|  |  |
| --- | --- |
| **Российский университет транспорта (МИИТ)**  **Институт транспортной техники и систем управления**  **Кафедра «Управление и защита информации»** | |
| **Отчет**  **по практическому заданию**  **по теме «Исследование и реализация методов ассиметричной криптографии»**  **по дисциплине «Криптографические методы защиты информации»** | |
|  | Выполнил:  Студент группы ТКИ-342  Белов С.В.  Проверил:  Доцент кафедры УиЗи, к.т.н., с.н.с.  Михалевич И.Ф. |
| Москва 2023 | |

**Оглавление**

[Задание 3](#_Toc1544506013)

[Исходные данные 4](#_Toc1163256968)

[1. Вычисление простого числа 4](#_Toc1504746980)

[1.1. Решето Эратосфена 5](#_Toc327052847)

[1.1.1. Теория 5](#_Toc739787853)

[1.1.2. Практика 5](#_Toc1950597120)

[1.2. Альтернативные алгоритмы 6](#_Toc361591191)

[1.2.1. Теория 6](#_Toc2059215141)

[1.2.2. Практика 7](#_Toc992435753)

[2. Проверка чисел на взаимную простоту 7](#_Toc718190065)

[2.1. Теорема Эйлера 7](#_Toc618917188)

[2.1.1. Теория 7](#_Toc364962991)

[2.1.2. Практика 7](#_Toc1569511584)

[2.2. Альтернативные алгоритмы 7](#_Toc1362665697)

[2.2.1. Теория 7](#_Toc569658081)

[2.2.2. Практика 7](#_Toc1852618274)

[3. Исследование метода Эль-Гамаля 7](#_Toc1912809680)

[4. Реализация метода 7](#_Toc1483856844)

[4.1. Теорема Эйлера 7](#_Toc1100235216)

[4.1.1. Теория 7](#_Toc260070799)

[4.1.2. Практика 7](#_Toc2120200871)

[4.2. Альтернативные алгоритмы 7](#_Toc1255696126)

[4.2.1. Теория 7](#_Toc1653359714)

[4.2.2. Практика 7](#_Toc831414859)

[5. Область применения 7](#_Toc1916641519)

[5.1. Теорема Эйлера 7](#_Toc332684937)

[5.1.1. Теория 7](#_Toc725559765)

[5.1.2. Практика 7](#_Toc2031525149)

[5.2. Альтернативные алгоритмы 7](#_Toc141754092)

[5.2.1. Теория 7](#_Toc400252125)

[5.2.2. Практика 7](#_Toc990756062)

[Заключение 7](#_Toc977737778)

# Задание

Задание1. Вычислить простое число p (привести описание трех или более методов проверки простоты, реализовать один или более, проверить число на простоту)

2. Проверить числа lи (b+ f) на взаимную простоту (привести описание методов проверки взаимной простоты чисел, реализовать один или более, проверить, являются ли числа lи (b+ f) взаимно простыми)

3.Описать метод (дать общую характеристику исследуемого метода)

4. Реализовать метод (в Эксельи программно)

5. Описать области применения метода (привести примеры)

6. Оформить отчет

# Исходные данные

1. b–восьмиразрядное число, отражающее день рождения студентав формате дмг(день, месяц, год полностью)Пример. b= 01091999 для 1 сентября 1999 года

2. f –восьмиразрядное число, образованное суммой чисел 10 и двухразрядного номера студента в списке группы, дополненное шестью нулями справаПример. Номер в списке 5 : 10+05, f= 15000000

3. p –простое число, ближайшее меньшее к числу b+ f :p ≤ (b + f)Пример. b+ f= 16091999 при b= 01091999, f= 15000000

4. l–шестиразрядное число, образованное исключением первогоитретьегоразрядов слева из числа b. Пример.l=191999при b= 01091999

# 1. Вычисление простого числа

## 1.1. Решето Эратосфена

### 1.1.1. Теория

Алгоритм Евклида используется для нахождения наибольшего общего делителя (НОД) двух чисел.

Алгоритм Евклида используется для нахождения наибольшего общего делителя (НОД) двух чисел.

Схема алгоритма: пусть даны два числа a1 и a2, a1 > a2. Делим a1 на a2 с остатком:

a1 = k1 a2 + a3 (k1 – натуральное, 0 ≤ a3 < a2).

Если a3 = 0, то, значит, a2 и есть искомый НОД. Если же нет, то делим a2 на a3 с остатком:

a2 = k2a3 + a4 (k2 – натуральное, 0 ≤ a4 < a3).

Если a4 = 0, то, значит, a3 и есть искомый НОД. Если же нет, то делим a3 на a4 с остатком:

a3 = k3a4 + a5 (k3 – натуральное, 0 ≤ a5 < a4),

и т. д., получаем последовательность шагов

an – 2 = kn an – 1 + an (все kn – натуральные, 0 ≤ an < an – 1).

Если какой-то из последовательных остатков an станет равным 0, алгоритм на этом останавливается; при этом предыдущий остаток an – 1 будет искомым НОД.

|  |  |
| --- | --- |
|  |  |

### 1.1.2. Практика

Согласно обратной теореме, всякая пара чисел (число) , ­, будет решением системы уравнения являются корнями уравнения .

|  |  |
| --- | --- |
|  |  |

## 1.2. Альтернативные алгоритмы

### 1.2.1. Теория

|  |  |
| --- | --- |
|  |  |

### 1.2.2. Практика

# 2. Проверка чисел на взаимную простоту

## 2.1. Теорема Эйлера

### 2.1.1. Теория

Напомним, что взаимно простые числами называются целые числа, не имеющие никаких общих делителей, кроме ±1. Если же в наборе более чем двух целых чисел любые два числа из набора взаимно просты, то такие числа называются попарно взаимно простыми (или просто попарно простыми).

Свойство попарной простоты более сильно, чем свойство взаимной простоты — попарно простые числа будут и взаимно простыми, но обратное неверно. Очевидно, что для двух чисел понятия «взаимно простые» и «попарно простые» совпадают.

Правило проверки на взаимную простоту вытекает из определения взаимно простых чисел - если НОД (наибольший общий делитель) нескольких чисел равен 1, то эти числа - взаимно простые.

Чтобы проверить числа на попарную простоту, можно воспользоваться следующим свойством: у попарно взаимно простых чисел НОК (наименьшее общее кратное) равно абсолютной величине их произведения. То есть достаточно найти НОК нескольких чисел и сравнить с их произведением, взятым по модулю. Если они равны - числа взаимно попарно простые.

### 2.1.2. Практика

## 2.2. Альтернативные алгоритмы

### 2.2.1. Теория

|  |  |
| --- | --- |
|  |  |

### 2.2.2. Практика

# 3. Исследование метода Эль-Гамаля

# 4. Реализация метода

## 4.1. Теорема Эйлера

### 4.1.1. Теория

### 4.1.2. Практика

## 4.2. Альтернативные алгоритмы

### 4.2.1. Теория

|  |  |
| --- | --- |
|  |  |

### 4.2.2. Практика

# 5. Область применения

## 5.1. Примеры

## 5.2. Стандарты

# Заключение

Текст заключения.