|  |  |
| --- | --- |
| **Российский университет транспорта (МИИТ)**  **Институт транспортной техники и систем управления**  **Кафедра «Управление и защита информации»** | |
| **Отчет**  **по практическому заданию**  **по теме «Разработка семейства полиалфавитных шифров: шифр 1»**  **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](#_Toc131711396)

[Исходные данные 4](#_Toc131711397)

[1. Краткие теоритические сведения о шифре 5](#_Toc131711398)

[1.1 Определения шифра и ключа 5](#_Toc131711399)

[1.2. Составные элементы шифра 5](#_Toc131711400)

[1.3. Алфавит 5](#_Toc131711401)

[1.4. Определение шифра в общем случае 6](#_Toc131711402)

[1.5. Полиалфавиный шифр 6](#_Toc131711403)

[1.6. Полиалфавитный шифр на основе ключевой последованности 7](#_Toc131711404)

[2. Практическая часть 8](#_Toc131711405)

[2.1. Зашифровка сообщения 8](#_Toc131711406)

[2.2. Расшифровка сообщения 10](#_Toc131711407)

[3. Анализ частотности текста 12](#_Toc131711408)

[3.1. Таблица и график частотности исходного алфавита 12](#_Toc131711409)

[3.2. Таблица и график частотности исходного текста 13](#_Toc131711410)

[3.3. Таблица и график частотности зашифрованного текста (шифр Цезаря) 14](#_Toc131711411)

[3.4. Таблица и график частотности зашифрованного текста (шифр 1) 15](#_Toc131711412)

[4. Заключение 16](#_Toc131711413)

# Задание

1. Разработать базовый полиалфавитный шифр.
2. Разобрать таблицы шифрования/расшифрования для шифра №1.
3. Подготовить, зашифровать и расшифровать сообщение.
4. Провести анализ слабостей шифра.
5. Оформить отчет.

# Исходные данные

1. Тип полиалфавитного шифра – квадрат Виженера (базовый, первая строка начинается с первого символа алфавита шифра).
2. Первая строка квадрата соответствует моноалфавитному шифру студента.
3. Первичный ключ шифра – ШИФРОВАНИЕ
4. Ключевая последовательность – повторение первичного ключа до размера передаваемого сообщения.
5. Передаваемое сообщение: «Уважаемый Игорь Феодосьевич, спешу сообщить Вам о том, что практическая работа 5 выполнена и готова к проверке. Дроздов Антон Дмитриевич 03.12.2002. Уважаемый Антон Дмитриевич, я безмерно рад нашему сотрудничеству, надеюсь на его дальнейшее успешное и взаимовыгодное развитие. С уважением, Игорь Феодосьевич».

# 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. Полиалфавиный шифр

Полиалфавитный шифр замены – шифр, при котором символы исходного сообщения заменяются символами исходного алфавита с переменным сдвигом по ключу.

Полиалфавитный шифр на основе ключевой последовательности:

Первичный ключ – любое слово или фраза.

Ключевая последовательность – последовательность символов, сформированная повторением первичного ключа до размера шифруемого сообщения.

*Mi*– символ на *i*-й позиции сообщения, *i ∈ Z.*

*Ci*– символ на *i*-й позиции криптограммы.

*Ci*– суперпозиция *i*-го символа сообщения и *i*-го символа ключевой последовательности.

*Ci*= *Mi*& *Si*

*Mi*= *Ci*& *Si*

## 1.6. Полиалфавитный шифр на основе ключевой последованности

Шифр Виженера – метод простого полиалфавитного шифра замены на основе ключевого слова, преобразованного в одноразмерный с сообщением ключ, задающий переменный параметр *ki* сдвига символов исходного сообщения.

*ki* – переменный параметр сдвига по ключевому слову.

|  |
| --- |
|  |
| 1. – Квадрат Виженера |

# 2. Практическая часть

## 2.1. Зашифровка сообщения

Ниже, на рисунке 2, представлена таблица порядка действий зашифровки исходного текста инициатора, а на рисунке 3, представлена таблица результата шифрования и длины сообщений.

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

## 2.2. Расшифровка сообщения

Ниже, на рисунке 4, представлена таблица порядка действий расшифровки текста, для получения исходного, а на рисунке 5, представлена таблица результата расшифровки и длины сообщений.

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

# 3. Анализ частотности текста

## 3.1. Таблица и график частотности исходного алфавита

Ниже, на рисунке 6, представлена таблица частотности исходного алфавита в порядке уменьшения, а на рисунке 7, представлен график построенный на основе данной таблицы.

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

## 3.2. Таблица и график частотности исходного текста

Ниже, на рисунке 8, представлена таблица частотности использования алфавита в исходном тексте в порядке уменьшения, а на рисунке 9, представлен график построенный на основе данной таблицы.

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

## 3.3. Таблица и график частотности зашифрованного текста (шифр Цезаря)

Ниже, на рисунке 10, представлена таблица частотности использования алфавита в зашифрованном тексте в порядке уменьшения, а на рисунке 11, представлен график построенный на основе данной таблицы.

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

## 3.4. Таблица и график частотности зашифрованного текста (шифр 1)

Ниже, на рисунке 12, представлена таблица частотности использования алфавита в зашифрованном тексте в порядке уменьшения, а на рисунке 13, представлен график построенный на основе данной таблицы.

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

# 4. Заключение

В ходе выполнения данной практической работы было реализован полиалфавитный шифр на основе квадрата Виженера, таблицы шифрования/расшифрования, зашифровано и расшифровано сообщение. Проведен анализ слабостей шифра, приведены таблицы и гистограммы частотности символов исходного алфавита и сообщения, зашифрованного разработанным шифром, описаны слабости шифра. Проведен сравнительный анализ моноалфавитного и полиалфавитного шифров, в результате чего выяснилось, что последний обладает большей криптостойкостью. Получены навыки в работе с полиалфавитными шифрами в Excel.