**Алгоритм рабина ключ p, q и b (без длинной арифметики)**

**Исходный текст:**  **BSUIR**

**P=11, Q=19 (**при этом 11 mod 4 = 3 и 19 mod 4 = 3. Т.е. условие p ≡ q ≡ 3 mod 4 выполняется)

Вычислим наш открытый ключ: **n = p\*q = 11\*19 = 209**.

Выбираем ***в<n. в=173.***

Зашифруем сообщение по формуле Сi=Mi\*(Mi+b) mod n

**Шифротекст: 99, 139, 194, 193, 10.**

Для расшифровки сначала вычислим **D2** по формуле: Di= (b2+4\*Ci) mod n.

**D[i]= 20, 180, 191, 187, 82.**

Вычислим Mp и Mq по формулам:

**Мрi = mod p = Di(p+1)/4 mod p**

**Мqi = mod q = Di(q+1)/4 mod q**

Получим:

**Mp[i]= 3, 9, 9, 0, 4**

**Mq[i]= 1, 16, 1, 4, 5**

По алгоритму Евклида найдем **Yp, Yq:**

**Yp= 7, Yq= -4**

Вычисляем квадратные корни из D, используя китайскую теорему об остатках, по формулам:

**d1 = (yp\*p\*mq + yq\*q\* mp) mod n**

**d2= n - d1**

**d3 = (yp\*p\*mq - yq\*q\* mp) mod n**

**d4 = n - d3**

Для наших исходных данных получим:

**d1 d2 d3 d4**

**-151, 360, 96, 113**

**130, 79, 35, 174**

**-189, 398, 134, 75**

**99, 110, 99, 110**

**81, 128, 62, 147**

Далее для расшифровки следует использовать формулу: **Mi = (-b+di)/2 mod n**

**Для корректной расшифровки следует добавить условие: если (Di - b) – четное, то шифруем по формуле выше. В противном случае шифруем по формуле Mi = (-b+n+di)/2 mod n**

Расшифрованный текст:

-162 198 **66**  30 **(B)**

**83** 47 69 105 **(S)**

181 8 **85** 49 **(U)**

37 **73** 37 73 **(I)**

46 **82** 49 13 **(R)**

**Алгоритм рабина ключ p, q и b (без длинной арифметики)**

**Исходный текст:**  **BSUIR**

**P=11, Q=31 (**при этом 11 mod 4 = 3 и 31 mod 4 = 3. Т.е. условие p ≡ q ≡ 3 mod 4 выполняется)

Вычислим наш открытый ключ: **n = p\*q = 11\*31 = 341**.

Выбираем ***в<n. в=173.***

Зашифруем сообщение по формуле Сi=Mi\*(Mi+b) mod n

**Шифротекст: 88, 106, 106, 226, 109.**

Для расшифровки сначала вычислим **D2** по формуле: Di= (b2+4\*Ci) mod n.

**D[i]= 273, 4, 4, 143, 16.**

Вычислим Mp и Mq по формулам:

**Мрi = mod p = Di(p+1)/4 mod p**

**Мqi = mod q = Di(q+1)/4 mod q**

Получим:

**Mp[i]= 3, 9, 9, 0, 4**

**Mq[i]= 5, 2, 2, 9, 4**

По алгоритму Евклида найдем **Yp, Yq:**

**Yp=-14, Yq= 5**

Вычисляем квадратные корни из D, используя китайскую теорему об остатках, по формулам:

**d1 = (yp\*p\*mq + yq\*q\* mp) mod n**

**d2= n - d1**

**d3 = (yp\*p\*mq - yq\*q\* mp) mod n**

**d4 = n - d3**

Для наших исходных данных получим:

**d1 d2 d3 d4**

**-305, 646, -212, 129**

**64, 277, 339, 2**

**64, 277, 339, 2**

**-22, 363, 22, 319**

**4, 337, 213, 128**

Далее для расшифровки следует использовать формулу: **Mi = (-b+di)/2 mod n**

**Для корректной расшифровки следует добавить условие: если (Di - b) – четное, то шифруем по формуле выше. В противном случае шифруем по формуле Mi = (-b+n+di)/2 mod n**

