Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Исследование криптографических шифров на основе перестановки символов**

Студент: Гвоздовский К.В.

ФИТ 3 курс 6 группа

Преподаватель:

Нистюк Ольга Александровна

1. **Цель работы**

Изучение и приобретение практических навыков разработки и использования приложений для реализации перестановочных шифров.

1. **Теоретическая часть**

Среди шифров рассматриваемого подкласса иногда выделяют шифры простой перестановки (или перестановки без ключа). Символы открытого текста Мi перемешиваются по каким-либо правилам. Формально каждое из таких правил может рассматриваться в качестве ключа.

Для использования шифров **одинарной перестановки** используется таблица, состоящая из двух строк: в первой строке записываются буквы, во второй – цифры J. Строки состоят из n столбцов. Буквы составляют шифруемое сообщение. Цифры J = j1, j2, …, jn, где j1 – номер позиции в зашифрованном сообщении первого символа открытого текста, где j2 – номер позиции в зашифрованном сообщении второго символа открытого текста и т. д. Таким образом, порядок следования цифр определяется используемым правилом (ключом) перестановки символов открытого текста для получения шифрограммы.

Шифры **простой блочной перестановки**. Блок должен состоять из 2-х или более символов. Если общее число таких символов в сообщении не кратно длине сообщения, то последний блок можно дополнить произвольными знаками.

Шифры **маршрутной перестановки**. Основой рассматриваемого типа является геометрическая фигура. Обычно прямоугольник или прямоугольная матрица. В ячейки этой фигуры по определенному маршруту записывается открытый текст.

Шифр **Скитала** (Сцитала). Известно, что в V веке до н. э. в Спарте существовала хорошо отработанная система секретной военной связи. Для этого использовался специальный жезл «скитала» (греч. σκυτάλη – первое, вероятно, простейшее криптографическое устройство, реализующее метод перестановки

**Организация маршрутной перестановки**. Уже упоминавшаяся маршрутная перестановка (записываем сообщение по строкам, считываем – по столбцам матрицы) можно усложнить и считывать не по столбцам, а по спирали, зигзагом, змейкой или каким-то другим способом.

Шифр **вертикальной перестановки.** Данный шифр является разновидностью шифра маршрутной перестановки. К особенностям вертикального шифра можно отнести следующие:

-количество столбцов в таблице фиксируется и определяется длиной ключа;

- маршрут вписывания: слева-направо, сверху-вниз;

-шифрограмма выписывается по столбцам в соответствии с их нумерацией (ключом).

Шифры **множественной перестановки.** 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.

**Множественная перестановка**

Особенностью шифров данного подкласса является минимум двукратная перестановка символов шифруемого сообщения. В простейшем случае это может задаваться перемешиванием не только столбцов, но и строк. Таким образом, этот случай соответствует использованию двух основных ключей: длина одного из них равна числу столбцов, другого – числу строк.

Для реализации множественной перестановки необходимо сформировать таблицу (ключи имя и фамилия – «kirill» и «gvozdovskiy»). Далее записываем последовательно шифруемое сообщение в каждую ячейку слева направо: «Honesty is the best policy that you can try to practice in your» (Табл. 1).

Таблица 1

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **k** | **i** | **r** | **i** | **l** | **l** |
| **g** | H | o | n | e | s | t |
| **v** | y |  | i | s |  | t |
| **o** | h | e |  | b | e | s |
| **z** | s | t |  | p | o | l |
| **d** | i | c | y |  | t | h |
| **o** | a | t |  | y | o | u |
| **v** |  | c | a | n |  | t |
| **s** | r | y |  | t | o |  |
| **k** | p | r | a | c | t | i. |
| **i** | c | e |  | i | n |  |
| **y** | y | o | u | r |  |  |

Затем сортируем по ключу в алфавитном порядке строки (один из ключей) (Табл. 2).

Таблица 2

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **k** | **i** | **r** | **i** | **l** | **l** |
| **d** | i | c | y |  | t | h |
| **g** | H | o | n | e | s | t |
| **i** | c | e |  | i | n |  |
| **k** | p | r | a | c | t | i. |
| **o** | h | e |  | b | e | s |
| **o** | a | t |  | y | o | u |
| **s** | r | y |  | t | o |  |
| **v** | y |  | i | s |  | t |
| **v** |  | c | a | n |  | t |
| **y** | y | o | u | r |  |  |
| **z** | s | t |  | p | o | l |

Затем сортируем столбцы в алфавитном порядке по второму ключу (Табл.3).

