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 работе № 3

Тема работы: Криптографические системы с открытым ключом

Выполнил Матюшенко В.A.

студент: гр. 151001

Проверила: Болтак С.В.

Минск 2023

1. **Пример работы алгоритма быстрого возведения в степень**

|  |  |  |  |
| --- | --- | --- | --- |
| а1(основание степени) | Z(степень) | х(результат) | Шаги выполнения |
| 4 | 7 | 1 | 0 |
| 4 | 6 | 4 | 1 |
| 5 | 3 | 4 | 2 |
| 5 | 2 | 9 | 3 |
| 14 | 1 | 9 | 4 |
| 14 | 0 | 5 | 5 |

1. **Пример поиска случайного первообразного корня**

Задано простое p = 11

p-1=10=2\*5

Проверяем является ли случайное число 2 первообразным корнем по модулю 11:

Число 2 является первообразным по модулю 11.

1. **Пример работы расширенного алгоритма Евклида**

x1\*25 + y1\*14 = 1, a = 25, b = 14, НОД(a,b) = 1

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **итерация** | **q** | **a0** | **a1** | **x0** | **x1** | **y0** | **y1** |
| 0 | - | 25 | 14 | 1 | 0 | 0 | 1 |
| 1 | 1 | 14 | 11 | 0 | 1 | 1 | -1 |
| 2 | 1 | 11 | 3 | 1 | -1 | -1 | 2 |
| 3 | 3 | 3 | 2 | -1 | 4 | 2 | -7 |
| 4 | 1 | 2 | 1 | 4 | -5 | -7 | 9 |
| 5 | 2 | 1 | 0 | -5 | 14 | 9 | 11 |

x1 = -5

y1 = 9

(-5)\*25 + 9 \* 14 = -125+126 = 1