МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждения образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Лабораторная работа №4**

по дисциплине «Криптографические методы защиты информации»

на тему: ИССЛЕДОВАНИЕ КРИПТОГРАФИЧЕСКИХ ШИФРОВ НА ОСНОВЕ ПОДСТАНОВКИ (ЗАМЕНЫ) СИМВОЛОВ

Выполнил студентка 3 курса 5 группы специальность ПОИТ Буранко В.Д.

(Ф.И.О.)

Преподаватель ассистент Савельева Маргарита Геннадьевна

(Ф.И.О.)

Содержание

[**Теоретические сведения** 3](#_Toc130744489)

[**Практические задания** 6](#_Toc130744490)

[Задание 1 6](#_Toc130744491)

[Задание 2 8](#_Toc130744492)

[Задание 3 9](#_Toc130744493)

[**Выводы** 10](#_Toc130744494)

**Цель:** изучение и приобретение практических навыков разработки и использования приложений для реализации подстановочных шифров.

**Задачи:**

* Закрепить теоретические знания по алгебраическому описанию, алгоритмам реализации операций зашифрования/расшифрования и оценке криптостойкости подстановочных шифров;
* Ознакомиться с особенностями реализации и свойствами различных подстановочных шифров;
* Разработать приложение для реализации указанных преподавателем методов подстановочного зашифрования/расшифрования;
* Выполнить исследование криптостойкости шифров на основе статистических данных о частотах появления символов в исходном и зашифрованном сообщениях;
* Оценить скорость зашифрования/расшифрования реализованных способов шифров;
* Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

# **Теоретические сведения**

**Сущность подстановочного шифрования** состоит в том, что исходный текст (из множества *М*) и зашифрованный текст (из множества *С*) основаны на использовании одного и того же или разных алфавитов, а тайной или ключевой информацией является алгоритм подстановки.

Если в сообщении *Мi* содержится несколько букв *ax*, то каждая из них заменяется на символ *ay* либо на любой из символов {*АхС*}. За счет этого с помощью одного ключа можно сгенерировать различные *Сi* для одного и того же *Мi*. Так как множества {*АхС*}*b* и {*АхС*}*n* попарно не пересекаются, то по каждому символу *С* можно однозначно определить, какому множеству он принадлежит, и, следовательно, какую букву открытого сообщения *Мi* он заменяет. В силу этого открытое сообщение восстанавливается из зашифрованного однозначно.

Приведенные утверждения справедливы для следующих типов подстановочных шифров:

* *моноалфавитных* (шифры однозначной замены или простые подстановочные);
* *полиграммных*;
* *омофонических* (однозвучные шифры или шифры многозначной замены);
* *полиалфавитных*.

Для математического описания криптографического преобразования предполагаем, что зашифрованная буква *ay* (*ay* ∈ *Сi*), соответствующая символу *aх* (*aх* ∈ *Мi*), находится на позиции

где *x*, *y* – индекс (порядковый номер, начиная с 0) символа в используемом алфавите; *k* – ключ.

Для расшифрования сообщения *Сi* необходимо произвести расчеты, обратные выражению (2.1), т. е.

(2.2)

Соотношениям (2.1) и (2.2) соответствует классический шифр подстановки – *шифр Цезаря*.

В данных шифрах операция замены производится раздельно над каждым одиночным символом сообщения *Мi*.

Применяя одновременно операции сложения и умножения по модулю n над элементами множества (индексами букв алфавита), можно получить систему подстановок, которую называют ***аффинной системой подстановок Цезаря***. Определим процедуру зашифрования в такой системе:

(2.3)

где *a* и *b* – целые числа.

При этом взаимно однозначные соответствия между открытым текстом и шифртекстом будут иметь место только при выполнении следующих условий: 0 ≤ *a*, *b* < *N*, наибольший общий делитель (НОД) чисел *a*, *N* равен 1, т. е. эти числа являются *взаимно простыми*.

В ***полиграммных шифрах*** одна подстановка соответствует сразу нескольким символам исходного текста.

***Омофонические* *шифры*** (***омофоническая замена***), или однозвучные шифры подстановки, создавались с целью увеличить сложность частотного анализа шифртекстов путем маскировки реальных частот появления символов текста с помощью *омофонии*.

***Полиалфавитные*** (или ***многоалфавитные***) ***шифры*** состоят из нескольких шифров однозначной замены. Выбор варианта алфавита для зашифрования одного символа зависит от особенностей метода шифрования.

***Шифр Виженера***. В 1586 г. французский дипломат Блез Виженер представил перед комиссией Генриха III описание простого, но довольно стойкого шифра, в основе которого лежит таблица Трисемуса.

В этом шифре мы имеем дело с последовательностью сдвигов, циклически повторяющейся. Основная идея заключается в следующем. Создается таблица (таблица Виженера) размером *N*×*N* (*N* – число знаков в используемом алфавите). Эти знаки могут включать не только буквы, но и, например, пробел или иные знаки. В первой строке таблицы записывается весь используемый алфавит. Каждая последующая строка получается из предыдущего циклического сдвига последней на 1 символ влево. Таким образом, при мощности алфавита (английского языка), равной 26, необходимо выполнить последовательно 25 сдвигов для формирования всей таблицы.