Таблица 3

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **i** | **i** | **k** | **l** | **l** | **r** |
| **d** | c |  | i | t | h | y |
| **g** | o | e | H | s | t | n |
| **i** | e | i | c | n |  |  |
| **k** | r | c | p | t | i. | a |
| **o** | e | b | h | e | s |  |
| **o** | t | y | a | o | u |  |
| **s** | y | t | r | o |  |  |
| **v** |  | s | y |  | t | i |
| **y** | c | n |  |  | t | a |
| **z** | o | r | y |  |  | u |
|  | t | p | s | o | l |  |

Получим зашифрованное сообщения, считывая символы по порядку по столбцам сверху вниз. На выходе получим такое сообщение: «coerety cot eicbytsnrpiHcphary ystsnteoo oht isu tt lyn a iau ».

**Маршрутная перестановка (маршрут: зигзагом)**

Маршрутная перестановка (записываем сообщение по строкам, считываем – по столбцам матрицы) можно усложнить и считывать не по столбцам, а по спирали, зигзагом, змейкой или каким-то другим способом. Такие способы шифрования несколько усложняют процесс, однако усиливают криптостойкость шифра.

В соответствии с вариантом по условию лабораторной маршрутная перестановка осуществляется зигзагом. Графическое представление метода маршрутной перестановки зигзагом приведено на рисунке 2.

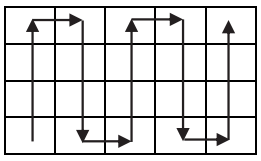


Рисунок 2 – Графическое представление метода маршрутной перестановки зигзагом

Наглядно изобразим алгоритм шифрования в виде таблицы (Табл. 4).

Таблица 4

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| H | o | n | e | s | t | y |  |
| i | s |  | t | h | e |  | b |
| e | s | t |  | p | o | l | i |
| c | y |  | t | h | a | t |  |
| y | o | u |  | c | a | n |  |
|  | t | r | y |  | t | o |  |
| p | r | a | c | t | i | c | e |
|  | i | n |  | y | o | u | r |
|  | l | i | f | e | . |  |  |

В итоге должно получится такое зашифрованное сообщение: « p y ceiHossyotrilinaru t net t yc fshphc tyeteoaatio.y ltnocu bi er ».

1. **Задание**

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

1. 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;
2. формировать гистограммы частот появления символов для исходного и зашифрованного сообщений;
3. оценивать время выполнения операций зашифрования/расшифрования.
4. **Ход работы**

В соответствии с вариантом, алфавит выбран английский, для первого задания использовалась маршрутная перестановка (маршрут – зигзаг), для второго задания использовалась множественная перестановка, ключевые слова – собственные имя и фамилия.

Для обоих заданий следовало оценить время выполнения операций шифрования/дешифрования сообщений. Для этого был использован специальный метод Date.now() на языке JavaScript, который предоставляет функциональность для измерения времени выполнения операций. Пример использования объекта данного метода представлен на рисунке 3.1.

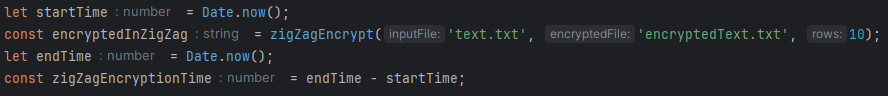


Рисунок 3.1 – Пример использования метода Date.now()

Также, для этих заданий следовало сформировать гистограммы частот появления символов для исходного и зашифрованного сообщений. Для этой цели была разработана функция CountCharacterFrequency, представленная на рисунке 3.2.



Рисунок 3.2 – Функция для определения частот появления символов

Для выполнения первого задания были разработаны функции ZigZagEncrypt и ZigZagDecrypt, которые осуществляют шифрование и дешифрование текста с использованием маршрутной перестановки. Они представлены на рисунках 3.3 и 3.4.



