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

1. Алгоритм быстрого возведения в степень (7^15 mod 19)

Давайте проверим вычисление 66^777 mod 666 по алгоритму быстрого возведения в степень:

| **Шаг** | **a** | **n** | **e** | **Действие** | **r mod x** |
| --- | --- | --- | --- | --- | --- |
| **1** | **66** | **777** | **нет** | **r = 1 \* 66 mod 666 = 66** | **66** |
| **2** | **66** | **776** | **да** | **a = 66² mod 666 = 4356 mod 666 = 198** | **66** |
| **3** | **198** | **388** | **да** | **a = 198² mod 666 = 39204 mod 666 = 198** | **66** |
| **4** | **198** | **194** | **да** | **a = 198² mod 666 = 39204 mod 666 = 198** | **66** |
| **5** | **198** | **97** | **нет** | **r = 66 \* 198 mod 666 = 13068 mod 666 = 216** | **216** |
| **6** | **198** | **96** | **да** | **a = 198² mod 666 = 39204 mod 666 = 198** | **216** |
| **7** | **198** | **48** | **да** | **a = 198² mod 666 = 39204 mod 666 = 198** | **216** |
| **8** | **198** | **24** | **да** | **a = 198² mod 666 = 39204 mod 666 = 198** | **216** |
| **9** | **198** | **12** | **да** | **a = 198² mod 666 = 39204 mod 666 = 198** | **216** |
| **10** | **198** | **6** | **да** | **a = 198² mod 666 = 39204 mod 666 = 198** | **216** |
| **11** | **198** | **3** | **нет** | **r = 216 \* 198 mod 666 = 42768 mod 666 = 216** | **216** |
| **12** | **198** | **2** | **да** | **a = 198² mod 666 = 39204 mod 666 = 198** | **216** |
| **13** | **198** | **1** | **нет** | **r = 216 \* 198 mod 666 = 42768 mod 666 = 216** | **216** |

**Нахождение первообразных корней для числа 53**

1. Проверка простоты: 53 - простое

2. Fi(53) = 53 - 1 = 52

3. Факторизация Fi(53): 52 = 2 \* 13

4. Поиск первообразных корней:

Условия: для каждого g от 1 до 52 проверяем:

- g^26 mod 53 != 1

- g^4 mod 53 != 1

5. Подробная проверка каждого кандидата:

Проверка g = 1:

- НОД(1,53) = 1 -> OK

- 1^26 mod 53 = 1 == 1 -> не корень

Проверка g = 2:

- НОД(2,53) = 1 -> OK

- 2^26 mod 53 = 52 != 1 -> OK

- 2^4 mod 53 = 16 != 1 -> OK

==> 2 - первообразный корень!

Проверка g = 3:

- НОД(3,53) = 1 -> OK

- 3^26 mod 53 = 52 != 1 -> OK

- 3^4 mod 53 = 28 != 1 -> OK

==> 3 - первообразный корень!

Проверка g = 4:

- НОД(4,53) = 1 -> OK

- 4^26 mod 53 = 1 == 1 -> не корень

Проверка g = 5:

- НОД(5,53) = 1 -> OK

- 5^26 mod 53 = 52 != 1 -> OK

- 5^4 mod 53 = 42 != 1 -> OK

==> 5 - первообразный корень!

Проверка g = 6:

- НОД(6,53) = 1 -> OK

- 6^26 mod 53 = 1 == 1 -> не корень

Проверка g = 7:

- НОД(7,53) = 1 -> OK

- 7^26 mod 53 = 1 == 1 -> не корень

Проверка g = 8:

- НОД(8,53) = 1 -> OK

- 8^26 mod 53 = 52 != 1 -> OK

- 8^4 mod 53 = 15 != 1 -> OK

==> 8 - первообразный корень!

