Лабораторная работа № 5

Выполнил Казачинский Глеб, 3 курс 6 группа

```
1. import random
2. import hashlib
3.
4.
5. def gcdex(a, b):
6.     if b == 0:
7.         return a, 1, 0
8.     else:
9.         d, x, y = gcdex(b, a % b)
10.         return d, y, x - y * (a // b)
11.
12.
13. def fast_p(x, n, m):
14.     res = 1
15.     while n:
16.         if n % 2:
17.             res = res * x % m
18.         x = (x ** 2) % m
19.         n = n // 2
20.     return res
21.
22.
23. def gen(q):
24.     while True:
25.         R = random.randint(0, 4 * (q + 1))
26.         R += R % 2
27.         p = R * q + 1
28.         if not (fast_p(2, q * R, p) != 1 or fast_p(2, R, p) == 1):
29.             print('R :', R)
30.             print('p :', p)
31.             break
32.     g = 1
33.     while g == 1:
```

```
        x = random.randint(1, p - 1)
        g = fast_p(x, R, p)
    print('x:', x)
    print('g:', g)
    d = random.randint(1, q - 1)
    e = fast_p(g, d, p)
    return p, q, g, e, d


def hash(m):
    hash_ = hashlib.sha256()
    hash_.update(m.encode())
    return int(hash_.hexdigest(), 16)


def sign(p, q, g, d, M):
    m = hash(M)
    k = random.randint(1, q - 1)
    r = fast_p(g, k, p)
    gcd, x, y = gcdex(k, q)
    k_ex = x % q
    s = (k_ex * (m - d * r)) % q
    return r, s


def verify(p, q, g, e, M, r, s):
    if s < 0 or s > q or r > p or r < 0:
        return False
    m = hash(M)
    return (fast_p(e, r, p) * fast_p(r, s, p)) % p == fast_p(g, m, p)


q =
112971461064154869310834029706569828562173472410416149342082034001846987882313
M = 'Я, Глеб Казачинский, люблю МиКОЗИ'

```

```
69. p, q, g, e, d = gen(q)
70.
71. r, s = sign(p, q, g, d, M)
72.
73. print(verify(p, q, g, e, M, r, s))
```

Результаты:

```
R : 45153391639833722457879765348144202368546652505174819443258754296788137312246 6
p : 5101044625554011362729626378113115575523846931907381150085625366862391110892116964630937051927428450177378267050989820959542413450333148816366207374434385 9
x: 476790950543241067369274607142120639008012374574529850746745009703354340694055344946403521690402301919751402341951277366814717483893310898628902493851081 69
g: 365084804729499878479639612586281479108321204988715315312220467946131122174711447123005286031646948997017947268461216714746961496261711461516528069860006 12
True
```