Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ  
ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий

[Кафедра информационных](https://www.belstu.by/fakultety/fit/vm) систем и технологий

Специальность 1-40 01 01 Программное обеспечение информационных технологий

**Отчёт по лабораторной работе №4**

по дисциплине Информационная безопасность

Тема: Исследование криптографических шифров на основе подстановки (замены) символов

Исполнитель:

Студент 3 курса группы 6

Руководитель:

Ассистент Нистюк О. А.

Минск, 2024

**Лабораторная работа №4**

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

**Задачи:**

1. Закрепить теоретические знания по алгебраическому описанию, алгоритмам реализации операций зашифрования/расшифрования и оценке криптостойкости подстановочных шифров.

2. Ознакомиться с особенностями реализации и свойствами различных подстановочных шифров на основе готового программного средства (L\_LUX).

3. Разработать приложение для реализации указанных преподавателем методов подстановочного зашифрования/расшифрования.

4. Выполнить исследование криптостойкости шифров на основе статистических данных о частотах появления символов в исходном и зашифрованном сообщениях.

5. Оценить скорость зашифрования/расшифрования реализованных способов шифров.

6. 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.

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

Максимальное количество ключей для любого шифра этого вида не превышает N!, где N – количество символов в алфавите.

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

y ≡ x + k mod N,

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

Для расшифрования сообщения Сi необходимо произвести расчеты, обратные выражению, т. е.

х ≡ у – k mod N.

Одним из существенных недостатков моноалфавитных шифров является их низкая криптостойкость. Зачастую метод криптоанализа базируется на частоте встречаемости букв исходного текста.

Система шифрования Цезаря с ключевым словом (лозунгом) также является одноалфавитной системой подстановки. Особенностью этой системы является использование ключевого слова (лозунга) для смещения и изменения порядка символов в алфавите подстановки (желательно, чтобы все буквы ключевого слова были различными). Ключевое слово пишется в начале алфавита подстановки.

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:

y ≡ ax + b mod N,

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.

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

Таблица Трисемуса. Зашифрование осуществляется так: заготавливается таблица подстановки (так называемая «таблица Трисемуса» – таблица со стороной, равной N, где N – мощность алфавита), где первая строка – это алфавит, вторая – алфавит, сдвинутый на один символ, и т. д. При зашифровании первая буква открытого текста заменяется на букву, стоящую в первой строке, вторая – на букву, стоящую во второй строке, и т. д. После использования последней строки вновь возвращаются к первой. При шифровании с ключевым словом буква открытого текста заменяется буквой, расположенной ниже нее в том же столбце. Если буква текста оказывается в нижней строке таблицы, тогда для шифртекста берут самую верхнюю букву из того же столбца.

Шифр Виженера. 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.

Криптоанализ – это раздел криптологии, занимающийся методами взлома шифров или методами организации криптографических атак на шифры.

Основные криптоатаки:

* Атака с известным шифртекстом;
* Атака с выбором шифртекста;
* Адаптивная атака с выбором шифртекста;
* Атака с известным открытым текстом;
* Атака с выбором открытого текста;
* Адаптивная атака с выбором открытого текста;
* Атака на основе связанных ключей;
* Атака с выбором ключа.

# Ход работы

Целью работы была разработка приложения, позволяющего выполнять шифрование/расшифрование текстовых документов, созданных на основе алфавита белорусского языка.

Для начала, был реализован алгоритм шифрования и расшифрования с помощью шифра Цезаря с ключевым словом. Функция шифрования caesarEncode принимает на вход исходный текст и алфавит подстановки. Код функции представлен на рисунке 2.1.



Рисунок 2.1 – Код функции шифрования с помощью шифра Цезаря

Функция расшифрования caesarDecode принимает на вход зашифрованный текст и алфавит подстановки. Код функции представлен на рисунке 2.2.

