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

**Оглавление**

[Задание 5](#_Toc129262633)

[Исходные данные 5](#_Toc129262634)

[1. Способы преобразования и проверки правильности преобразования 6](#_Toc129262635)

[1.1. Метод разбиения (breakdown method) 6](#_Toc129262636)

[1.2. Преобразование чисел методом вычисления значений полиномов (многочленов) 6](#_Toc129262637)

[1.3. Метод преобразования числа ручным пересчётом 7](#_Toc129262638)

[1.4. Схема Горнера 7](#_Toc129262639)

[2. Преобразование и проверка для двоичной системы 8](#_Toc129262640)

[2.1. Вычисление значения исходного числа ДР 8](#_Toc129262641)

[2.1.1. Метод деления 8](#_Toc129262642)

[2.1.2. Проверка методом полиномов и Горнера 8](#_Toc129262643)

[2.2. Вычисление значения исходного числа ДЗ 9](#_Toc129262644)

[2.2.1. Метод деления 9](#_Toc129262645)

[2.2.2. Проверка методом полиномов и Горнера 9](#_Toc129262646)

[2.3. Вычисление значения суммы чисел ДР и ДЗ 10](#_Toc129262647)

[2.3.1. Метод деления 10](#_Toc129262648)

[2.3.2. Проверка методом полиномов и Горнера 10](#_Toc129262649)

[3. Преобразование и проверка для троичной системы 11](#_Toc129262650)

[3.1. Вычисление значения исходного числа ДР 11](#_Toc129262651)

[3.1.1. Метод деления 11](#_Toc129262652)

[3.1.2. Проверка методом полиномов и Горнера 11](#_Toc129262653)

[3.2. Вычисление значения исходного числа ДЗ 12](#_Toc129262654)

[3.2.1. Метод деления 12](#_Toc129262655)

[3.2.2. Проверка методом полиномов и Горнера 12](#_Toc129262656)

[3.3. Вычисление значения суммы чисел ДР и ДЗ 13](#_Toc129262657)

[3.3.1. Метод деления 13](#_Toc129262658)

[3.3.2. Проверка методом полиномов и Горнера 13](#_Toc129262659)

[4. Преобразование и проверка для четверичной системы 14](#_Toc129262660)

[4.1. Вычисление значения исходного числа ДР 14](#_Toc129262661)

[4.1.1. Метод деления 14](#_Toc129262662)

[4.1.2. Проверка методом полиномов и Горнера 14](#_Toc129262663)

[4.2. Вычисление значения исходного числа ДЗ 15](#_Toc129262664)

[4.2.1. Метод деления 15](#_Toc129262665)

[4.2.2. Проверка методом полиномов и Горнера 15](#_Toc129262666)

[4.3. Вычисление значения суммы чисел ДР и ДЗ 16](#_Toc129262667)

[4.3.1. Метод деления 16](#_Toc129262668)

[4.3.2. Проверка методом полиномов и Горнера 16](#_Toc129262669)

[5. Преобразование и проверка для восьмеричной системы 17](#_Toc129262670)

[5.1. Вычисление значения исходного числа ДР 17](#_Toc129262671)

[5.1.1. Метод деления 17](#_Toc129262672)

[5.1.2. Проверка методом полиномов и Горнера 17](#_Toc129262673)

[5.2. Вычисление значения исходного числа ДЗ 18](#_Toc129262674)

[5.2.1. Метод деления 18](#_Toc129262675)

[5.2.2. Проверка методом полиномов и Горнера 18](#_Toc129262676)

[5.3. Вычисление значения суммы чисел ДР и ДЗ 19](#_Toc129262677)

[5.3.1. Метод деления 19](#_Toc129262678)

[5.3.2. Проверка методом полиномов и Горнера 19](#_Toc129262679)

[6. Преобразование и проверка для шестнадцатеричной системы 20](#_Toc129262680)

[6.1. Вычисление значения исходного числа ДР 20](#_Toc129262681)

[6.1.1. Метод деления 20](#_Toc129262682)

[6.1.2. Проверка методом полиномов и Горнера 20](#_Toc129262683)

[6.2. Вычисление значения исходного числа ДЗ 21](#_Toc129262684)

[6.2.1. Метод деления 21](#_Toc129262685)

[6.2.2. Проверка методом полиномов и Горнера 21](#_Toc129262686)

[6.3. Вычисление значения суммы чисел ДР и ДЗ 22](#_Toc129262687)

[6.3.1. Метод деления 22](#_Toc129262688)

[6.3.2. Проверка методом полиномов и Горнера 22](#_Toc129262689)

[7. Заключение 23](#_Toc129262690)

# Задание

Разработать моноалфавитный шифр, таблицы шифрования / расшифрования (для варианта шифра). Подготовить сообщение путем СЛИЯНИЯ сообщений инициатора и ответчика. Зашифровать и расшифровать сообщение. Провести анализ слабостей шифра (привести таблицы и гистограммы частотности символов исходного алфавита и сообщения, зашифрованного разработанным шифром, описать слабости шифра). Оформить отчет.