Рисунок 3.3 – Функция для шифрования текста с помощью маршрутной перестановки (маршрут – зигзаг)

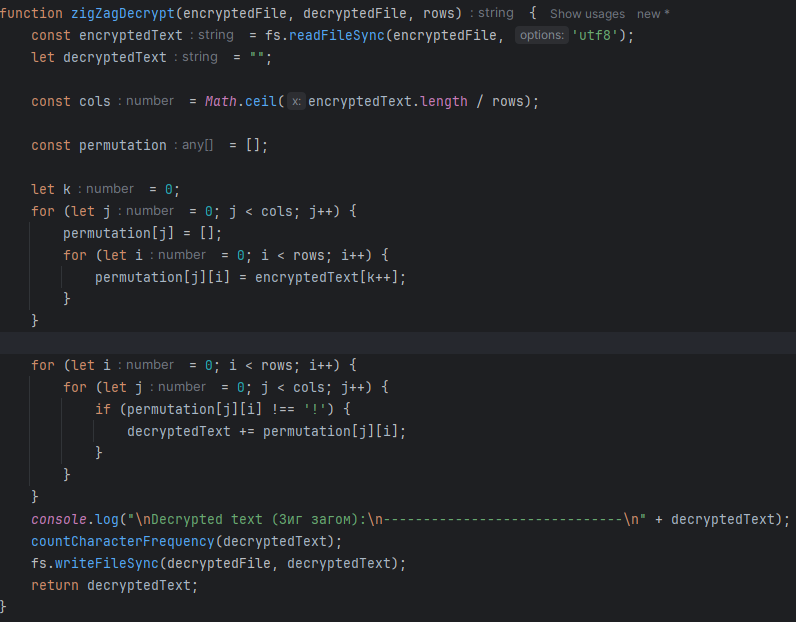


Рисунок 3.4 – Функция для дешифрования текста с помощью маршрутной перестановки (маршрут – зигзаг)

Результаты выполнения данных функций и время их выполнения представлены на рисунках 3.6 и 3.7.

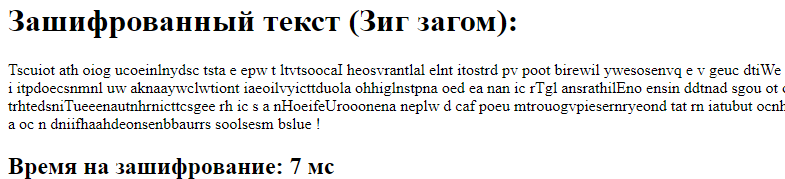


Рисунок 3.6 – Текст, зашифрованный с помощью функции ZigZagEncrypt и время его выполнения

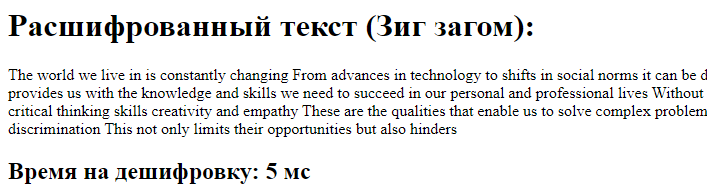


Рисунок 3.7 – Текст, расшифрованный с помощью функции ZigZagDecrypt и время его выполнения

Частота появления символов в этих текстовых файлах представлена на рисунках 3.8 и 3.9 соответственно.

Рисунок 3.8 – Гистограмма частот появления символов для зашифрованного текста

Рисунок 3.9 – Гистограмма частот появления символов для расшифрованного текста

Для выполнения второго задания были разработаны функции multiplePermutationEncrypt и multiplePermutationDecrypt, которые реализуют алгоритм шифрования текста с помощью алгоритма множественной перестановки (ключ – имя и фамилия). Код реализации этих функций представлен на рисунках 3.10 и 3.11.