# **Практические задания**

Разработать авторское приложение в соответствии с целью лабораторной работы. Приложение должно реализовывать следующие операции:

Задание 1:

* выполнять зашифрование/расшифрование текстовых документов (объемом не менее 5 тысяч знаков), созданных на основе алфавита языка в соответствии с нижеследующей таблицей вариантов задания; при этом использованы шифр на основе аффинной системы подстановок Цезаря (a = 7, b = 10) и шифр Виженера (ключевое слово — собственная фамилия);



Рисунок 1 — Содержание документа с исходным текстом



Рисунок 2 — Содержание документа, содержащего зашифрованный исходный текст при помощи аффинного шифра Цезаря



Рисунок 3 — Содержание документа, содержащего расшифрованный текст при помощи аффинного шифра Цезаря



Рисунок 4 — Содержание документа, содержащего зашифрованный исходный текст при помощи шифра Виженера



Рисунок 5 — Содержание документа, содержащего расшифрованный текст при помощи шифра Виженера

Задание 2:

* сформировать гистограммы частот появления символов для исходного и зашифрованного сообщений;

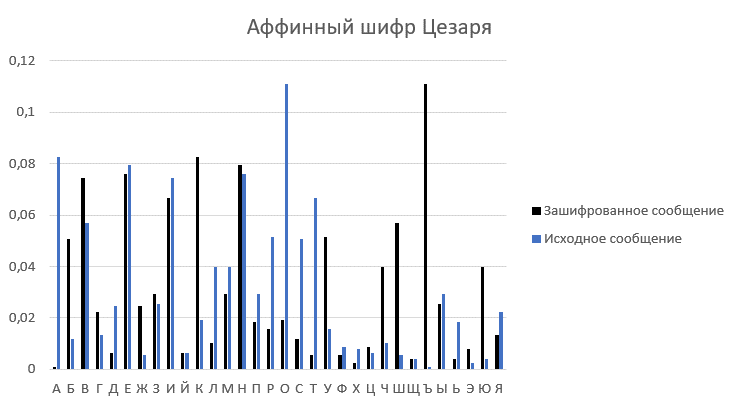


Рисунок 6 — Гистограмма частот появления символов для зашифрованного и исходного сообщения при помощи аффинного шифра Цезаря

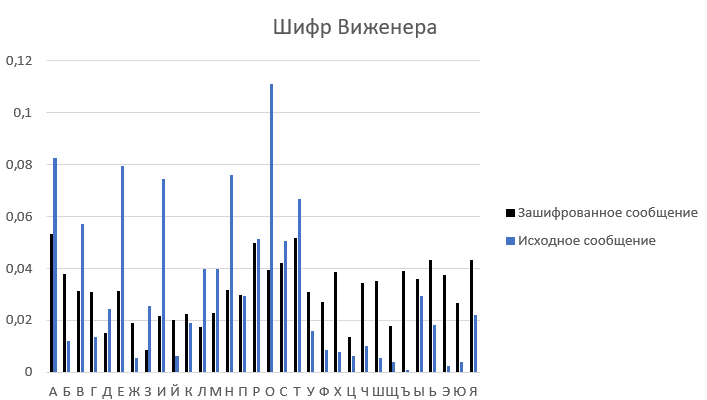


Рисунок 7 — Гистограмма частот появления символов для зашифрованного и исходного сообщения при помощи шифра Виженера

Задание 3:

* оценить время выполнения операций зашифрования/расшифрования.

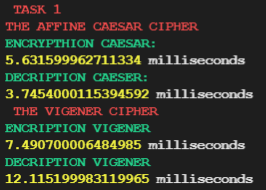


Рисунок 8 — Время выполнения операций зашифрования/расшифрования для аффинного шифра Цезаря и шифра Виженера

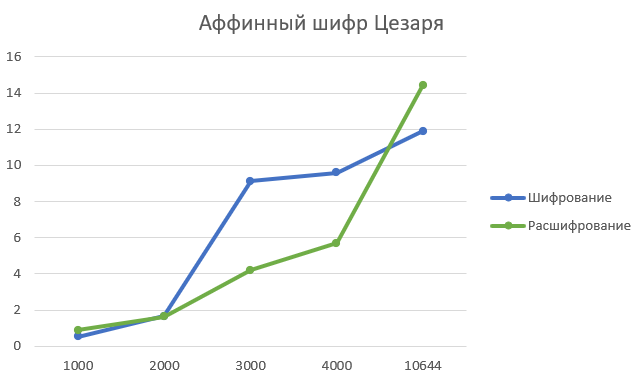


Рисунок 9 — Зависимость времени выполнения зашифрования/расшифрования от количества символов для аффинного шифра Цезаря

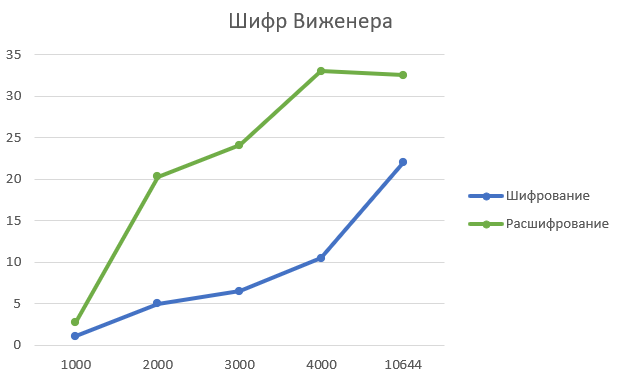


Рисунок 10 — Зависимость времени выполнения зашифрования/расшифрования от количества символов для шифра Виженера

# **Выводы**

В ходе выполнения лабораторной работы было разработано приложение, позволяющее выполнять функции зашифрования и расшифрования при помощи шифра на основе аффинной системы подстановок Цезаря и шифра Виженера. Так же были построены гистограммы частот появления символов для зашифрованного и исходного сообщений и график зависимости времени выполнения зашифрования/расшифрования от количества символов.