Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерных систем и сетей

Кафедра программного обеспечения информационных технологий

Дисциплина: Теория информации (ТИ)

ОТЧЕТ

По лабораторной работе №3

Тема работы: Криптосистемы с открытым ключом

Выполнил

студент: гр. 051007 Захаренко Н.А.

Проверил: Болтак С.В.

Минск 2022

## Пример работы алгоритма быстрого возведения в степень

1311 % 23 = 1

A = 13, Z = 11

|  |  |  |  |
| --- | --- | --- | --- |
| I | A | Z | X (результат) |
| 0 | 13 | 11 | 1 |
| 1 | 13 | 11-1=10 | (13\*1)%23=13 |
| 2 | (13\*13)%23=8 | 10/2=5 | 13 |
| 3 | 8 | 5-1=4 | (8\*13)%23=12 |
| 4 | (8\*8)%23=18 | 4/2=2 | 12 |
| 5 | (18\*18)%23=2 | 2/2=1 | 12 |
| 6 | 2 | 1-1=0 | (2\*12)%23=1 |

## Пример работы расширенного алгоритма Евклида

А = 2341, B = 1789, GCD(A, B) = 1

X0\*A + Y0\*B = GCD(A, B)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Итерация | Quotient | A | B | X0 | X1 | Y0 | Y1 |
| 0 | - | 2341 | 1789 | 1 | 0 | 0 | 1 |
| 1 | 1 | 1789 | 552 | 0 | 1 | 1 | -1 |
| 2 | 3 | 552 | 133 | 1 | -3 | -1 | 4 |
| 3 | 4 | 133 | 20 | -3 | 13 | 4 | -17 |
| 4 | 6 | 20 | 13 | 13 | -81 | -17 | 106 |
| 5 | 1 | 13 | 7 | -81 | 94 | 106 | -123 |
| 6 | 1 | 7 | 6 | 94 | -175 | -123 | 229 |
| 7 | 1 | 6 | 1 | -175 | 269 | 229 | -352 |
| 8 | 6 | 1 | 0 | 269 | -1789 | -352 | 2341 |

X0 = 269; Y0 **= -**352

**269 \* 2341 + (-352) \* 1789 = 1 = GCD(2341, 1789)**

## Пример поиска случайного первообразного корня

P = 13

Простые делители P-1 = 12 = 2\*2\*3

|  |  |  |
| --- | --- | --- |
| Число | Проверка | Первообразный |
| 2 | 212/2 mod 13 = 12  212/3mod 13 = 3 | + |
| 3 | 312/2 mod 13 = 1  312/3mod 13 = 3 | - |
| 4 | 412/2 mod 13 = 1  412/3mod 13 = 9 | - |
| 5 | 512/2 mod 13 = 12  512/3mod 13 = 1 | - |
| 6 | 612/2 mod 13 = 12  612/3mod 13 = 9 | + |
| 7 | 712/2 mod 13 = 12  712/3mod 13 = 9 | + |
| 8 | 812/2 mod 13 = 12  812/3mod 13 = 1 | - |
| 9 | 912/2 mod 13 = 1  912/3mod 13 = 9 | - |
| 10 | 1012/2 mod 13 = 1  1012/3mod 13 = 3 | - |
| 11 | 1112/2 mod 13 = 12  1112/3mod 13 = 3 | + |
| 12 | 1112/2 mod 13 = 1  1112/3mod 13 = 1 | ­­­­­- |

Первообразные корни: 2, 6, 7, 11