Алгоритм:

RSA

z=1;

**for** i =s-1 **downto** 0 **do**

z= z2 **mod** n

**if** ci =1 **then** z=z\*x **mod** n

1567^2417mod 8461 = 2386

c = 2417

x = 1567

n = 8461

(2417)10 = (100101110001) = Ci

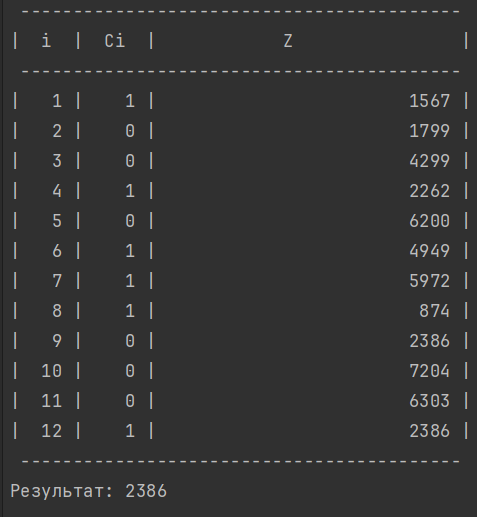
Практический пример:

|  |  |  |
| --- | --- | --- |
| i | Ci | Z=1 |
| 11 | 1 | z= z^2 mod n = 1^2 mod 2971=1 \* 1567mod 8461= 1567 |
| 10 | 0 | z= z^2 mod n = 1567^2 mod 8461=1799 |
| 9 | 0 | z= z^2 mod n = 1799^2 mod 8461=4299 |
| 8 | 1 | z= z^2 mod n = 4299^2 mod 8461 = 2577\*1567 mod 8461 = 2262 |
| 7 | 0 | z= z^2 mod n = 2262^2 mod 8461=6200 |
| 6 | 1 | z= z^2 mod n = 6200^2 mod 8461= 1677 \* 1567 mod 8461 = 4949 |
| 5 | 1 | z= z^2 mod n = 4949^2 mod 8461=6467 \* 1567mod 8461= 5972 |
| 4 | 1 | z= z^2 mod n = 5972^2 mod 8461=1669 \* 1567 mod 8461 = 874 |
| 3 | 0 | z= z^2 mod n = 874^2 mod 8461=2386 |
| 2 | 0 | z= z^2 mod n = 2386^2 mod 8461=7204 |
| 1 | 0 | z= z^2 mod n = 7204^2 mod 8461 = 6303 |
| 0 | 1 | z= z^2 mod n = 6303^2 mod 8461=3414 \* 1567mod 8461= 2386 |

C# код:

void Alg1()  
{  
 int x = 1567;  
 int c = 2417;  
 int n = 8461;  
  
 BigInteger z = 1;  
  
 string binary = Convert.ToString(c, 2).PadLeft(12, '0');  
   
 Console.WriteLine(" ------------------------------------------");  
 Console.WriteLine("| i | Ci | Z |");  
 Console.WriteLine(" ------------------------------------------");  
   
 for (int i = 11; i >= 0; i--)  
 {  
 int index = 12 - i;  
 char Ci = binary[11 - i];   
   
 z = (z \* z) % n;  
   
 if (Ci == '1')  
 {  
 z = (z \* x) % n;  
 }  
   
 Console.WriteLine($"| {index,3} | {Ci,3} | {z,27} |");  
 }  
   
 Console.WriteLine(" ------------------------------------------");  
   
 Console.WriteLine($"Результат: {z}");  
}  
  
string IntToString(int value, char[] baseChars)  
{  
 string result = string.Empty;  
 int targetBase = baseChars.Length;  
  
 do  
 {  
 result = baseChars[value % targetBase] + result;  
 value = value / targetBase;  
 }   
 while (value > 0);  
  
 return result;  
}

Результат:



Alg extins Euclid

Calculul inversei modulo:

1. n0 = n; b0 = b; t0 = 0; t = 1;

2.q = n0 / b0; r = n0 – q\*b0;

**3.while** r > 0 **do**

3.1.temp = t0 – q\*t;

3.2.**if** temp >= 0 **then** temp = temp **mod** n

**else** temp = n – ((- temp) **mod** n)

3.3n0 = b0; b0 = r; t0 = t; t= temp;

3.4.q = [n0/ b0]; r = n0 – q\*b0;

