|  |  |
| --- | --- |
| **Российский университет транспорта (МИИТ)**  **Институт транспортной техники и систем управления**  **Кафедра «Управление и защита информации»** | |
| **Отчёт**  **по практическому заданию**  **по теме «Разработка полиалфавитного шифра 1 (на основе ключевой последовательности)»**  **по дисциплине «Криптографические методы защиты информации»** | |
|  | Выполнил:  Студент группы ТКИ-342  Белов С.В.  Проверил:  Доцент кафедры УиЗИ, к.т.н., с.н.с  Михалевич И.Ф. |
| Москва 2023 | |

**ОГЛАВЛЕНИЕ**

[ЗАДАНИЕ 4](#_Toc103678252)

[ИСХОДНЫЕ ДАННЫЕ 5](#_Toc103678253)

[1. Краткие теоретические сведения о шифре 6](#_Toc103678254)

[1.1. Определения шифра и ключа 6](#_Toc103678255)

[1.2. Составные элементы шифра 6](#_Toc103678256)

[1.3. Алфавит 6](#_Toc103678257)

[1.4. Определение шифра в общем случае 7](#_Toc103678258)

[1.5. Полиалфавитный шифр 7](#_Toc103678259)

[1.6. Полиалфавитный шифр на основе ключевой последовательности 8](#_Toc103678260)

[1.6.1 Шифр Виженера 8](#_Toc103678261)

[1.6.2 Квадрат Виженера: 8](#_Toc103678262)

[1.6.3 Шифрование по ключевому слову при начальном ключе k = 0 9](#_Toc103678263)

[1.6.4 Шифрование по ключевому слову при начальном ключе k = 32 10](#_Toc103678264)

[1.6.5 Длина ключа 10](#_Toc103678265)

[1.6.6 Зависимость полиафавитного шифрования от качества ключа 12](#_Toc103678266)

[1.7. Некоторые пути повышения стойкости шифрования 13](#_Toc103678267)

[2. Практическая часть 14](#_Toc103678268)

[2.1. Исходные данные 14](#_Toc103678269)

[2.2. Квадрат Виженера 14](#_Toc103678270)

[2.3. Зашифровка и расшифровка сообщения 15](#_Toc103678271)

[2.3.1 Зашифровка сообщения 15](#_Toc103678272)

[2.3.2 Расшифровка сообщения 16](#_Toc103678273)

[2.4. Анализ частотности текста 18](#_Toc103678274)

[2.4.1 Частотность символов алфавита 18](#_Toc103678275)

[2.4.2 Частотность символов исходного текста 19](#_Toc103678276)

[2.4.3 Частотность символов текста, зашифрованного моноалфавитным шифром (на основе шифра Цезаря) 20](#_Toc103678277)

[2.4.4 Частотность символов текста, зашифрованного полиалфавитным шифром 1 (с использованием ключевой последовательности) 21](#_Toc103678278)

[2.4.5 Анализ графиков частотности 22](#_Toc103678279)

[2.5. Результаты частотного анализа 24](#_Toc103678280)

[ЗАКЛЮЧЕНИЕ 25](#_Toc103678281)

ЗАДАНИЕ

1. Разработать базовый полиалфавитный шифр.
2. Разработать таблицы шифрования/расшифрования для шифра.
3. Подготовить, зашифровать и расшифровать сообщение.
4. Провести анализ слабостей шифра, сравнить с результатами предыдущих заданий.
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 – Криптограф
4. Ключевая последовательность – повторение первичного ключа до размера передаваемого сообщения: КриптографКриптографКриптографКриптограф…
5. Передаваемое сообщение: «Уважаемый Игорь Феодосьевич, спешу сообщить вам о том, что вторая практическая работа готова к проверке. 6.08.2002. Белов Сергей Владимирович Уважаемый, Сергей Владимирович, безмерно рад нашему сотрудничеству, надеюсь на его дальнейшее успешное и взаимовыгодное развитие. С уважением, Игорь Феодосьевич».
6. Краткие теоретические сведения о шифре
   1. 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. Составные элементы шифра
* алфавит;
* алгоритмы обратимых преобразований исходного сообщения в криптограммы и обратного преобразования криптограмм в открытое сообщение (зашифрования и расшифрования);
* множество ключей.
  1. 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. 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* : *Е*k(*m*) = *c* ,

