РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

ОТЧЕТ ПО

ЛАБОРАТОРНОЙ РАБОТЕ №7

дисциплина: Математические основы защиты информации и информационной безопасности

Студент: Хиссен Али Уэддей
Группа: НПМмд-02-20
Ст. билет № 1032209306

Цель работы

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

Теоретические часть

Алгоритм, реализующий p-метод Полларда.

Теоретические сведения P-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 ax = b (mod p), если такой показатель существует.

1. Выбрать произвольные целые числа u, v и положить c = a^u^.b^v^(modp), 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 = d (mod p).
3. Приравняв логарифмы для c и d, вычислить логарифм x решением сравнения по модулю r. Результат: x или "Решений не

програмная часть

```
#definition de la fonction f
a,b,p=10,64,107
u,v=2,2


def f(c):

    if c<p//2 :
```

```
        return (a*c)%p
    else:
        return (b*c)%p
c=(a**u*b**v)%p
d=c
while(True):
    print (c,d)
    c=f(c)%p

    d=f(f(d))%p
    if c==d:
        print (c,d)
        break
```

результат при заданом некоторый аргумент

```
4 4
40 79
79 56
27 75
56 3
53 86
75 42
92 23
3 53
30 92
86 30
47 47
```

вывод Мы изучали алгоитм реализующий P-метод Полларда для задач дискретного логорифмирования .Данная лабораторная работа нужна подправка