КОЩАВЦЕВ ДАНИИЛ ВАСИЛЬЕВИЧ (4ПМ)

**Задание 1.**

Алфавит: АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯпробел

Шифр: НСЬГЕЩЗЕВЖГРЛЛОВЕГФЛОЯЗЕЛЪВ

**Задание 2.**

К – 11001010

О – 11001110

Щ – 11011001

А – 11000000

В – 11000010

Ц – 11010110

Е – 11000101

В – 11000010

Пробел – 00100000

Д – 11000100

А – 11000000

Н – 11001101

L0 = 11001010 11001110 11011001 11000000

R0 = 11000010 11010110 11000101 11000010

X0 = 00100000 11000100 11000000 11001101

**Шаг 1**

1100 0010 1101 0110 1100 0101 1100 0010

0010 0000 1100 0100 1100 0000 1100 1101

1110 0011 1001 1011 1000 0110 1000 1111

**Шаг 2**

8 7 6 5 4 3 2 1

1110 0011 1001 1011 1000 0110 1000 1111

14 3 9 11 8 6 8 15

1000 0001 0110 1110 1110 0100 0010 0011

**Шаг 3**

(После сдвига) 0111 0111 0010 0001 0001 1100 0000 1011

**Шаг 4**

1100 1010 1100 1110 1101 1001 1100 0000

0111 0111 0010 0001 0001 1100 0000 1011

0011 0001 1110 1111 1110 0101 1100 1011

L1 = 1100 0010 1101 0110 1100 0101 1100 0010

R1 = 0011 0001 1110 1111 1110 0101 1100 1011

**Задание 3.**

p = 13, q = 31, , n = 403, d = 107

**Шаг 1**

****

s = 6

= = 323 (mod 360)

**Шаг 2**

Текст: КДВ = 12 5 3

Открытый ключ: (323, 360) Закрытый ключ: (107, 360)

= 288

= 245

= 27

**Шаг 3**

= 72

= 5

= 243

**Задание 4.**

Текст: КОЩАВЦЕВ = (12, 16, 27, 1, 3, 24, 6, 3)

p = 13, q = 31, n = 403, 0 = 38

H1 = mod 403 = 82

H2 = mod 403 = 335

H3 = mod 403 = 69

H4 = mod 403 = 64

H5 = mod 403 = 56

H6 = mod 403 = 355

H7 = mod 403 = 152

H8 = mod 403 = 248

Хеш-образ: 248

**Задание 5.**

Хеш-образ: 248

RSA: (107, 360)

s = mod 360 = 272

H = mod 360 = 248