Расшифрованный текст:

239 **66** 190 22 **(B)**

116 52 **83** 85 **(S)**

116 52 83  **85** **(U)**

**73** 95 95 73 **(I)**

86 **82** 20 148 **(R)**

**Алгоритм рабина ключ p, q и b (с длинной арифметикой)**

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

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

**Q = 900900900900990990990991**

Открытый ключ: **n = p\*q = 10010010010011011011010911011011011001001001001**

Выбираем ***в<n. в=* 100100100100110110110109110**

Зашифруем сообщение по формуле Сi=Mi\*(Mi+b) mod n

**Шифротекст: 6606606606607267267267205616**

**8308308308309139139139063019**

**8508508508509359359359281575**

**7307307307308038038037970359**

**8208208208209029029028953744**

Для расшифровки сначала вычислим **D2** по формуле: Di= (b2+4\*Ci) mod n.

**D[i]= 10021032043054993483573563646384282170812563**

**10021032043055000290380370453871769658242175**

**10021032043055001091181171254752650539116399**

**10021032043054996286376366449467365253871535**

**10021032043054999889979970053431329217805075**

|  |  |
| --- | --- |
| **Mp[i]** | **Mq[i]** |
| **11011011001001001000868**  **11011011001001001000834**  **11011011001001001000830**  **11011011001001001000854**  **100100110110110110275** | **100100100100110110109241**  **100100100100110110109275**  **800800800800880880881712**  **100100100100110110109255**  **100100100100110110109273** |

**yP = -8189100008100008918109**

**yQ = 100998900099890010100**

d1 0 = 1999320003736003935662435662455628305626309174

d2 0 = 8010690006275007075348475348555382695374691827

d3 0 = 10010010010011011010910810910910900890890891759

d4 0 = 100100100100110110110109242

d1 1 = 8186640009856010673789173789255567105558927940

d2 1 = 1823370000155000337221737221755443895442073061

d3 1 = 10010010010011011010910810910910900890890891725

d4 1 = 100100100100110110110109276

d1 2 = 100100100100110110110109280

d2 2 = 10010010010011011010910810910910900890890891721

d3 2 = 1095449999434999544500944500955451095450000265

d4 2 = 8914560010576011466509966510055559905551000736

d1 3 = 4547040006256006710185210185255603105598563960

d2 3 = 5462970003755004300825700825755407895402437041

d3 3 = 10010010010011011010910810910910900890890891745

d4 3 = 100100100100110110110109256

d1 4 = 10010010010011011010910810910910900890890891727

d2 4 = 100100100100110110110109274

d3 4 = 7822680009496010277428777428855570705562891542

d4 4 = 2187330000515000733582133582155440295438109459

m1 0 = 999660001868001967781167781177759097758100032

m2 0 = 9010350008143009043129643129733141793132791859

m3 0 = 10010010010011011010910810910910900890890891825

m4 0 = **66**

m1 1 = 4093320004928005336844536844577728497724409415

m2 1 = 5916690005083005674066274066333172393166482476

m3 1 = 10010010010011011010910810910910900890890891808

m4 1 = **83**

m1 2 = **85**

m2 2 = 10010010010011011010910810910910900890890891806

m3 2 = 5552730004723005277705877705933175993170446078

m4 2 = 4457280005288005733204933204977724897720445813

m1 3 = 2273520003128003355042555042577746497744227425

m2 3 = 7736490006883007655868255868333154393146664466

m3 3 = 10010010010011011010910810910910900890890891818

m4 3 = **73**

m1 4 = 10010010010011011010910810910910900890890891809

m2 4 = **82**

m3 4 = 3911340004748005138664338664377730297726391216

m4 4 = 6098670005263005872246472246533170593164500675

**Вариант 2Б ключ p и q (без длинной арифметики)**

**Исходный текст:**  **BSUIR**

**P=11, Q=31 (**при этом 11 mod 4 = 3 и 31 mod 4 = 3. Т.е. условие p ≡ q ≡ 3 mod 4 выполняется)

Вычислим наш **открытый ключ:** **n = p\*q = 11\*19 = 341**.

