МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образование «Белорусский государственный технологический университет»

Кафедра информационных систем и технологий

**«Отчет к лабораторной работе №5**

**Исследование криптографических шифров на основе перестановки символов»**

Студент:

Септилко Анастасия Антоновна

Преподаватель:

Блинова Евгения Александровна

Минск 2020

**ЗАДАНИЯ:**

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

• выполнять зашифрование/расшифрование текстовых документов (объемом не менее 500 знаков) созданных на основе алфавита языка в соответствии с нижеследующей таблицей вариантов задания; при этом следует использовать шифры подстановки из третьего столбца данной таблицы;

1. Маршрутная перестановка (маршрут: зигзагом; параметры таблицы – по указанию преподавателя)

2. Множественная перестановка, ключевые слова – собственные имя и фамилия

• формировать гистограммы частот появления символов для исходного и зашифрованного сообщений;

• оценивать время выполнения операций зашифрования/расшифрования (напоминание: во многих языках программирования есть встроенные методы для замеров времени; при отсутствии такового в используемом языке можно воспользоваться разностью двух дат (например, в миллисекундах: время после выполнения программы – время до начала выполнения преобразования).

Для начала сформировала алфавит для шифрования двумя методами.

Массив Alphavit используется для шифрования маршрутной перестановка (маршрут: зигзагом). Массив Alphabet используется для шифрования множественной перестановки с ключевыми словами (рисунок 1.1).

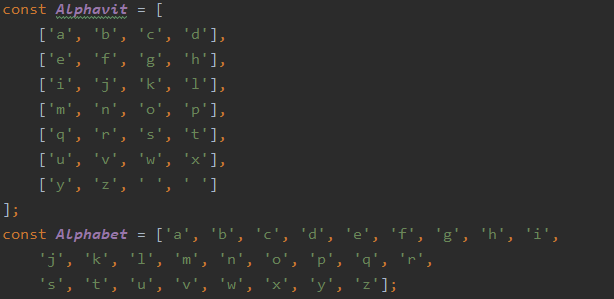


Рисунок 1.1 – Формирование алфавитов

Маршрутная перестановка (маршрут: зигзагом) уже упоминавшаяся маршрутная перестановка (записываем сообщение по строкам, считываем – по столбцам матрицы) можно усложнить и считывать не по столбцам, зигзагом на рисунке 1.2 показан маршрут.

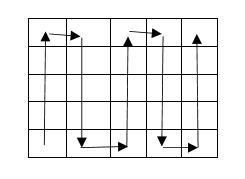


Рисунок 1.2 – Маршрут зигзак

Функция реализующая данный метод шифра перестановки продемонстрирована на рисунке 1.3

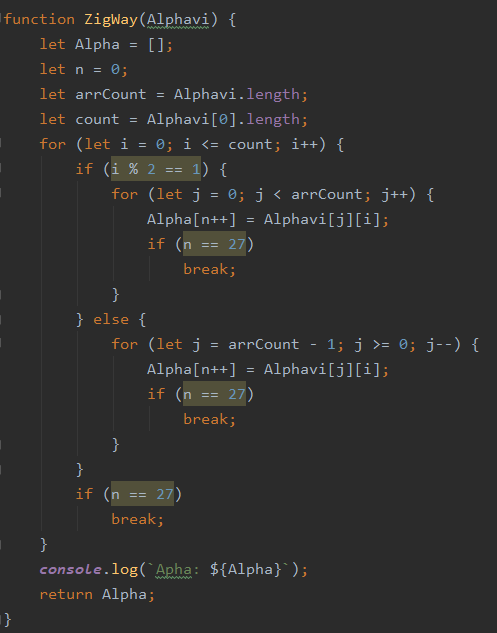


Рисунок 1.3а – Функция ZigWay()



Рисунок 1.3б – Функция WaySН()

Здесь мы формируем алфавит из указанного ранее массива и строим маршрут.

Работа маршрутной перестановки (зигзагом) предоставлен на рисунке 1.4.