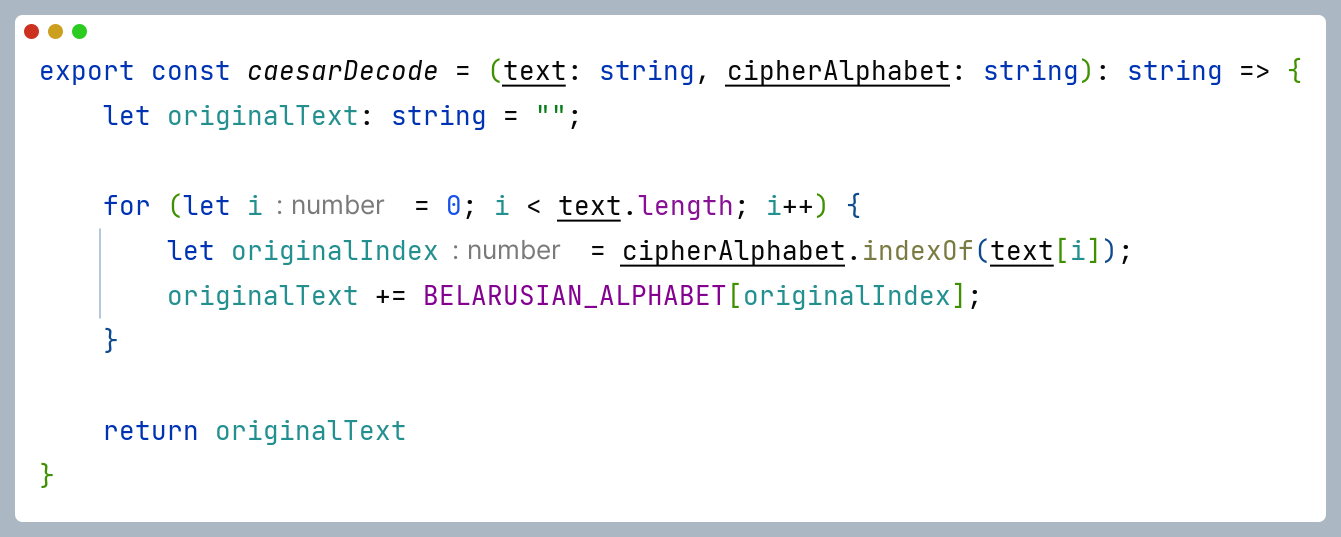


Рисунок 2.2 – Код функции расшифрования шифра Цезаря

Результат работы функций приведен на рисунке 2.3.



Рисунок 2.3 – Результат шифрования и дешифрования текста с помощью шифра Цезаря с ключевым словом «інфарматыка»

Далее, нужно было сформировать гистограммы частот появления символов для исходного и зашифрованного сообщений. Гистограмма частот появления символов исходного сообщения приведена на рисунке 2.4.

Рисунок 2.4 – Гистограмма частот появления символов исходного сообщения

Гистограмма частот появления символов зашифрованного сообщения приведена на рисунке 2.5.

Рисунок 2.5 – Гистограмма частот появления символов зашифрованного сообщения

Сопоставив гистограммы частот появления символов исходного и зашифрованного сообщений можно определить алфавит подстановки.

Также было определено, что как зашифрование, так и расшифрование текста с помощью шифра Цезаря выполняется примерно за 1.5-2 миллисекунды.

Затем были разработаны несколько функций, выполняющих шифрование и дешифрование текста с использованием таблицы Трисемуса, где ключевое слово – собственное имя.

Сначала была разработана функция formTrithemiusTable, которая принимает размер таблицы и с помощью ключевого слова формирует результирующую таблицу Трисемуса. Код функции представлен на рисунке 2.6.