Проверка g = 9:

- НОД(9,53) = 1 -> OK

- 9^26 mod 53 = 1 == 1 -> не корень

Проверка g = 10:

- НОД(10,53) = 1 -> OK

- 10^26 mod 53 = 1 == 1 -> не корень

Проверка g = 11:

- НОД(11,53) = 1 -> OK

- 11^26 mod 53 = 1 == 1 -> не корень

Проверка g = 12:

- НОД(12,53) = 1 -> OK

- 12^26 mod 53 = 52 != 1 -> OK

- 12^4 mod 53 = 13 != 1 -> OK

==> 12 - первообразный корень!

Проверка g = 13:

- НОД(13,53) = 1 -> OK

- 13^26 mod 53 = 1 == 1 -> не корень

Проверка g = 14:

- НОД(14,53) = 1 -> OK

- 14^26 mod 53 = 52 != 1 -> OK

- 14^4 mod 53 = 44 != 1 -> OK

==> 14 - первообразный корень!

Проверка g = 15:

- НОД(15,53) = 1 -> OK

- 15^26 mod 53 = 1 == 1 -> не корень

Проверка g = 16:

- НОД(16,53) = 1 -> OK

- 16^26 mod 53 = 1 == 1 -> не корень

Проверка g = 17:

- НОД(17,53) = 1 -> OK

- 17^26 mod 53 = 1 == 1 -> не корень

Проверка g = 18:

- НОД(18,53) = 1 -> OK

- 18^26 mod 53 = 52 != 1 -> OK

- 18^4 mod 53 = 36 != 1 -> OK

==> 18 - первообразный корень!

Проверка g = 19:

- НОД(19,53) = 1 -> OK

- 19^26 mod 53 = 52 != 1 -> OK

- 19^4 mod 53 = 47 != 1 -> OK

==> 19 - первообразный корень!

Проверка g = 20:

- НОД(20,53) = 1 -> OK

- 20^26 mod 53 = 52 != 1 -> OK

- 20^4 mod 53 = 46 != 1 -> OK

==> 20 - первообразный корень!

Проверка g = 21:

- НОД(21,53) = 1 -> OK

- 21^26 mod 53 = 52 != 1 -> OK

- 21^4 mod 53 = 24 != 1 -> OK

==> 21 - первообразный корень!

Проверка g = 22:

- НОД(22,53) = 1 -> OK

- 22^26 mod 53 = 52 != 1 -> OK

- 22^4 mod 53 = 49 != 1 -> OK

==> 22 - первообразный корень!

Проверка g = 23:

- НОД(23,53) = 1 -> OK

- 23^26 mod 53 = 52 != 1 -> OK

- 23^4 mod 53 = 1 == 1 -> не корень

Проверка g = 24:

- НОД(24,53) = 1 -> OK

- 24^26 mod 53 = 1 == 1 -> не корень

Проверка g = 25:

- НОД(25,53) = 1 -> OK

- 25^26 mod 53 = 1 == 1 -> не корень

Проверка g = 26:

- НОД(26,53) = 1 -> OK

- 26^26 mod 53 = 52 != 1 -> OK

- 26^4 mod 53 = 10 != 1 -> OK

==> 26 - первообразный корень!

Проверка g = 27:

- НОД(27,53) = 1 -> OK

- 27^26 mod 53 = 52 != 1 -> OK

- 27^4 mod 53 = 10 != 1 -> OK

==> 27 - первообразный корень!

Проверка g = 28:

- НОД(28,53) = 1 -> OK

- 28^26 mod 53 = 1 == 1 -> не корень

Проверка g = 29:

- НОД(29,53) = 1 -> OK

- 29^26 mod 53 = 1 == 1 -> не корень

Проверка g = 30:

- НОД(30,53) = 1 -> OK

- 30^26 mod 53 = 52 != 1 -> OK

- 30^4 mod 53 = 1 == 1 -> не корень

Проверка g = 31:

- НОД(31,53) = 1 -> OK

- 31^26 mod 53 = 52 != 1 -> OK

- 31^4 mod 53 = 49 != 1 -> OK

==> 31 - первообразный корень!

Проверка g = 32:

- НОД(32,53) = 1 -> OK

- 32^26 mod 53 = 52 != 1 -> OK

- 32^4 mod 53 = 24 != 1 -> OK

==> 32 - первообразный корень!