*c*  *C* : *Dk*(*c*) = *m*

* 1. Полиалфавитный 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. Полиалфавитный шифр на основе ключевой последовательности
     1. Шифр Виженера

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:

|  |
| --- |
|  |

* + 1. Шифрование по ключевому слову при начальном ключе k = 0

|  |
| --- |
|  |

* + 1. Шифрование по ключевому слову при начальном ключе k = 32

|  |
| --- |
|  |

* + 1. Длина ключа

|  |
| --- |
| Изображение выглядит как текст  Автоматически созданное описание |

Ключ подготавливается равным длине сообщения, одному и тому же символу сообщения соответствуют разные символы шифрограммы.

Фактически для шифрования задействуется не весь набор моноалфавитных шифров (таблица), а только часть, соответствующая значениям уникальных элементов ключевой последовательности (2 значения)

|  |
| --- |
|  |

Фактически для шифрования задействуется не весь набор моноалфавитных шифров (таблица), а только часть, соответствующая значениям уникальных элементов ключевой последовательности (5 значений)

|  |
| --- |
|  |

* + 1. Зависимость полиафавитного шифрования от качества ключа

Криптограмма фактически не скрывает сообщение

|  |
| --- |
|  |

Криптограмма скрывает сообщение

|  |
| --- |
|  |

* 1. Некоторые пути повышения стойкости шифрования

1. Применение ключей, обладающих специальными свойствами (случайных, псевдослучайных последовательностей).
2. Смена сеансовых ключей.
3. Дополнение сообщений до заданного минимального объема.

Как минимум задействование всего квадрата моноалфавитных шифров!!!

1. Практическая часть
   1. Исходные данные

|  |
| --- |
|  |

|  |
| --- |
|  |

* 1. Квадрат Виженера
  2. Зашифровка и расшифровка сообщения
     1. Зашифровка сообщения

|  |
| --- |
|  |

Для разделения сообщения на отдельные символы используем функцию =ПСТР(B$2;A11;1), где первый аргумент – разделяемый текст, второй – начальная позиция, третий – количество символов.

Чтобы перевести символы исходного алфавита в символы зашифрованного, используем формулу: =ДВССЫЛ(АДРЕС(ПОИСКПОЗ(C11;КлючПослед;0)+1;ПОИСКПОЗ(B11;Симв;0)+1;;;"Квадрат Виженера")).

|  |
| --- |
|  |

* + 1. Расшифровка сообщения

|  |
| --- |
|  |

Для расшифровки сообщения используем формулу =ЕСЛИ(B11=C11;"A";ДВССЫЛ(АДРЕС(1;ПОИСКПОЗ(B11;СМЕЩ(Нач;ПОИСКПОЗ(C11;КлючПослед;0);0;1;46);0);;;"Квадрат Виженера"))).

|  |
| --- |
|  |

* 1. Анализ частотности текста
     1. Частотность символов алфавита

|  |
| --- |
|  |

* + 1. Частотность символов исходного текста

|  |
| --- |
|  |

* + 1. Частотность символов текста, зашифрованного моноалфавитным шифром (на основе шифра Цезаря)

|  |
| --- |
|  |

* + 1. Частотность символов текста, зашифрованного полиалфавитным шифром 1 (с использованием ключевой последовательности)

|  |
| --- |
|  |

* + 1. Анализ графиков частотности

|  |
| --- |
|  |

|  |
| --- |
|  |

|  |
| --- |
|  |
|  |

* 1. Результаты частотного анализа

В сравнении с моноалфавитным шифром, в нашем случае это шифр Цезаря, полиалфавитный шифр на основе квадрата Виженера обладает большей криптостойкостью, это можно заметить, исследуя частотность символов зашифрованного текста. Частоты символов при применении полиалфавитного шифра распределены более равномерно, что значительно усложняет подбор ключа. Криптостойкость шифра Виженера зависит от сложности ключа, а именно от его размера и количества используемых символов. Если ключ будет недостаточно сложным, то злоумышленник сможет восстановить шифруемое сообщение.

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.