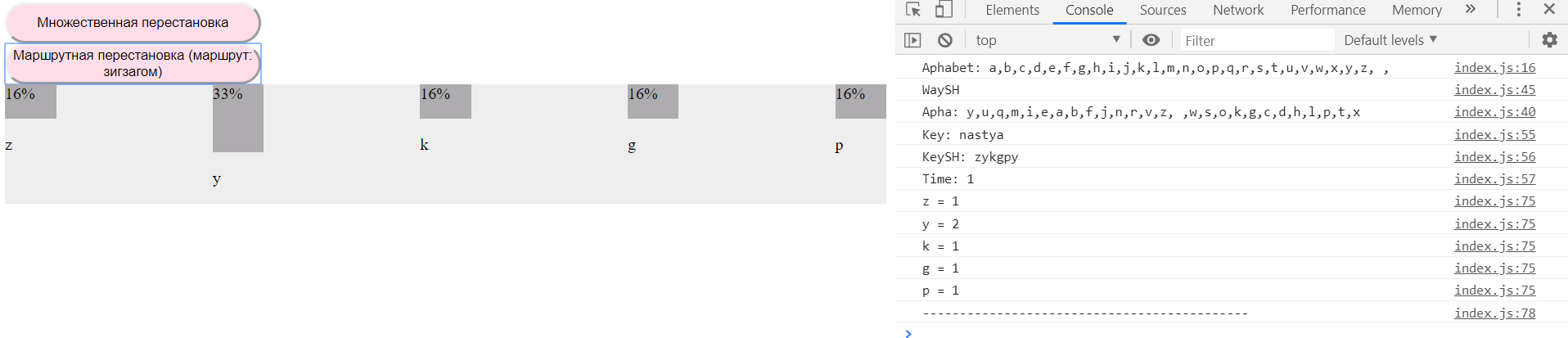


Рисунок 1.4 – Работа маршрутной перестановки

Множественная перестановка, ключевые слова – собственные имя и фамилия.

Особенностью шифров данного подкласса является минимум двукратная перестановка символов шифруемого сообщения. В простейшем случае это может задаваться перемешиваем не только столбцов (как в примере 4), но и строк. Таким образом, этот случай соответствует использованию двух основных ключей: длина одного из них равна числу столбцов, другого – числу строк. К ключевой информацию мы можем относить также способы вписывания сообщения и считывания отдельных символов из текущего столбца матрицы.

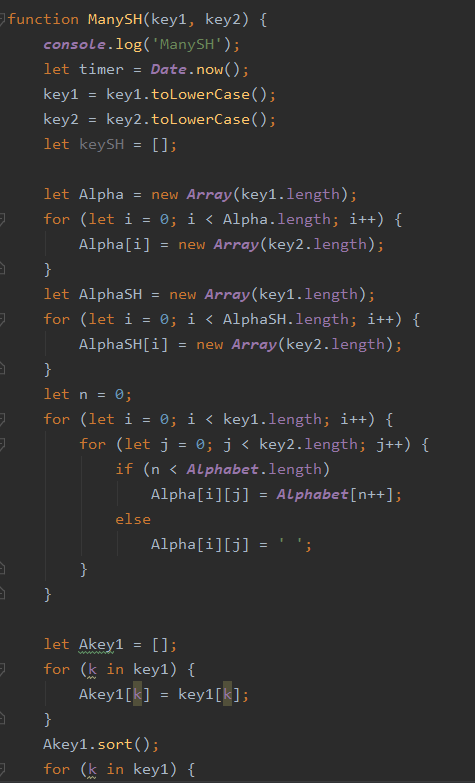
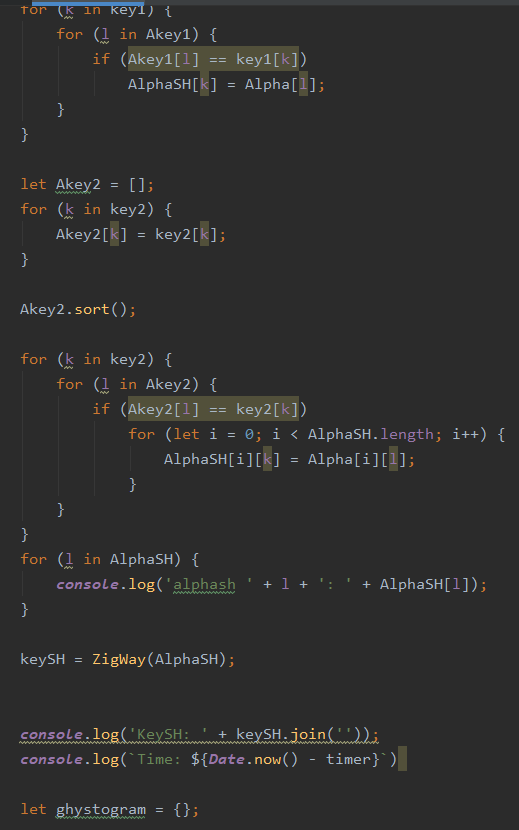
Шифры гаммирования рассматриваются как самостоятельный класс. Такие шифры схожи с перестановочными тем, что в обоих случаях можно использовать табличное представление выполняемых операций на основе ключей. Вместе с тем, шифры гаммирования имеют много общего с происходит подмена одних символов на другие (рисунок 1.5).



