**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:

34. x = random.randint(1, p - 1)

35. g = fast\_p(x, R, p)

36. **print**('x:', x)

37. **print**('g:', g)

38. d = random.randint(1, q - 1)

39. e = fast\_p(g, d, p)

40. **return** p, q, g, e, d

41.

42.

43. **def** hash(m):

44. hash\_ = hashlib.sha256()

45. hash\_.update(m.encode())

46. **return** int(hash\_.hexdigest(), 16)

47.

48.

49. **def** sign(p, q, g, d, M):

50. m = hash(M)

51. k = random.randint(1, q - 1)

52. r = fast\_p(g, k, p)

53. gcd, x, y = gcdex(k, q)

54. k\_ex = x % q

55. s = (k\_ex \* (m - d \* r)) % q

56. **return** r, s

57.

58.

59. **def** verify(p, q, g, e, M, r, s):

60. **if** s < 0 **or** s > q **or** r > p **or** r < 0:

61. **return** False

62. m = hash(M)

63. **return** (fast\_p(e, r, p) \* fast\_p(r, s, p)) % p == fast\_p(g, m, p)

64.

65.

66. q = 112971461064154869310834029706569828562173472410416149342082034001846987882313

67. M = 'Я, Глеб Казачинский, люблю МиКОЗИ'

68.

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:** 