Математические основы защиты информации и информационной безопасности.

Лабораторная работа №7.

Сапёров Максим Александрович.

Содержание

List of Figures

List of Tables

1 Цель работы

Освоить на практике вычисление дискретного логарифма методом ро-Полларда

2 Задание

1. Реализовать вычисление дискретного логарифма методом ро-Полларда

3 Выполнение лабораторной работы

Написал код для вычисления дискретного логарифма

```python
import sys

def ext_euclid(a, b):
    if b == 0:
        return a, 1, 0
    else:
        d, xx, yy = ext_euclid(b, a % b)
        x = yy
        y = xx - (a / b) * yy
        return d, x, y


def inverse(a, n):
    return ext_euclid(a, n)[1]


def xab(x, a, b, G, H, P, Q):
    sub = x % 3 # Subsets

    if sub == 0:
        x = x*G % P
        a = (a+1) % Q

    if sub == 1:
        x = x * H % P
        b = (b + 1) % Q

    if sub == 2:
        x = x*x % P
        a = a*2 % Q
        b = b*2 % Q

    return x, a, b
```

Figure 3.1: Код для вычисления дискретного логарифма

```python
def pollard(G, H, P):
    Q = (P - 1) / 2


    x = G*H
    a = 1
    b = 1

    X = x
    A = int(a)
    B = int(b)

    for i in range(1, P):
        x, a, b = xab(x, a, b, G, H, P, Q)
        X, A, B = xab(X, A, B, G, H, P, Q)
        X, A, B = xab(X, A, B, G, H, P, Q)

        if x == X:
            break


    nom = int(a-A)
    denom = int(B-b)

    print (nom, denom)

    res = (inverse(denom, int(Q) * nom) % int(Q))

    if verify(G, H, P, res):
        return res

    return int(res + Q)


def verify(g, h, p, x):
    return pow(int(g), int(x), p) == h
```

Figure 3.2: Код для вычисления дискретного логарифма

Код для примеров

```python
g=int(64)
h=int(10)
p=int(107)


print ("g =",g)
print ("h =",h)
print ("p =",p)




print (h,"=",g,"^x (mod",p,")")
print ("\n==============")

x = int(pollard(g,h,p))
print ("Solution x=",x)
print ("Solution:",verify(g, h, p, x))
```

```
g = 64
h = 10
p = 107
10 = 64 ^x (mod 107 )

==============
16 2
Solution x= 54
Solution: False
```

Figure 3.3: Код для примеров

4 Выводы

Освоил на практике вычисление дискретного логарифма методов ро-Полларда