Министерство образования Республики Беларусь

Учреждение образования «Белорусский государственный технологический университет»

Факультет информационных технологий

Кафедра информационных систем и технологий

**Отчет к лабораторной работе**:

Исследование криптографических шифров на основе подстановки (замены) символов

Выполнил:

студент 3 курса 4 группы

специальности ПОИТ

Матюх А.А.

Минск 2020

1. **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.

* моноалфавитных (шифры однозначной замены или простые подстановочные);

В данных шифрах операция замена производится только над каждым одиночным символом сообщения Мi. Для наглядной демонстрации шифра простой замены достаточно выписать под заданным алфавитом тот же алфавит, но в другом порядке или, например, со смещением. Записанный таким образом алфавит называют алфавитом замены.

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

В шифре **Цезаря** шифрование:

y = x + k (mod N),

а расшифрование: х = у – k (mod N).

**Атбаш**. Этот шифр состоит в замене каждой буквы другой буквой, которая находится в алфавите на таком же расстоянии от конца алфавита.

Система шифрования **Цезаря с ключевым словом**. Особенностью этой системы является использование ключевого слова для смещения и изменения порядка символов в алфавите подстановки. Ключевое слово пишется в начале алфавита подстановки.

* полиграммных;

В таких шифрах одна подстановка соответствует сразу нескольким символам исходного текста.

Шифр **Порты** представляется в виде таблицы. Наверху горизонтально и слева вертикально записывался стандартный алфавит. В ячейках таблицы записываются числа в определенном порядке

Шифр **Плейфера** и шифр **Хилла**.

* омофонических (однозвучные шифры или шифры многозначной замены);

Создавались с целью увеличить сложность частотного анализа шифртекстов путем маскировки реальных частот появления символов текста с помощью омофонии.

**Книжный** шифр. Шифрозамена для каждой буквы определялась набором цифр, которые указывали на номер страницы, строки и позиции в строке.

* полиалфавитных.

Состоят из нескольких шифров однозначной замены. Выбор варианта алфавита для зашифрования одного символа зависит от особенностей метода шифрования.

Диск **Альберти.** Он состоял из двух дисков – внешнего неподвижного и внутреннего подвижного дисков, на которые были нанесены буквы алфавита. Процесс шифрования заключался в нахождении буквы открытого текста на внешнем диске и замене ее на букву с внутреннего диска, стоящую под ней.

Таблица **Трисемуса**. 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.

Шифр **Виженера**. Основная идея заключается в следующем. Создается таблица размером N·N, в первой строке таблицы записывается весь используемый алфавит. Каждая последующая строка получается из предыдущего циклического сдвига последней на 1 символ влево.

1. **Практическая часть**

В данной лабораторной работе необходимо разработать авторское приложение для шифрования и расшифрования с использованием английского алфавита:

• На основе аффинной системы подстановок Цезаря; a=6, b=7;

• Таблица Трисемуса.

Пример реализации аффинной системы подстановок Цезаря:



Рисунок 2.1 – Пример аффинной системы подстановок Цезаря

Пример реализации Трисемуса:

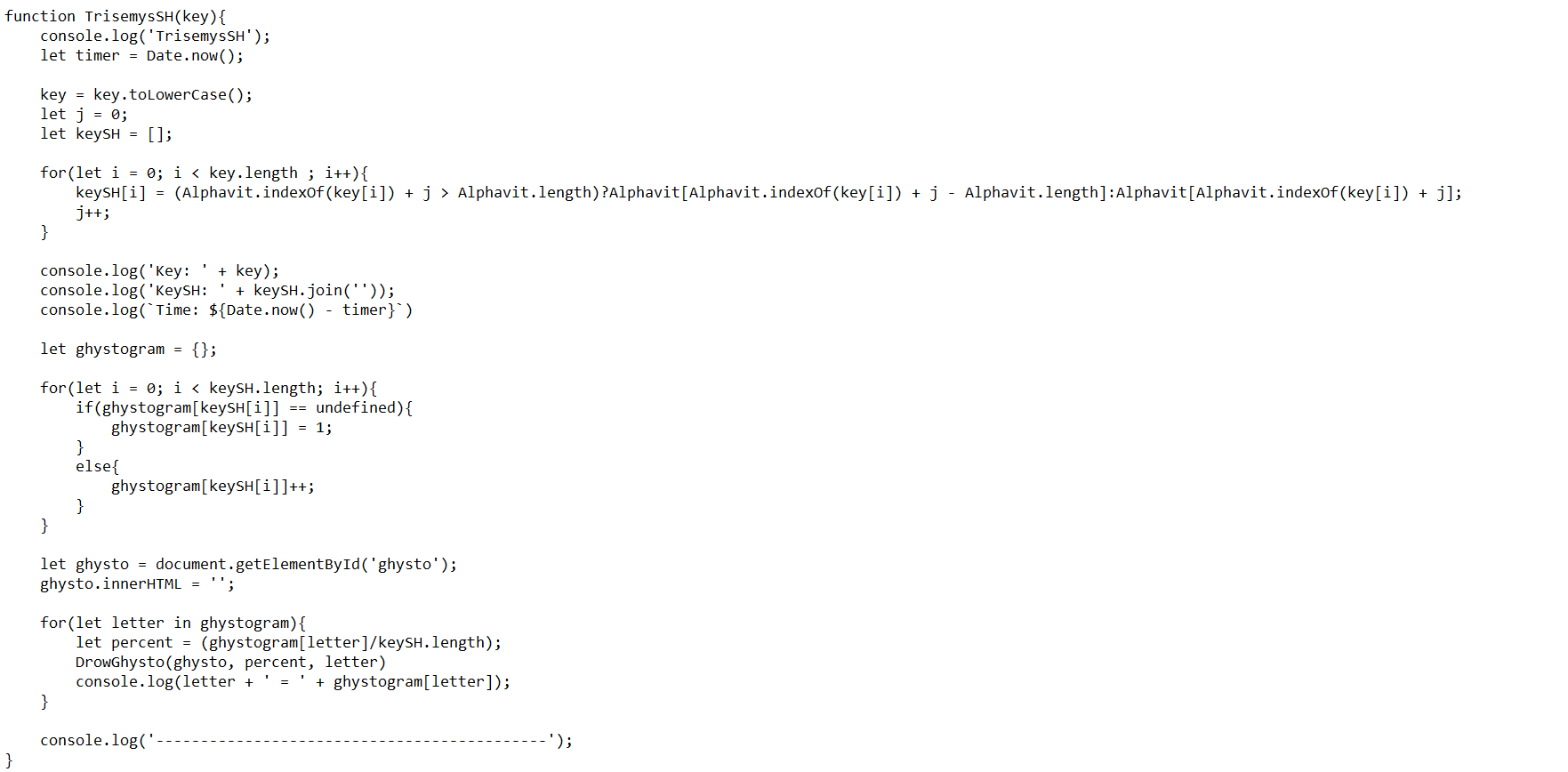


Рисунок 2.2 – Пример Трисемуса

**Вывод**

В данной лабораторной работе я закрепил теоретические знания по подстановочным шифрам. А также, разработал приложение для работы с таблицей Трисемуса и аффинной системой подстановок Цезаря.