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 83**

**Шаг 1: Вычисляем φ(83)**

Для простого числа:

φ(97) = 83−1= *82*

**Шаг 2: Факторизуем φ(83) = 82**

Разложение на простые множители:

96=41×2

Таким образом, простые делители:

q∈{2,41}

**Шаг 3: Критерий проверки первообразного корня**

Число gявляется первообразным корнем по модулю 83, если:

g^41!= 1 mod 83 и g^2 != 1 mod 83

где:

* 41=82/2​ (проверка для q=2),
* 2=82/41​ (проверка для q=41),

**Шаг 4: Перебираем числа и получаем все корни:**

5,7,10,13,14,15,17,21,23,26,29,30,31,34,35,37,38,39,40,41,43,45,47,51,53,57,58,59,60,63,65,66

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





