**Пример 1.**

1) выберем два простых числа: ***p* = 3557 и *q* = 2579**;

2) вычислим их произведение *r* = *p·q* = 9173503;

3) вычислим функцию Эйлера: ***φ*(*r*) = (*p*–1)*·*(*q*–1) = 9167368**;

4) выберем ***КО* = 3**;

5)найдем значение ***КС***, для которого выполняется: 3*·KС* = 1 mod *φ*(*r*) =   
= 1 mod 9167368. ***КС* = 6111579**.

Текст для шифрования: 111111

Зашифрованное сообщение:

**Пример 2.**

1. Выберем **p=3** and **q=11**;
2. Определим их произведение **r= 3·11=33**;
3. Вычислим функцию Эйлера: **(p-1) · (q-1)=20**;
4. выберем ***КО* = 3**;
5. найдем значение ***КС,*** для которого выполняется: (3*·KС)* mod 20 = 1. ***КС=*7**

Текст для шифрования: САВ.

Представим шифруемое сообщение как последовательность чисел в диапазоне от 0 до 32   
(**не забывайте, что кончается на n-1**). Буква **А =1, В=2, С=3**.

Теперь зашифруем сообщение, используя открытый ключ {3,33}

**C1 = (3^3) mod 33 = 27 mod 33 = 27;   
C2 = (1^3) mod 33 = 3 mod 33 = 3;   
C3 = (2^3) mod 33 = 8 mod 33 = 8;   
Пример 3.**

1) выберем два простых числа: *p*= 41 и *q*= 59;

2) вычислим их произведение *r*= *p·q*= 2419;

3) вычислим функцию Эйлера: *φ*(*r*) = (*p*–1)*·*(*q*–1) = 40*·*58 = 2320;

4) выберем *КО* = 157; (2320, 157) = (157, 122) = (122, 35) = (35, 17) = 1;

5)найдем значение *КС*, для которого выполняется: 157*·KС*= 1 mod *φ*(*r*) =   
= 1 mod 2320. Положив *а* равным *φ*(*r*) и *b* равным *KО*, по расширенному алгоритму Евклида вычислим *КС* = *y*1 = 133.

В качестве примера зашифруем строку «BSUIR». Символам исходного текста соответствуют следующие десятичные ASCII-коды:

«B»: 66;

«S»: 83;

«U»: 85;

«I»: 73;

«R»: 82.

Таким образом, исходный текст *M* будет представлять собой последовательность чисел: *M*={66, 83, 85, 73, 82}. Тогда компоненты шифротекста *C* будут получены следующим образом:

*C*[1] = *M*[1]*KO*mod*r =*66157mod 2419 = 1425;

*C*[2] = *M*[2]*KO*mod*r =*83157mod 2419 = 575;

*C*[3] = 85157mod 2419 = 1473;

*C*[4] = 73157mod 2419 = 483;

*C*[5] = 82157mod 2419 = 2296.

Для расшифрования шифротекста *C*={1425, 575, 1473, 483, 2296} воспользуемся закрытым ключом *KC*:

*M*[1] = *C*[1]*KC*mod*r =*1425133mod 2419 = 66;

*M*[2] *=*575133mod 2419 = 83;

*M*[3] *=*1473133mod 2419 = 85;

*M*[4] *=*483133mod 2419 = 73;

*M*[5] *=*2296133mod 2419 = 82.

Таким образом, мы вновь получили исходный текст {66, 83, 85, 73, 82}, который соответствует строке «BSUIR».

**Пример 4**

**Шифруемый файл: BSUIR = 66 83 85 73 82**

**P = 11111111111111111111111 (всего 23 единицы)**

**Q = 900900900900990990990991**

**K (закрытый ключ) = 909090909090909091**

**R = 10010010010011011011010911011011011001001001001**

**K (открытый ключ) = 642057382979961832300653966089873831988598111**

**Выходной файл:**

**8129373381298850235619664716607504857587127790**

**4384752619449928713916601571381966648939193598**

**5187472847849390031874336852288511944623214666**

**5187472847849390031874336852288511944623214666**

**2936198203751516195242978606713896872892128180**

**Пример 5**

**Шифруемый файл: BSUIR = 66 83 85 73 82**

**P = 1125899839733759**

**Q = 18014398241046527**

**K (закрытый ключ) = 4398042316799**

**R = 20282408092494394779761211604993**

**K (открытый ключ) = 6872477891855582597287422486683**

**Выходной файл:**

**3118122894237163959320202699974**

**12373462813640541927793066897695**

**7016792235849909084380938893018**

**17087570667036504897864153598184**

**4919934515770599072985879527139**

**Пример 6**

**Шифруемый файл: BSUIR = 66 83 85 73 82**

**P = 35742549198872617291353508656626642567**

**Q = 359334085968622831041960188598043661065388726959079837**

**K (закрытый ключ) = 27644437**

**R = 12843516246565424159612232119158450558500502533923843847710718949148609993889068965015621579**

**K (открытый ключ) = 1728878421902762998097455220819211776576604992212759706380229508756002499918000451466532133**

**Выходной файл:**

**5259808662167131263406775095926984121392652839381485093106880803692231712553405268914821634**

**12588617860966273031636424712749020016575599586856247948153704655096205776001178045767981195**

**8888648696613494554784749592044376097907682165228480059525415352480943196421802669946968025**

**9421293887715419424154962662598759056229915131664340534916124485291873306972676937404407404**

**7008771028448985640819818593064275294985364719748994166370762278266578140879773007793784960**