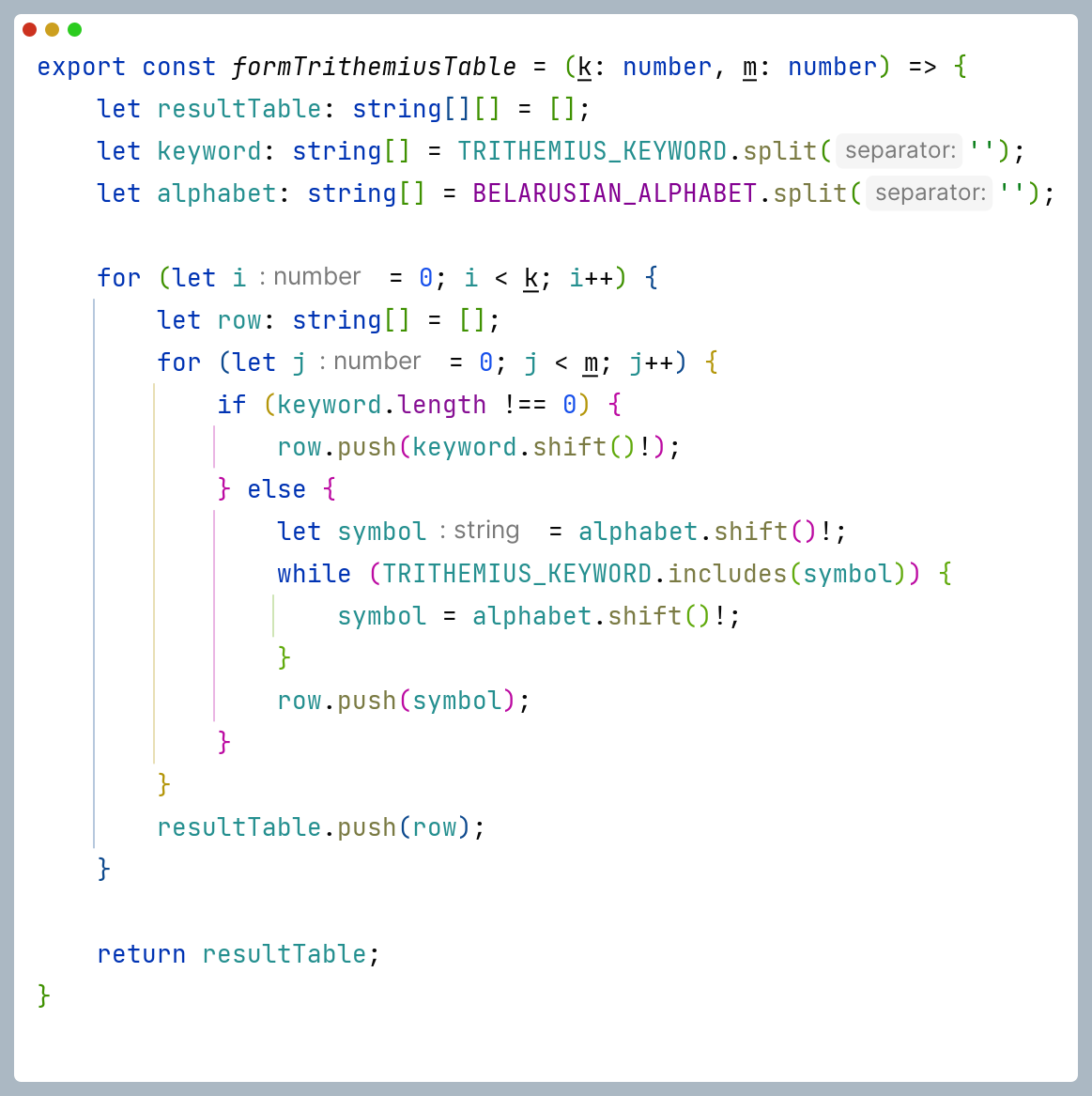


Рисунок 2.6 – Функция, формирующая таблицу Трисемуса

Результат работы функции приведен на рисунке 2.7.



Рисунок 2.7 – Таблица Трисемуса

Функция шифрования trithemiusEncode принимает на вход исходный текст и таблицу Трисемуса. Код функции представлен на рисунке 2.8.



Рисунок 2.8 – Код функции шифрования с помощью таблицы Трисемуса

Функция расшифрования trithemiusDecode принимает на вход зашифрованный текст и таблицу Трисемуса. Код функции представлен на рисунке 2.9.

