Учреждение образования

«Белорусский государственный технологический университет»

**Кафедра информационных систем и технологий**

**«Отчёт по лабораторной работе 4»**

“ ИССЛЕДОВАНИЕ КРИПТОГРАФИЧЕСКИХ ШИФРОВ НА ОСНОВЕ ПОДСТАНОВКИ (ЗАМЕНЫ) СИМВОЛОВ”

**Выполнил:** студент 3 курса

4 группы специальности ПОИТ

Примаков Максим Николаевич

**Проверил:** преподаватель

Блинова Евгения Александровна

Минск 2021

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

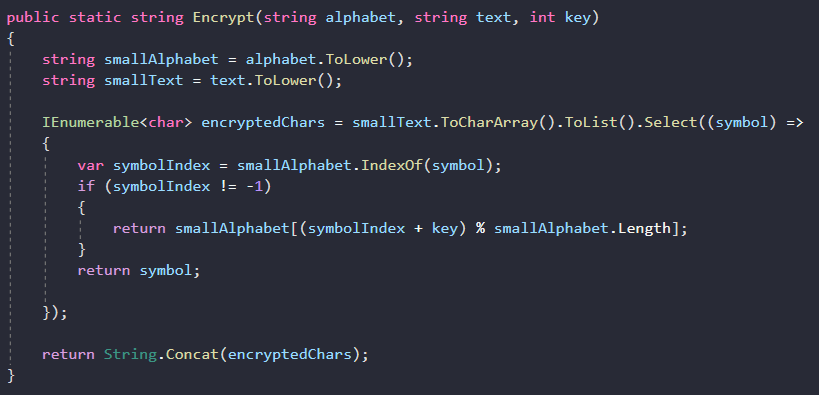
****

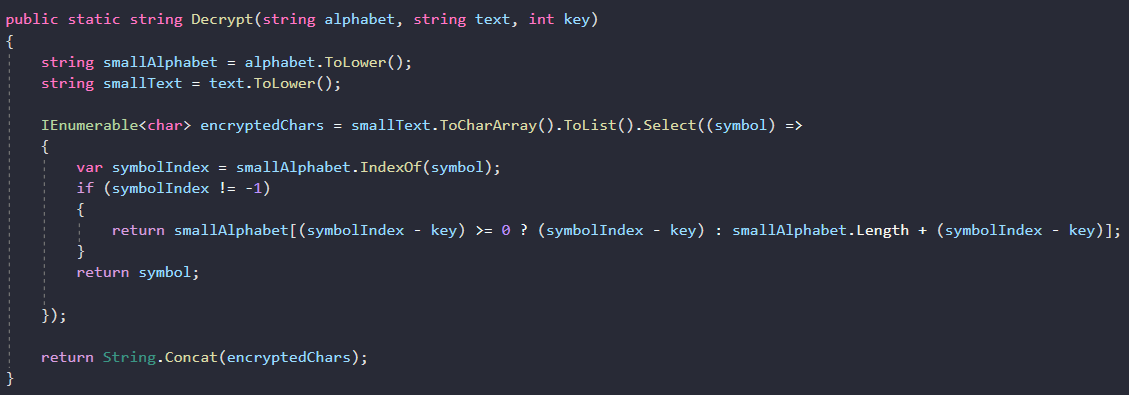
где x, y – индекс (порядковый номер, начиная с 0) символа в используемом алфавите, k – ключ.

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

****

Код реализации этого шифра на языке C# :

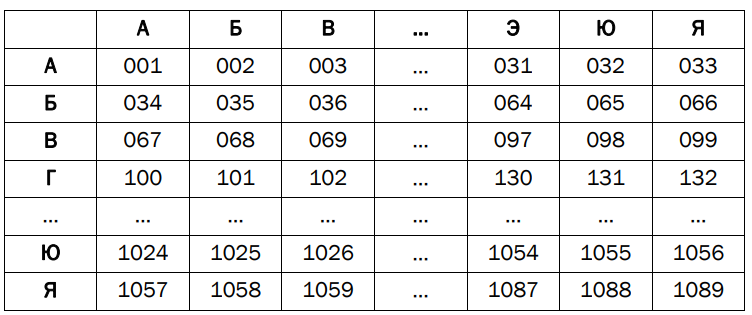




1. **Шифр Порты**.

Шифр представляется в виде таблицы. Наверху горизонтально и слева

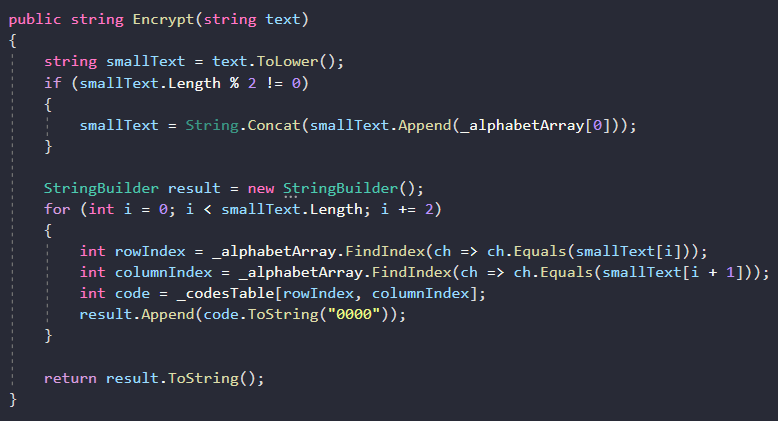
вертикально записывается стандартный алфавит. В ячейках таблицы записываются числа в определенном порядке. Фрагмет таблицы для алфавита русского показан ниже.

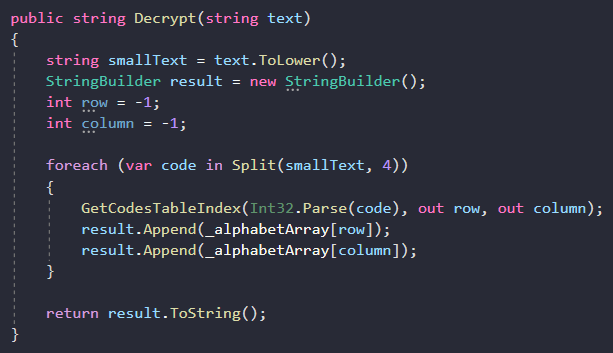
**** Шифрование выполняется парами букв исходного сообщения. Первая

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# :





Статистические данные:

