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: Криптографические системы с открытым ключом

Выполнил

студент: гр. 151003 Барановский Р.А.

Проверил: Болтак С.В.

Минск 2023

Пример работы алгоритма быстрого возведения в степень

314  mod 5 = (1 \* 47) mod 5 = (4 \* 46) mod 5 = (4 \* 13) mod 5 =

(4 \* 12) mod 5 = (4 \* 11) mod 5 = 4

|  |  |  |  |
| --- | --- | --- | --- |
| а1(основание степени) | z1(степень) | x(результат) | Шаги выполнения |
| 3 | 14 | 1 | 0 |
| (3 \* 3) mod 5 = 4 | 14 / 2 = 7 | 1 | 1 |
| 4 | 7 – 1 = 6 | (1 \* 4) mod 5 = 4 | 2 |
| (4 \* 4) mod 5 = 1 | 6 / 2 = 3 | 4 | 3 |
| 1 | 3 – 1 = 2 | (4 \* 1) mod 5 = 4 | 4 |
| 1 | 2 / 2 = 1 | 4 | 5 |
| 1 | 1 – 1 = 0 | (4 \* 1) mod 5 = 4 | 6 |

Пример поиска первообразных корней

p = 13

p-1 = 12 = 2 \* 2 \* 3; Простые делители = [2, 3]

Первообразные корни(q) = [2, 6, 7, 11]

Пример работы расширенного алгоритма Евклида

X1\*a + y1\*b = НОД(a, b), a = 58, b = 63, (a, b) = 1

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **итерация** | **q** | **a0** | **a1** | **x0** | **x1** | **y0** | **y1** |
| 0 | - | 58 | 63 | 1 | 0 | 0 | 1 |
| 1 | 0 | 63 | 58 | 0 | 1 | 1 | 0 |
| 2 | 1 | 58 | 5 | 1 | -1 | 0 | 1 |
| 3 | 11 | 5 | 3 | -1 | 12 | 1 | -11 |
| 4 | 1 | 3 | 2 | 12 | -13 | -11 | 12 |
| 5 | 1 | 2 | **1** | -13 | **25** | 12 | **-23** |
| 6 | 2 | 1 | 0 | 25 | -63 | -23 | 58 |