# Исходные данные

1. Алфавит, выбранный студентом на основе алфавита русского языка.
2. Ключ – номер студента в группе.
3. Шифр – алфавит со сдвигом вправо по ключу.
4. Передаваемые сообщения: сообщение инициатора, сообщение ответчика.

|  |
| --- |
|  |
| 1. – Исходный и зашифрованный алфавит с ключом |
|  |
| 1. – Сообщение инициатора и ответчика |

# 1. Теоретические сведения о шифре

## Основные определения

Шифр – система заранее оговоренных обратимых преобразований защищаемой информации (текста, изображений, аудио, видео и др.) с помощью ключа.

Ключ – переменный параметр для обратимых преобразований защищаемой информации (данных).

Ключ – минимальная информация, необходимая для обратимого преобразования защищаемой информации (шифрования и расшифрования, формирования и проверки контрольных сумм и др.).

Алфавит – это набор уникальных символов для записи шифрованных сообщений (буквы, цифры, знаки препинания, специальные символы и др.).

Мощность алфавита – полное число символов алфавита.

Шифр (общий случай) – множество обратимых функций отображения множества открытых сообщений на множество криптограмм , зависящих от выбранного ключа шифрования из множества и соответствующие им обратные функции расшифрования , зависящие от выбранного ключа расшифрования из множества , отображающие множество криптограмм на множество открытых сообщений .

## 1.2. Составные элементы шифра

К составным элементам шифра относится алфавит, алгоритмы обратимых преобразований исходного сообщения в криптограммы и обратного преобразования криптограмм в открытое сообщение (зашифрования и расшифрования), а также множество ключей.

## 1.3. Мощность алфавита (в общем случае)

Для русского языка мощность алфавита – 33, а для английского – 26.

Алфавит может дополнительно включать цифры, знаки препинания, специальные символы.

## 1.4. Запись общего алгоритма шифрования

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

## 1.5. Моноалфавитный шифр

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

– ключ,

– мощность алфавита

*–* символ на -й позиции исходного сообщения,

– символ на -й позиции криптограммы (замененный символ на -й позиции сообщения по ключу )

## 1.6. Шифра Цезаря

Шифра Цезаря – метод создания простого моноалфавитного шифра на основе ключа с постоянным параметром сдвига на символов.

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

– позиция символа в алфавите шифра

, – исходный и зашифрованные символы

– параметр сдвига (ключа)

– мощность алфавита шифра

# 2. Практическая часть

## 2.1. Зашифровка сообщения инициатора

|  |
| --- |
|  |
| 1. – Зашифровка сообщения (1 часть) |
|  |
| 1. – Зашифровка сообщения (2 часть) |
|  |
| 1. – Зашифровка сообщения (3 часть) |
|  |
| 1. – Результат шифрования |

## 2.2. Расшифровка сообщения инициатора

|  |
| --- |
|  |
| 1. – Расшифровка сообщения (1 часть) |
|  |
| 1. – Расшифровка сообщения (2 часть) |
|  |
| 1. – Расшифровка сообщения (3 часть) |
|  |
| 1. – Результат расшифрования |

## 2.3. Зашифровка сообщения ответчика

|  |
| --- |
|  |
| 1. – Зашифровка сообщения (1 часть) |
|  |
| 1. – Зашифровка сообщения (2 часть) |
|  |
| 1. – Зашифровка сообщения (3 часть) |
|  |
| 1. – Зашифровка сообщения (4 часть) |
|  |
| 1. – Результат шифрования |

## 2.4. Расшифровка сообщения ответчика

|  |
| --- |
|  |
| 1. – Расшифровка сообщения (1 часть) |
|  |
| 1. – Расшифровка сообщения (2 часть) |
|  |
| 1. – Расшифровка сообщения (3 часть) |
|  |
| 1. – Результат расшифрования |

# 3. Анализ частотности текста

## 3.1. Таблица и график частотности исходного алфавита

|  |
| --- |
|  |
| 1. – Таблица частоты исходного алфавита |
|  |
| 1. – График частотности исходного алфавита |

## 3.2. Таблица и график частотности исходного текста

|  |
| --- |
|  |
| 1. – Таблица частоты исходного текста |
|  |
| 1. – График частотности исходного текста |

## 3.3. Таблица и график частотности зашифрованного текста

|  |
| --- |
|  |
| 1. – Таблица частоты зашифрованного текста |
|  |
| 1. – График частотности зашифрованного текста |

# 4. Заключение

В ходе выполнения данной практической работы было реализовано шифрование и расшифрование сообщения с помощью моно алфавитного шифра, произведен анализ слабостей данного шифра. Были получены навыки по работе с Excel и реализацией алгоритмов шифрования.