Лабораторная работа № 4

Выполнил Казачинский Глеб, 3 курс 6 группа

№ вар.	p	q	e	X1	Y2
11	148250911826341	202614773351219	127764707833222901558553896 71	269266957344327693125367581 39	706085475679501894004246456 3

```
1. def gcdex(a, b):
2.     if b == 0:
3.         return a, 1, 0
4.     else:
5.         d, x, y = gcdex(b, a % b)
6.         return d, y, x - y * (a // b)
7.
8.
9. def fast_p(x, n, m):
10.     res = 1
11.     while n:
12.         if n % 2:
13.             res = res * x % m
14.         x = (x ** 2) % m
15.         n = n // 2
16.     return res
17.
18.
19. p = 148250911826341
20. q = 202614773351219
21. e = 127764707833222901558553896 71
22. X1 = 269266957344327693125367581 39
23. Y2 = 706085475679501894004246456 3
24.
25. n = p * q
26. fi = (p - 1) * (q - 1)
27.
28. gcd, x, y = gcdex(e, fi)
29.
30. d = 0
```

```
31. if gcd == 1:
32.     d = x % fi
33.     print('d: ', d)
34.
35. Y1 = fast_p(X1, e, n)
36. print('Y1: ', Y1)
37.
38. X1_ = fast_p(Y1, d, n)
39. print('X1_: ', X1_)
40. print('X1 - X1_ :', X1 - X1_)
41.
42.
43. X2 = fast_p(Y2, d, n)
44. print('X2: ', X2)
```

Результаты:

```
d:  14873008553280748334153343991
Y1:  28885559050485773364835147196
X1_:  26926695734432769312536758139
X1 - X1_ : 0
X2:  24325122744076232534395127334
```