Рисунок 1.5 – Функции для реализации множственной подстановки

Пример работы множественной перестановки предоставлен на рисунке 1.6.

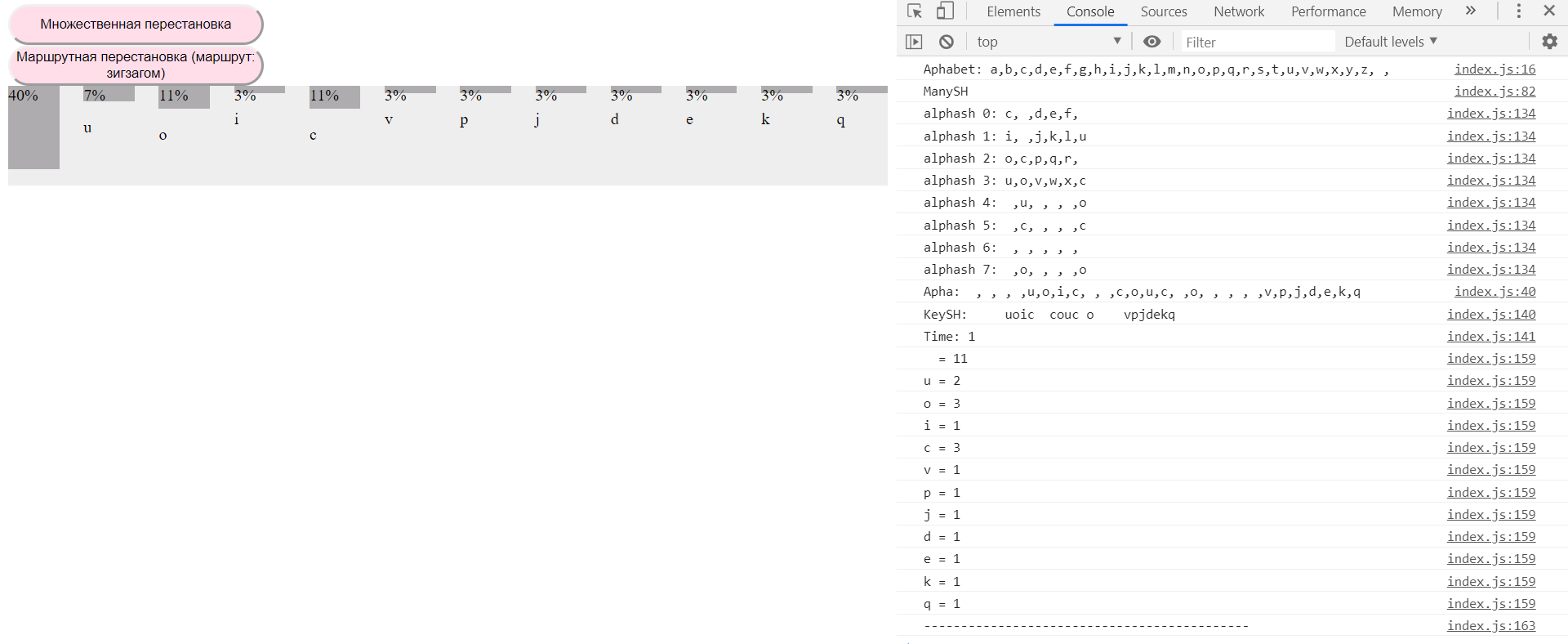


Рисунок 1.6 – Пример работы множественной перестановки