Зашифруем сообщение по формуле ci = mi2 mod n

«B»: 66;

«S»: 83;

«U»: 85;

«I»: 73;

«R»: 82.

**Шифротекст:** **264, 69, 64, 214, 245.**

Для дешифрации нужно решить уравнение mi2 = ci  (mod n)

При дешифрации сначала, используя алгоритм Евклида, из уравнения yp\*p+yq\*q=1 находят числа **Yp** и **Yq:**

**Yp= -14, Yq= 5**

Найдем Mp и Mq по формулам: **Мрi= Ci(p+1)/4 mod p, Мqi= Ci(q+1)/4 mod q.**

**Mp[i]= 0, 5, 3, 4, 5.**

**Mq[i]= 4, 10, 8, 20, 20.**

Используя китайскую теорему об остатках для извлечения квадратного корня вычисляют для каждого блока зашифрованного текста четыре числа. Одно из этих чисел и будет истинным открытым текстом М:

**r = (yp\*p\*mq + yq\*q\* mp) mod n**

**-r = n-r**

**s = (yp\*p\*mq - yq\*q\* mp) mod n**

**-s = n-s**

**Расшифрованный текст:**

275  **66**  275 66 **(B)**

**83** 258269 72 **(S)**

**85** 256 333 8 **(U)**

**73**  268 290 51 **(I)**

259  **82** 104 237 **(R)**

**Вариант 2Б ключ p и q (с длинной арифметикой)**

**Исходный текст:**  **BSUIR**

**shifroText 0 = 4356**

**shifroText 1 = 6889**

**shifroText 2 = 7225**

**shifroText 3 = 5329**

**shifroText 4 = 6724**

mp 0 = 11111111111111111111045

++++++++++++++++++++++++++++++++++++++++++++++++++++++

mq 0 = 66

++++++++++++++++++++++++++++++++++++++++++++++++++++++

mp 1 = 83

++++++++++++++++++++++++++++++++++++++++++++++++++++++

mq 1 = 83

++++++++++++++++++++++++++++++++++++++++++++++++++++++

mp 2 = 85

++++++++++++++++++++++++++++++++++++++++++++++++++++++

mq 2 = 900900900900990990990906

++++++++++++++++++++++++++++++++++++++++++++++++++++++

mp 3 = 11111111111111111111038

++++++++++++++++++++++++++++++++++++++++++++++++++++++

mq 3 = 73

++++++++++++++++++++++++++++++++++++++++++++++++++++++

mp 4 = 11111111111111111111029

++++++++++++++++++++++++++++++++++++++++++++++++++++++

mq 4 = 82

++++++++++++++++++++++++++++++++++++++++++++++++++++++

yP = -8189100008100008918109

yQ = 100998900099890010100

d1 0 = 8009340008142008942128742128822140802132800868

d2 0 = 2000670001869002068882168882188870198868200133

d3 0 = 10010010010011011011010911011011011001001000935

d4 0 = **66**

d1 1 = **83**

d2 1 = 10010010010011011011010911011011011001001000918

d3 1 = 5094330004929005437945537945588839598834509516

d4 1 = 4915680005082005573065373065422171402166491485

d1 2 = 4551720004722005176704976705022175002170455087

d2 2 = 5458290005289005834305934305988835998830545914

d3 2 = **85**

d4 2 = 10010010010011011011010911011011011001001000916

d1 3 = 6735480006882007554867354867422153402146673475

d2 3 = 3274530003129003456143556143588857598854327526

d3 3 = 10010010010011011011010911011011011001001000928

d4 3 = **73**

d1 4 = 5097660005262005771245571245622169602164509684

d2 4 = 4912350004749005239765339765388841398836491317

d3 4 = 10010010010011011011010911011011011001001000919

d4 4 = **82**