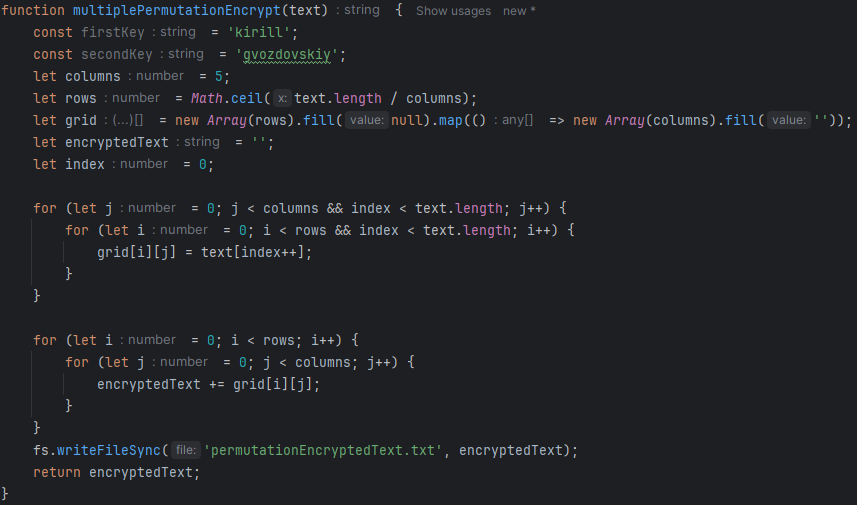


Рисунок 3.10 – Функция для шифрования текста с помощь алгоритма множественной перестановки

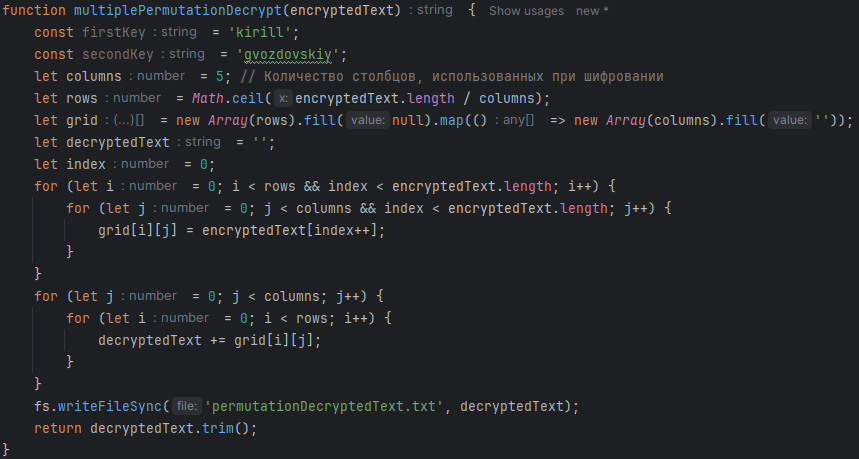


Рисунок 3.11 – Функция для дешифрования текста с помощью алгоритма множественной перестановки

В результате получаем следующие файлы и вывод, представленные на рисунках 3.12 и 3.13.

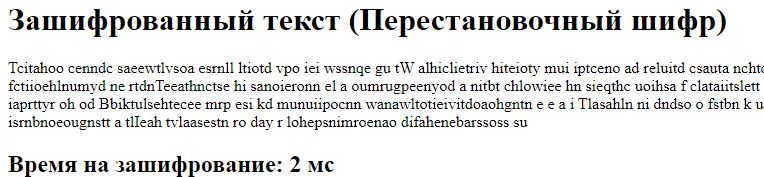


Рисунок 3.13 – Текст, зашифрованный с помощью функции multiplePermutationEncrypt и время его выполнения

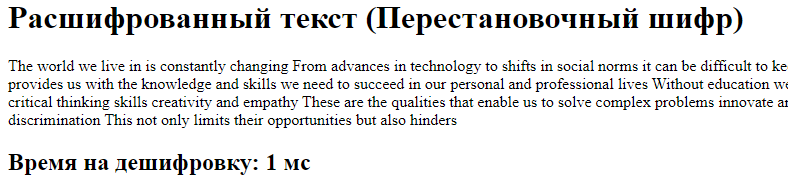


Рисунок 3.14 – Текст, расшифрованный с помощью функции multiplePermutationDecrypt и время его выполнения

Частота появления символов в этих текстовых файлах представлена на рисунках 3.15 и 3.16 соответственно.

Рисунок 3.15 – Гистограмма частот появления символов для зашифрованного текста

Рисунок 3.16 – Гистограмма частот появления символов для расшифрованного текста

**Вывод**

В ходе лабораторной работы были изучены и приобретены практические навыки разработки и использования приложений для реализации перестановочных шифров.

Кроме того, были сформированы гистограммы появления частот на основе зашифрованных/расшифрованных сообщений. Из графиков видно, что частота символов в зашифрованном тексте вовсе не отличается от частоты символов в исходном тексте. Это обусловлено тем, что перестановочные шифры не заменяют символы открытого текста на другие символы или последовательность символов, а просто меняют порядок их следования.

Также было разработано авторское приложение в соответствии с целью лабораторной работы.