|  |  |
| --- | --- |
| **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  Пономарев А.Д.  Проверил:  Доцент кафедры УиЗи, к.т.н., с.н.с.  Михалевич И.Ф. |
| Москва 2023 | |

**Оглавление**

[Задание 3](#_Toc129556737)

[Исходные данные 3](#_Toc129556738)

[1. Краткие теоритические сведения о шифре 4](#_Toc129556739)

[1.1 Определения шифра и ключа 4](#_Toc129556740)

[1.2. Составные элементы шифра 4](#_Toc129556741)

[1.3. Алфавит 4](#_Toc129556742)

[1.4. Определение шифра в общем случае 5](#_Toc129556743)

[1.5. Моноалфавитный шифр 5](#_Toc129556744)

[1.6. Шифр Цезаря 5](#_Toc129556745)

[2. Практическая часть 7](#_Toc129556746)

[2.1. Зашифровка сообщения инициатора 7](#_Toc129556747)

[2.2. Расшифровка сообщения инициатора 9](#_Toc129556748)

[2.3. Зашифровка сообщения ответчика 11](#_Toc129556749)

[2.4. Расшифровка сообщения ответчика 13](#_Toc129556750)

[4. Заключение 14](#_Toc129556751)

# Задание

1. Разработать моноалфавитный шифр, таблицы шифрования/расшифрования (для варианта шифра).

2. Подготовить сообщение (конкатенация сообщений инициатора и ответчика).

3. Зашифровать и расшифровать сообщение.

4. Провести анализ слабостей шифра (привести таблицы и гистограммы частотности символов исходного алфавита и сообщения, зашифрованного разработанным шифром, описать слабости шифра).

5. Оформить отчет.

# Исходные данные

1. Сообщение, передаваемое инициатором:

«Уважаемый Игорь Феодосьевич, сообщаю Вам, что я выполнил практическое задание номер три, Пономарев Антон Дмитриевич 09.10.2002.».

1. Сообщение, передаваемое ответчиком:

«Уважаемый Антон Дмитриевич, я безмерно рад нашему сотрудничеству, Надеюсь на его дальнейшее успешное и взаимовыгодное развитие. С уважением Игорь Феодосьевич.».

1. Ключ = 13

# 1. Краткие теоритические сведения о шифре

## Определения шифра и ключа

Шифр – система заранее оговоренных обратимых преобразований защищаемой информации (текста, изображений, аудио, видео, ...) 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, ...).

## 1.2. Составные элементы шифра

* алфавит;
* алгоритмы обратимых преобразований исходного сообщения в криптограммы и обратного преобразования криптограмм в открытое сообщение (зашифрования и расшифрования);
* множество ключей.

## 1.3. Алфавит

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

Мощность алфавита –полное число символов алфавита.

Мощность алфавита (в общем случае):

* русского языка – 33
* английского – 26

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

## 1.4. Определение шифра в общем случае

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

Запись алгоритма шифрования (общего)

Еk , k ∈ KED : M → C ,

Dk , k ∈ KED : C → M ,

∀k ∈ KE ∃k ∈ KD ,

∀m ∈ M : Еk(m) = c ,

∀c ∈ C : Dk(c) = m

## 1.5. Моноалфавитный шифр

*Ci* = *Mi* + *K* mod *n*

*Mi* = *Ci* – *K* mod *n*

*K* – ключ, 0 < *K* ≤ *n*

*n* – мощность алфавита

*Mi* – символ на *i*-й позиции исходного сообщения, *i* ∈ *N*

*Ci* – символ на *i*-й позиции криптограммы (замененный символ *M* на *i*-й позиции сообщения по ключу *K*)

## 1.6. Шифр Цезаря

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

*E*: *Ci* = *Mi* + *K* mod *n*

*D: Mi* = *Ci* – *K* mod *n*

*i* – позиция символа в алфавите шифра

*Mi* , *Ci* – исходный и зашифрованный символы

*К* – параметр сдвига (ключ)

*n* – мощность алфавита шифра.

# 2. Практическая часть

## 2.1. Зашифровка сообщения инициатора

|  |
| --- |
|  |
| 1. – Зашифровка сообщения |
|  |
| 1. – Результат шифрования |

## 2.2. Расшифровка сообщения инициатора

|  |
| --- |
|  |
| 1. – Расшифровка сообщения |
|  |
| 1. – Результат расшифровки |

## 2.3. Зашифровка сообщения ответчика

|  |
| --- |
|  |
| 1. – Зашифровка сообщения ответчика |
|  |
| 1. – Результат шифрования |

## 2.4. Расшифровка сообщения ответчика

|  |
| --- |
|  |
| 1. – Расшифровка сообщения |
|  |
| 1. – Результат расшифровки |

# 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.