

Отчёт по лабораторной работе 7

Кочетов Андрей Владимирович

08 декабря, 2022

Реализовать алгоритм.

Лабораторная работа подразумевает написание программы на языке python, которая реализует логарифмирование в конечном поле

Выполнение лабораторной работы

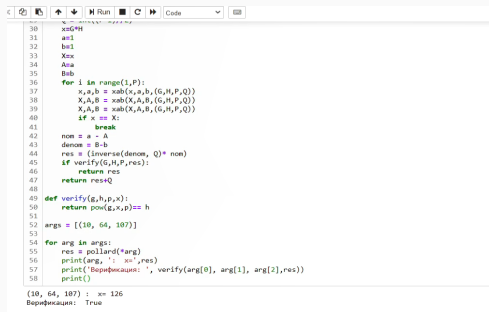
Выполнение лабораторной работы

1. Начинаю реализовывать код

```
In [ ]: 1 def euclid_extended(a, b):
2     if b == 0:
3         return a, 1, 0
4     else:
5         d, xx, yy = euclid_extended(b, a%b)
6         x = yy
7         y = xx - (a // b) * yy
8         return d, x, y
9
10 def inverse(a, n):
11     return (euclid_extended(a, n)[1])
12
13 def xab(x, a, b, x_swap):
14     (G, H, P, Q) = x_swap
15     sub = x % 3
16     if sub == 0:
17         x = x * x_swap[0] % x_swap[2]
18         a = (a+1) % Q
19     if sub == 1:
20         x = x * x_swap[1] % x_swap[2]
21         b = (b+1) % x_swap[2]
22     if sub == 2:
23         x = x * x_swap[2]
24         a = a * 2 % x_swap[3]
25         b = b * 2 % x_swap[3]
26     return x, a, b
27
28 def
```

Figure 1: рис.1. Начало

2. Закончил код, проверил работоспособность.



```
30 xabGH
31 a=1
32 b=1
33 X=x
34 A=a
35 B=b
36 for i in range(1,P):
37     X,a,b = xab(x,a,b,(G,H,P,Q))
38     X,A,B = xab(X,A,B,(G,H,P,Q))
39     X,A,B = xab(X,A,B,(G,H,P,Q))
40     if x == X:
41         break
42     nom = a - A
43     denom = B-b
44     res = (inverse(denom, Q)* nom)
45     if verify(G,H,P,res):
46         return res
47     return res+Q
48
49 def verify(g,h,p,x):
50     return pow(g,x,p)== h
51
52 args = [(10, 64, 107)]
53
54 for arg in args:
55     res = pollard(*arg)
56     print(arg, ': x=',res)
57     print('Верификация: ', verify(arg[0], arg[1], arg[2],res))
58     print()
```

(10, 64, 107) : x= 126
Верификация: True

Figure 2: рис.2. Запуск

Выводы

Я написал программный код, который реализует логарифмирование в конечном поле.

Спасибо за внимание!