БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

**Лабораторная работа №4**

**«**Исследование криптографических шифров на основе подстановки(замены) символов»

Выполнила:

студентка 3 курса 5 группы

Почиковская Юлия Сергеевна

Вариант 10

Проверил:

Берников В. О.

Минск 2022

1. **На основе соотношений (2.1) и (2.2); k=28**

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

Мпроцедура Расшифрования основана на использовании соотношения

****

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

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

****

Код реализации этого шифра на языке C# представлен на рисунке 1.1 - 1.2

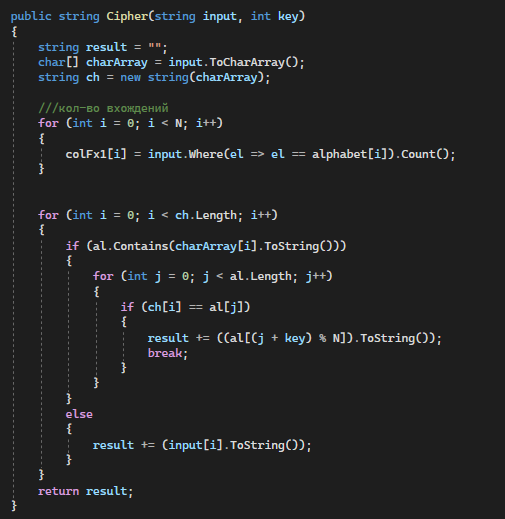


Рисунок 1.1 – Шифрование на основе Аффинного Шифра Цезаря

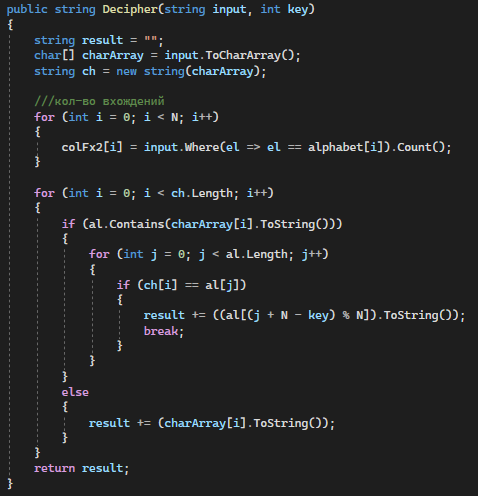


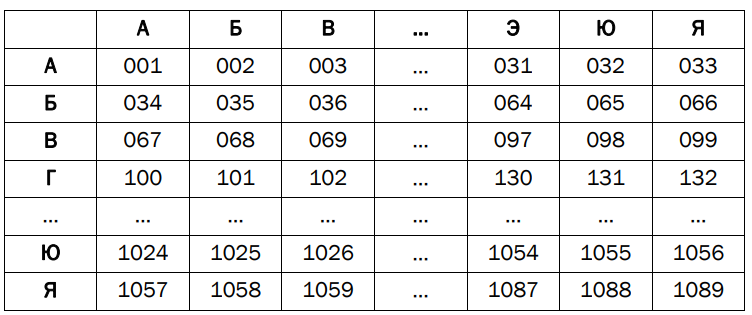
Рисунок 1.2 – Расшифрование на основе Аффинного Шифра Цезаря

1. **Шифр Порты**.

Шифр представляется в виде таблицы. Наверху горизонтально и слева

вертикально записывается стандартный алфавит. В ячейках таблицы записываются числа в определенном порядке. Фрагмент таблицы для алфавита русского показан ниже.

Таблица 2.1 – алфавит русского языка для шифра Порты

**** Шифрование выполняется парами букв исходного сообщения. Первая

буква пары указывает на строку, вторая – на столбец. В случае нечетного количества букв в сообщении Мi к нему добавляется вспомогательный символ, например «А».

Для процедуры расшифрования используется эта же таблица. Нужно найти ячейку с вашим набором символов и сопоставить ей пару букв. Первая буква пары – строка, вторая – столбец.

Код реализации этого шифра на языке C# представлен на рисунке 2.1-2.2

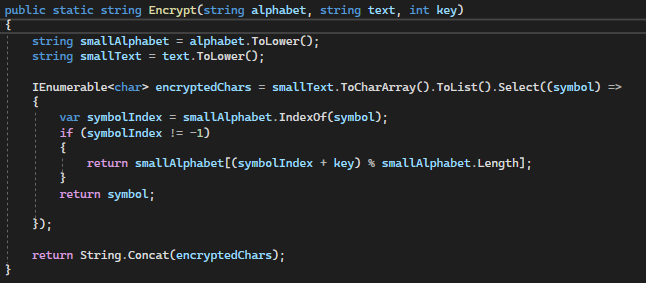


Рисунок 2.1 – Шифрование на основе шифра Порты

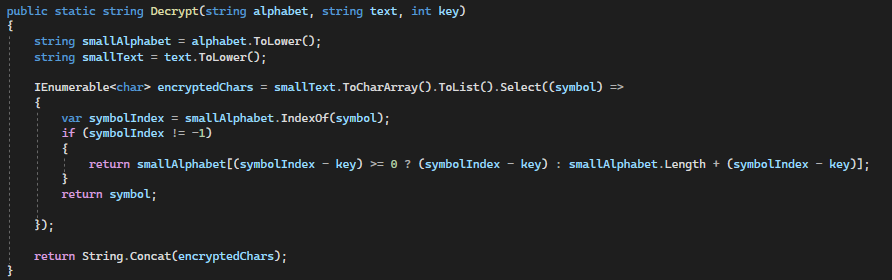


Рисунок 2.2 – Расшифрование на основе шифра Порты

Статистические данные на рисунке 2.3

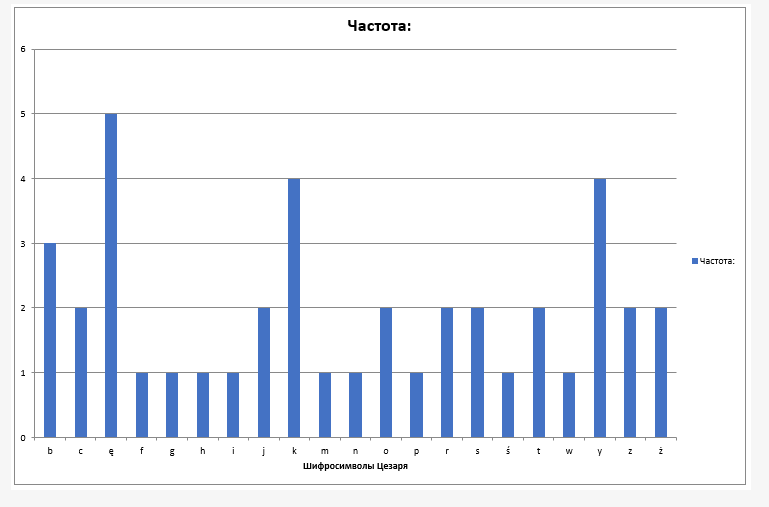


Рисунок 2.3 – Статистика шифрования