|  |  |
| --- | --- |
| **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 3](#_Toc130123409)

[Исходные данные 3](#_Toc130123410)

[1. Теоретические сведения о шифре 4](#_Toc130123411)

[1.1. Основные определения 4](#_Toc130123412)

[1.2. Составные элементы шифра 5](#_Toc130123413)

[1.3. Мощность алфавита (в общем случае) 5](#_Toc130123414)

[1.4. Запись общего алгоритма шифрования 6](#_Toc130123415)

[1.5. Моноалфавитный шифр 6](#_Toc130123416)

[1.6. Шифра Цезаря 6](#_Toc130123417)

[2. Практическая часть 7](#_Toc130123418)

[2.1. Зашифровка сообщения инициатора 7](#_Toc130123419)

[2.2. Расшифровка сообщения инициатора 9](#_Toc130123420)

[2.3. Зашифровка сообщения ответчика 11](#_Toc130123421)

[2.4. Расшифровка сообщения ответчика 14](#_Toc130123422)

[3. Анализ частотности текста 16](#_Toc130123423)

[3.1. Таблица и график частотности исходного алфавита 16](#_Toc130123424)

[3.2. Таблица и график частотности исходного текста 17](#_Toc130123425)

[3.3. Таблица и график частотности зашифрованного текста 18](#_Toc130123426)

[4. Заключение 19](#_Toc130123427)

# 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.

В первую очередь необходимо обозначить исходный и зашифрованный алфавит, а также ключ 4, что было сделано на рис. 1.

|  |
| --- |
|  |
| 1. – Исходный и зашифрованный алфавит с ключом |

Далее указываем исходные сообщения инициатора и ответчика – рис.2

|  |
| --- |
|  |
| 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

На рис.3 – рис.5 представлена зашифровка сообщения инициатора.

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

А результат шифрования – рис.6.

|  |
| --- |
|  |
| 1. – Результат шифрования |

## 2.2. Расшифровка сообщения инициатора

На рис.7 – рис.9 представлена расшифровка сообщения инициатора.

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

А на рис. 10 – результат шифрования.

|  |
| --- |
|  |
| 1. – Результат расшифрования |

## 2.3. Зашифровка сообщения ответчика

На рис.11 – рис.14 содержится зашифровка сообщения ответчика.

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

А результат шифрования – это рис.15.

|  |
| --- |
|  |
| 1. – Результат шифрования |

## 2.4. Расшифровка сообщения ответчика

Следующий этап – это расшифровка, представленная на рис.16 – рис.18.

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

А результат расшифрования на рис.19.

|  |
| --- |
|  |
| 1. – Результат расшифрования |

# 3. Анализ частотности текста

## 3.1. Таблица и график частотности исходного алфавита

Рис. 20 – это частотность исходного алфавита, а на рис. 21 изображен график частотности.

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

## 3.2. Таблица и график частотности исходного текста

Рис. 22 – это частотность исходного текста, а на рис. 23 изображен график частотности.

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

## 3.3. Таблица и график частотности зашифрованного текста

Рис. 24 – это частотность зашифрованного текста, а на рис. 25 изображен график частотности.

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

## 3.3. Общие данные частотности

На рис. 26 представленная общая таблица в практической работе.

|  |
| --- |
|  |
| 1. – Общая таблица частотности |

# 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.