф.-м.н., проф. Кулябов Дмитрий Сергеевич

25 декабря, 2021, Москва

Прагматика

Прагматика данной лабораторной работы

- В рамках дисциплины “Математические основы защиты информации и информационной безопасности” нам необходимо изучить ее разделы.
- Данная работа необходима для более глубоко и детального понимания работы алгоритмов шифрования.

Цель

Цель выполнения данной лабораторной работы

- Цель данной лабораторной работы изучение задачи и алгоритмов дискретного логарифмирования в конечном поле.

Задачи

Задачи выполнения данной лабораторной работы

1. Реализовать программно алгоритм, реализующий p-метод Полларда для задач дискретного логарифмирования.

Результаты выполнения данной лабораторной работы

Реализация p-метод Полларда

In [1]:
```
def f(c, u, v):
    if c < 53:
        return 10*c%107, u+1, v
    else:
        return 64*c%107, u, v+1
```

Figure 1: Сжимающая функция f

In [3]:
```
def discrlog(p, a, r, b, u, v):
    c = a**u * b**v % p
    d = c
    uc, vc = u, v
    ud, vd = u, v
    c, uc, vc = f(c, uc, vc)
    c %= p
    d, ud, vd = f(*f(d, ud, vd))
    d %= p
    while (c-d)%p != 0:
        c, uc, vc = f(c, uc, vc)
        c %= p
        d, ud, vd = f(*f(d, ud, vd))
        d %= p
    v = vc - vd
    u = ud - uc
    d, x, y = extended_euclid(v, r)
    while d != 1:
        v /= d
        u /= d
        r /= d
        d, x, y = extended_euclid(v, r)
    return x*u%r
```

In [4]:
```
discrlog(107, 10, 53, 64, 2, 2)
```

Out[4]: 20.0

Figure 2: Результаты p-метода Полларда

Выводы

- Исходя из теоретических сведений, программа выполнена без ошибок, чему свидетельствуют полученные результаты.
- В ходе данной лабораторной работы я реализовала программно $/rho$-метод Полларда для задач дискретного логарифмирования.