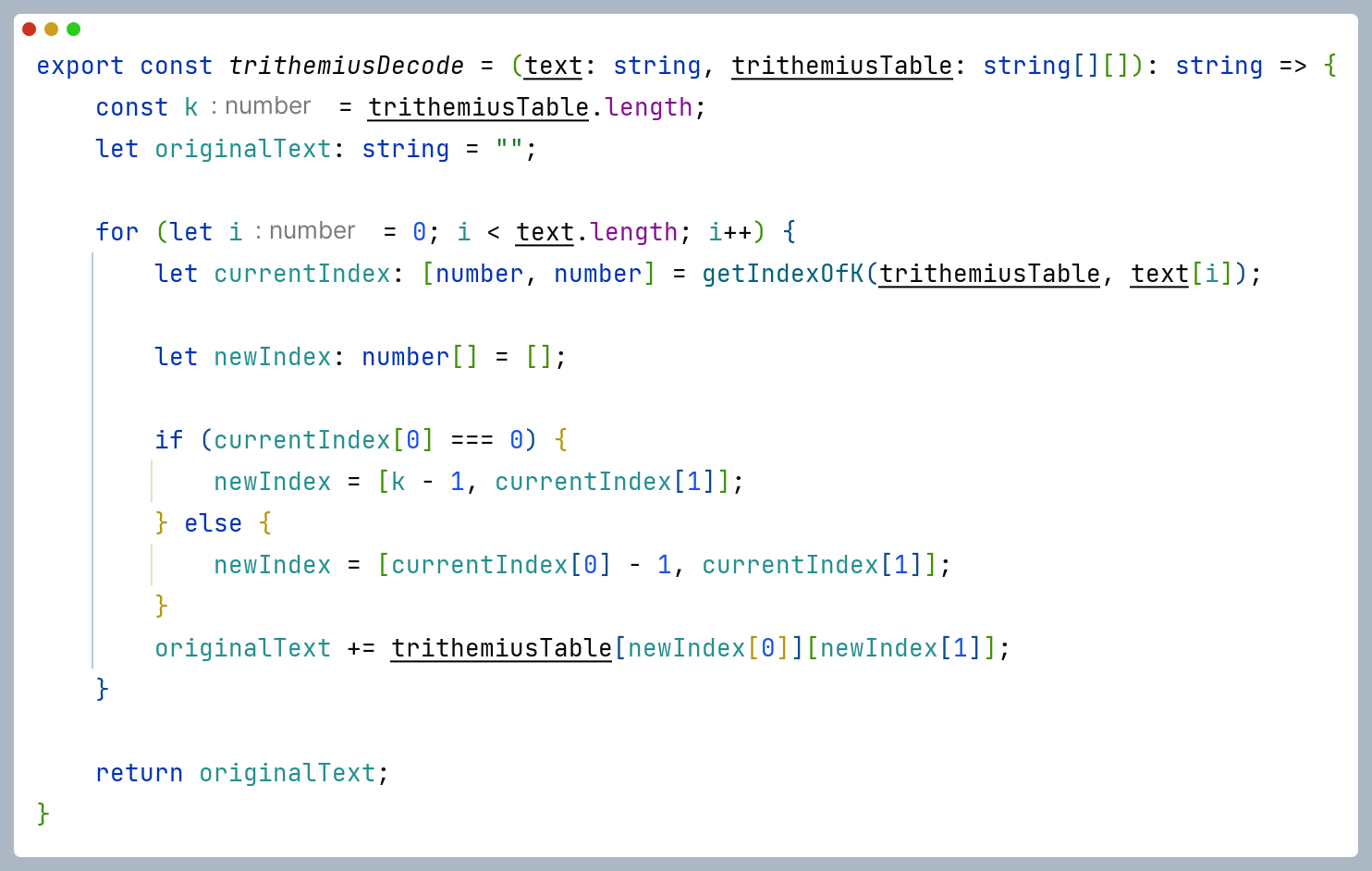


Рисунок 2.9 – Код функции расшифрования с помощью таблицы Трисемуса

Результат работы функций приведен на рисунке 2.10.

