|  |  |
| --- | --- |
| **Российский университет транспорта (МИИТ)**  **Институт транспортной техники и систем управления**  **Кафедра «Управление и защита информации»** | |
| **Отчет**  **по практическому заданию**  **по теме «Создание шаблонов отчетных документов»**  **по дисциплине «Криптографические методы защиты информации»** | |
|  | Выполнил:  Студент группы ТКИ-342  Пономарев А.Д.  Проверил:  Доцент кафедры УиЗи, к.т.н., с.н.с.  Михалевич И.Ф. |
| Москва 2023 | |

**Оглавление**

[1. Задание 3](#_Toc128319560)

[2. Исходные данные 3](#_Toc128319561)

[3. Теоретическая часть 3](#_Toc128319562)

[3.1 Бинарный алгоритм 3](#_Toc128319563)

[3.2 Описание алгоритма быстрого возведения в степень по модулю с использованием КТО (китайской теоремы об остатках) 4](#_Toc128319564)

[4. Практическая часть 6](#_Toc128319565)

[4.1 Бинарный алгоритм 6](#_Toc128319566)

[5. Результаты наблюдения 6](#_Toc128319567)

[Заключение 7](#_Toc128319568)

# 1. Задание

Произвести вычисления следующих выражений используя бинарный алгоритм и 1-2 альтернативных алгоритма.

|  |
| --- |
|  |
| Рисунок 1 – примеры для вычисления |

# 2. Исходные данные

Вариант 13

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

# 3. Теоретическая часть

## 3.1 Бинарный алгоритм

Пусть необходимо возвести число a в степень b по модулю c:

1 шаг: разложение b в двоичное число

2 шаг: вычисление где – степени разложенного b

3 шаг: подстановка вычисленных частей в разложенное произведение

|  |
| --- |
| Алгоритмы быстрого возведения в степень по модулю - Wikiwand |

– Блок-схема алгоритма

|  |
| --- |
|  |

– Псевдокод алгоритма

## 3.2 Описание алгоритма быстрого возведения в степень по модулю с использованием КТО (китайской теоремы об остатках)

Пусть необходимо возвести число a в степень b по модулю c:

можно разложить на простые множители и построить систему:

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

Т.о. можно представить как где – целое число

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

Постепенно подставляя из 1-го уравнения во 2, из 2 в 3, ... получим чему равно

# 4. Практическая часть

## 4.1 Бинарный алгоритм

Рисунок был взят из методических указаний к данной работе.

# 5. Результаты наблюдения

# Заключение

Изучены методы работы с «Word».