**4.if** b0 != 1 **then** b nu are inversă **mod** n

**else** b-1 **mod** n = t;

**Итерация 0:**

* n0: 1237
* b0: 2239
* q: 0
* r: 1237
* t0: 0
* t: 1
* temp: 0

**Итерация 1:**

* n0: 2239
* b0: 1237
* q: 1
* r: 1002
* t0: 1
* t: 0
* temp: 1

**Итерация 2:**

* n0: 1237
* b0: 1002
* q: 1
* r: 235
* t0: 0
* t: 1
* temp: 1236

**Итерация 3:**

* n0: 1002
* b0: 235
* q: 4
* r: 62
* t0: 1
* t: 1236
* temp: 5

**Итерация 4:**

* n0: 235
* b0: 62
* q: 3
* r: 49
* t0: 1236
* t: 5
* temp: 1221

**Итерация 5:**

* n0: 62
* b0: 49
* q: 1
* r: 13
* t0: 5
* t: 1221
* temp: 21

**Итерация 6:**

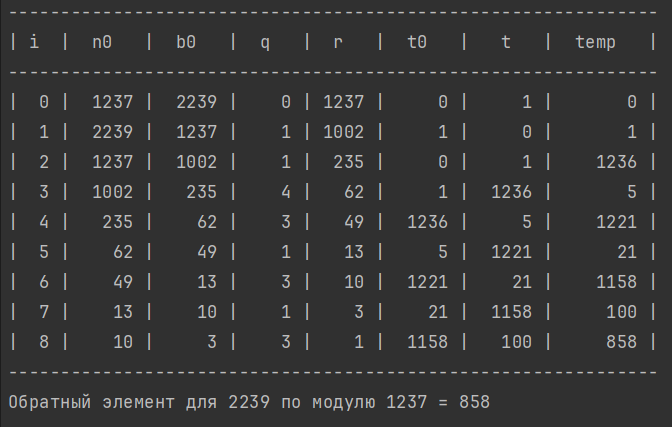
* n0: 49
* b0: 13
* q: 3
* r: 10
* t0: 1221
* t: 21
* temp: 1158

**Итерация 7:**

* n0: 13
* b0: 10
* q: 1
* r: 3
* t0: 21
* t: 1158
* temp: 100

**Итерация 8:**

* n0: 10
* b0: 3
* q: 3
* r: 1
* t0: 1158
* t: 100
* temp: 858



С# код

void EuclAlg2(int n, int b)  
{  
 int n0 = n;  
 int b0 = b;  
 int t0 = 0;  
 int t = 1;  
 int i = 0;  
   
 Console.WriteLine("--------------------------------------------------------------");  
 Console.WriteLine("| i | n0 | b0 | q | r | t0 | t | temp |");  
 Console.WriteLine("--------------------------------------------------------------");  
   
 int q = n0 / b0;  
 int r = n0 - q \* b0;  
  
 while (r > 0)  
 {  
 int temp = t0 - q \* t;  
   
 if (temp >= 0)  
 {  
 temp = temp % n;  
 }  
 else  
 {  
 temp = n - ((-temp) % n);  
 }  
   
 Console.WriteLine($"| {i,2} | {n0,5} | {b0,5} | {q,4} | {r,4} | {t0,5} | {t,5} | {temp,7} |");  
 i++;  
   
 n0 = b0;  
 b0 = r;  
 t0 = t;  
 t = temp;  
   
 q = n0 / b0;  
 r = n0 - q \* b0;  
 }  
   
 Console.WriteLine("--------------------------------------------------------------");  
   
 if (b0 != 1)  
 {  
 Console.WriteLine($"Обратного элемента для {b} по модулю {n} не существует.");  
 }  
 else  
 {  
 Console.WriteLine($"Обратный элемент для {b} по модулю {n} = {t}");  
 }  
}

RC2

Subkey = CS = 10000011 10100011

MOUNTAIN = 01001101 01001111 01010101 01001110 01010100 01000001 01001001 01001110

1. 01001101 01001111 XOR 10000011 10100011 = 11001110 11101100
2. 01010100 01000001 ^ 01001001 01001110 = 01000000 01000000
3. !(01001001 01001110) = 10110110 10110001
4. 01010101 01001110 ^ 10110110 10110001 = 11100011 11111111
5. 01000000 01000000 XOR 11100011 11111111 = 10100011 10111111
6. 11001110 11101100 XOR 10100011 10111111 = 01101101 01010011
7. 01010101 01001110 01010100 01000001 01001001 01001110 01101101 01010011

Конец 1 итерации.