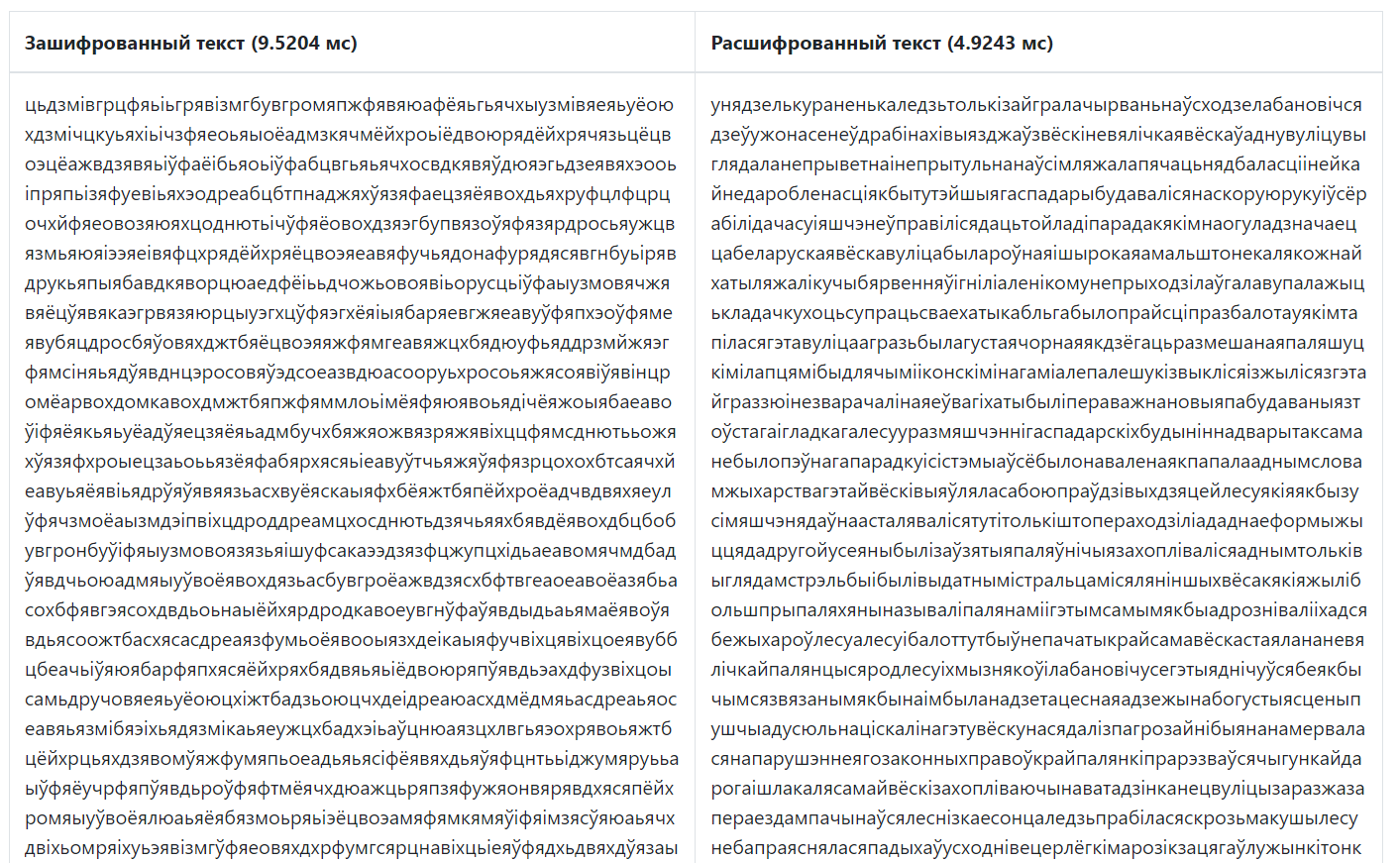


Рисунок 2.10 – Результат шифрования и дешифрования текста с помощью таблицы Трисемуса с ключевым словом «iван»

Гистограмма частот появления символов исходного сообщения приведена на рисунке 2.11.

Рисунок 2.11 – Гистограмма частот появления символов исходного сообщения

Гистограмма частот появления символов зашифрованного сообщения приведена на рисунке 2.12.

Рисунок 2.12 – Гистограмма частот появления символов зашифрованного сообщения

Сопоставив гистограммы частот появления символов исходного и зашифрованного сообщений также можно определить алфавит подстановки.

Также было определено, зашифрование текста с помощью таблицы Трисемуса выполняется примерно за 9 миллисекунд, а расшифрование за 4 миллисекунды, что значительно уступает по сравнению с шифрованием и расшифрованием с помощью шифра Цезаря.

**Вывод:** в ходе выполнения лабораторной работы были изучены основных принципов работы подстановочных шифров, методов их зашифрования и расшифрования. Также было разработано приложение для реализации указанных методов подстановочного зашифрования и расшифрования. Было выполнено исследование криптостойкости шифров на основе статистических данных о частотах появления символов в исходном и зашифрованном сообщениях. Было подтверждено, что шифры подстановки имеют низкую криптостойкость. Была проведена оценка скорости зашифрования и расшифрования реализованных способов шифров. Это позволило сравнить эффективность различных алгоритмов.