Проверка g = 33:

- НОД(33,53) = 1 -> OK

- 33^26 mod 53 = 52 != 1 -> OK

- 33^4 mod 53 = 46 != 1 -> OK

==> 33 - первообразный корень!

Проверка g = 34:

- НОД(34,53) = 1 -> OK

- 34^26 mod 53 = 52 != 1 -> OK

- 34^4 mod 53 = 47 != 1 -> OK

==> 34 - первообразный корень!

Проверка g = 35:

- НОД(35,53) = 1 -> OK

- 35^26 mod 53 = 52 != 1 -> OK

- 35^4 mod 53 = 36 != 1 -> OK

==> 35 - первообразный корень!

Проверка g = 36:

- НОД(36,53) = 1 -> OK

- 36^26 mod 53 = 1 == 1 -> не корень

Проверка g = 37:

- НОД(37,53) = 1 -> OK

- 37^26 mod 53 = 1 == 1 -> не корень

Проверка g = 38:

- НОД(38,53) = 1 -> OK

- 38^26 mod 53 = 1 == 1 -> не корень

Проверка g = 39:

- НОД(39,53) = 1 -> OK

- 39^26 mod 53 = 52 != 1 -> OK

- 39^4 mod 53 = 44 != 1 -> OK

==> 39 - первообразный корень!

Проверка g = 40:

- НОД(40,53) = 1 -> OK

- 40^26 mod 53 = 1 == 1 -> не корень

Проверка g = 41:

- НОД(41,53) = 1 -> OK

- 41^26 mod 53 = 52 != 1 -> OK

- 41^4 mod 53 = 13 != 1 -> OK

==> 41 - первообразный корень!

Проверка g = 42:

- НОД(42,53) = 1 -> OK

- 42^26 mod 53 = 1 == 1 -> не корень

Проверка g = 43:

- НОД(43,53) = 1 -> OK

- 43^26 mod 53 = 1 == 1 -> не корень

Проверка g = 44:

- НОД(44,53) = 1 -> OK

- 44^26 mod 53 = 1 == 1 -> не корень

Проверка g = 45:

- НОД(45,53) = 1 -> OK

- 45^26 mod 53 = 52 != 1 -> OK

- 45^4 mod 53 = 15 != 1 -> OK

==> 45 - первообразный корень!

Проверка g = 46:

- НОД(46,53) = 1 -> OK

- 46^26 mod 53 = 1 == 1 -> не корень

Проверка g = 47:

- НОД(47,53) = 1 -> OK

- 47^26 mod 53 = 1 == 1 -> не корень

Проверка g = 48:

- НОД(48,53) = 1 -> OK

- 48^26 mod 53 = 52 != 1 -> OK

- 48^4 mod 53 = 42 != 1 -> OK

==> 48 - первообразный корень!

Проверка g = 49:

- НОД(49,53) = 1 -> OK

- 49^26 mod 53 = 1 == 1 -> не корень

Проверка g = 50:

- НОД(50,53) = 1 -> OK

- 50^26 mod 53 = 52 != 1 -> OK

- 50^4 mod 53 = 28 != 1 -> OK

==> 50 - первообразный корень!

Проверка g = 51:

- НОД(51,53) = 1 -> OK

- 51^26 mod 53 = 52 != 1 -> OK

- 51^4 mod 53 = 16 != 1 -> OK

==> 51 - первообразный корень!

Проверка g = 52:

- НОД(52,53) = 1 -> OK

- 52^26 mod 53 = 1 == 1 -> не корень

=== Результаты ===

Всего проверено кандидатов: 52

Найдено первообразных корней: 24 (теория: Fi(52) = 24)

Список всех первообразных корней по модулю 53:

2, 3, 5, 8, 12, 14, 18, 19, 20, 21,

22, 26, 27, 31, 32, 33, 34, 35, 39, 41,

45, 48, 50, 51

Наименьший первообразный корень: 2

Наибольший первообразный корень: 51

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





