УО «Белорусский государственный университет информатики и радиоэлектроники»

Кафедра ПОИТ

Отчет по лабораторной работе №3

по предмету «Теория информации»

Выполнил:

Лазута Д.А.

гр. 351004

Проверила:

Болтак С.В.

Минск 2025

**Вариант №2**

. Криптосистема Эль-Гамаля

**Нахождение первообразных корней для числа 23**

1. Проверка простоты: 23 - простое

2. Fi(23) = 23 - 1 = 22

3. Факторизация Fi(23): 22 = 2 \* 11

4. Поиск первообразных корней:

Условия: для каждого g от 1 до 22 проверяем:

- g^11 mod 23 != 1

- g^2 mod 23 != 1

5. Подробная проверка каждого кандидата:

Проверка g = 1:

- НОД(1,23) = 1 -> OK

- 1^11 mod 23 = 1 == 1 -> не корень

Проверка g = 2:

- НОД(2,23) = 1 -> OK

- 2^11 mod 23 = 1 == 1 -> не корень

Проверка g = 3:

- НОД(3,23) = 1 -> OK

- 3^11 mod 23 = 1 == 1 -> не корень

Проверка g = 4:

- НОД(4,23) = 1 -> OK

- 4^11 mod 23 = 1 == 1 -> не корень

Проверка g = 5:

- НОД(5,23) = 1 -> OK

- 5^11 mod 23 = 22 != 1 -> OK

- 5^2 mod 23 = 2 != 1 -> OK

==> 5 - первообразный корень!

Проверка g = 6:

- НОД(6,23) = 1 -> OK

- 6^11 mod 23 = 1 == 1 -> не корень

Проверка g = 7:

- НОД(7,23) = 1 -> OK

- 7^11 mod 23 = 22 != 1 -> OK

- 7^2 mod 23 = 3 != 1 -> OK

==> 7 - первообразный корень!

Проверка g = 8:

- НОД(8,23) = 1 -> OK

- 8^11 mod 23 = 1 == 1 -> не корень

Проверка g = 9:

- НОД(9,23) = 1 -> OK

- 9^11 mod 23 = 1 == 1 -> не корень

Проверка g = 10:

- НОД(10,23) = 1 -> OK

- 10^11 mod 23 = 22 != 1 -> OK

- 10^2 mod 23 = 8 != 1 -> OK

==> 10 - первообразный корень!

Проверка g = 11:

- НОД(11,23) = 1 -> OK

- 11^11 mod 23 = 22 != 1 -> OK

- 11^2 mod 23 = 6 != 1 -> OK

==> 11 - первообразный корень!

Проверка g = 12:

- НОД(12,23) = 1 -> OK

- 12^11 mod 23 = 1 == 1 -> не корень

Проверка g = 13:

- НОД(13,23) = 1 -> OK

- 13^11 mod 23 = 1 == 1 -> не корень

Проверка g = 14:

- НОД(14,23) = 1 -> OK

- 14^11 mod 23 = 22 != 1 -> OK

- 14^2 mod 23 = 12 != 1 -> OK

==> 14 - первообразный корень!

Проверка g = 15:

- НОД(15,23) = 1 -> OK

- 15^11 mod 23 = 22 != 1 -> OK

- 15^2 mod 23 = 18 != 1 -> OK

==> 15 - первообразный корень!

Проверка g = 16:

- НОД(16,23) = 1 -> OK

- 16^11 mod 23 = 1 == 1 -> не корень

Проверка g = 17:

- НОД(17,23) = 1 -> OK

- 17^11 mod 23 = 22 != 1 -> OK

- 17^2 mod 23 = 13 != 1 -> OK

==> 17 - первообразный корень!

Проверка g = 18:

- НОД(18,23) = 1 -> OK

- 18^11 mod 23 = 1 == 1 -> не корень

Проверка g = 19:

- НОД(19,23) = 1 -> OK

- 19^11 mod 23 = 22 != 1 -> OK

- 19^2 mod 23 = 16 != 1 -> OK

==> 19 - первообразный корень!

Проверка g = 20:

- НОД(20,23) = 1 -> OK

- 20^11 mod 23 = 22 != 1 -> OK

- 20^2 mod 23 = 9 != 1 -> OK

==> 20 - первообразный корень!

Проверка g = 21:

- НОД(21,23) = 1 -> OK

- 21^11 mod 23 = 22 != 1 -> OK

- 21^2 mod 23 = 4 != 1 -> OK

==> 21 - первообразный корень!

Проверка g = 22:

- НОД(22,23) = 1 -> OK

- 22^11 mod 23 = 22 != 1 -> OK

- 22^2 mod 23 = 1 == 1 -> не корень

=== Результаты ===

Всего проверено кандидатов: 22

Найдено первообразных корней: 10 (теория: Fi(22) = 10)

Список всех первообразных корней по модулю 23:

5, 7, 10, 11, 14, 15, 17, 19, 20, 21

Наименьший первообразный корень: 5

Наибольший первообразный корень: 21

**Вычисление программой первообразных корней для некоторых чисел:**





