|  |  |
| --- | --- |
| **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 2»**  **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. Разобрать таблицы шифрования/расшифрования для шифра №2.
2. Подготовить, зашифровать и расшифровать сообщение.
3. Провести анализ слабостей шифра, сравнить с результатами предыдущих заданий.
4. 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. Размер шифруемого блока = мощность алфавита = 46.
4. С переходом к следующему блоку применяется следующий моноалфавитный шифр (следующая строка базового шрифта).
5. Передаваемое сообщение: «Уважаемый Игорь Феодосьевич, спешу сообщить Вам о том, что практическая работа 6 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

## Полиавлфавиный 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*

## 1.2. Определение полиафавитного шифра замены

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

## 1.3. Полиалфавитный шифр на основе шифрования блоков

Полиалфавитный шифр – квадрат Виженера с ключом студента.

Сообщение разбивается на блоки длиной *n*, соответствующей мощности моноалфавитного шифра.

Строки квадрата полиалфавитного шифра нумеруются от 0 до *n* – 1.

Нулевая строка в шифровании не участвует.

*Mi* – символ на *i*-й позиции сообщения.

*Mj*– символ на *j*-й позиции в *l*-м блоке сообщения, *l* = 1, … , *L*.

*j* = *i*/*n* mod *n* – позиция *i*-го символа в блоке.

*L* = [*I*/*n*] – число блоков сообщения, *I* – объем сообщения.

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

*Ci*= *Mi (l)*, *l* = [*i*/*n*] + 1 mod *n*

## 1.4. Пример квадрата Виженера для блочного шифрования

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

# 2. Практическая часть

## 2.1. Исходные данные

Ниже, на рисунке 2, представлены исходные данные, используемые в нашей практической работе, а на рисунке 3, представлен квадрат Виженера.

|  |
| --- |
|  |
| 1. – Исходные данные |
|  |
| 1. – Блокнот шифрования (таблица шифрования, шифр) |

## 2.1. Зашифровка сообщения

Ниже, на рисунке 4, представлена таблица порядка действий зашифровки исходного текста инициатора, а на рисунке 5, представлена таблица результата шифрования и длины сообщений.

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

## 2.2. Расшифровка сообщения

Ниже, на рисунке 6, представлена таблица порядка действий расшифровки текста, для получения исходного, а на рисунке 7, представлена таблица результата расшифровки и длины сообщений.

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

# 3. Анализ частотности шифров

Ниже, на рисунке 8, представлена сравнительная таблица частотности.

|  |
| --- |
|  |
| 1. – Таблица сравнения частоты |

Далее, на рисунке 9 представлен график частотности исходного алфавита. На рисунке 10 – график исходного текста.

|  |
| --- |
|  |
| 1. – График частотности исходного алфавита |
|  |
| 1. – График частотности исходного текста |

Рисунок 11 – это график частотности зашифрованного текста шифров Цезаря.

|  |
| --- |
|  |
| 1. – График частотности текста (на основе Цезаря) |

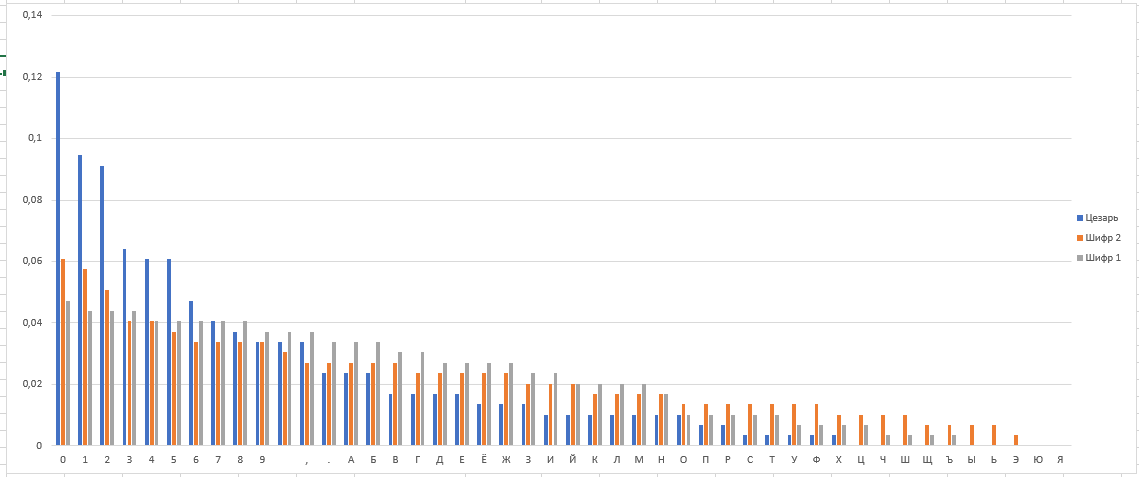
А на рисунках 12 и 13 – графики частотности зашифрованного текста на основе шифра 1 и блочного шифра соответственно.

|  |
| --- |
|  |
| 1. – График частотности текста (на основе шифра 1) |
|  |
| 1. – График частотности текста (на основе блочного шифра) |

# 4. Сравнение шифров

В сравнении с моноалфавитным шифром (на основе шифра Цезаря) и полиалфавитным шифром (на основе квадрата Виженера), полиалфавитный шифр, основанный на блочной шифровании обладает большей криптостойкостью, это можно заметить, исследуя частотность символов зашифрованного текста. Частоты символов при применении полиалфавитного шифра с блочным шифрованием распределены более равномерно, что значительно усложняет подбор ключа. Криптостойкость полиалфавитного шифра на основе шифрования блоков зависит от размера блоков, размера ключа и числа раундов шифрования. Чем хуже эти характеристики, тем меньше усилий понадобится злоумышленнику для нахождения ключа и взлома шифра.

Ниже, на рисунке 14, представлен график частотностей каждого шифра.



|  |
| --- |
| 1. – Общий график сравнения шифров |

# 5. Заключение

В ходе выполнения данной практической работы был реализован полиалфавитный шифр на основе шифрования блоков, 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 шифра, полиалфавитного шифров и полиалфавитного шифра на основе шифрования блоков, в результате чего выяснилось, что последний обладает наибольшей криптостойкостью. Получены навыки в работе с полиалфавитными шифрами в Excel.