Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Лабораторная работа №5

**ИССЛЕДОВАНИЕ КРИПТОГРАФИЧЕСКИХ ШИФРОВ НА ОСНОВЕ ПЕРЕСТАНОВКИ СИМВОЛОВ**

Студент: Сосновец М.И.

ФИТ 3 курс 4 группа

Преподаватель: Нистюк О.А.

Минск 2025

**Цель:** изучение и приобретение практических навыков разработки и использования приложений для реализации перестановочных шифров (работа рассчитана на 4 часа аудиторных занятий).

**Задачи:**

1. Закрепить теоретические знания по алгебраическому описанию, алгоритмам реализации операций зашифрования/расшифрования и оценке криптостойкости перестановочных шифров.
2. Ознакомиться с особенностями реализации и свойствами различных перестановочных шифров на основе готового программного средства (L\_LUX).
3. Разработать приложение для реализации указанных преподавателем методов перестановочного зашифрования/расшифрования.
4. Выполнить исследование криптостойкости шифров на основе статистических данных о частотах появления символов в исходном и зашифрованном сообщениях.
5. Оценить скорость зашифрования/расшифрования реализованных способов шифров.
6. Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

**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

В классической криптографии шифры перестановки делятся на два подкласса:

* шифры простой, или одинарной, перестановки – при зашифровании символы открытого текста Мi перемещаются с исходных позиций в новые (в шифртексте Сi) один раз;
* шифры сложной, или множественной, перестановки – при зашифровании символы открытого текста Мi перемещаются с исходных позиций в новые (в шифртексте Сi) несколько раз.

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.

Шифры простой блочной перестановки. Указанные шифры строятся по тем же правилам, что и шифры простой перестановки. Блок должен состоять из 2 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 современных шифров рассматриваемого типа является геометрическая фигура, обычно прямоугольник или прямоугольная матрица. В ячейки этой фигуры по определенному маршруту (слево направо, сверху вниз или каким-либо иным образом) записывается открытый текст. Для получения шифрограммы нужно записать символы этого сообщения в иной последовательности, т. е. по иному маршруту.

Шифр Скитала (Сцитала). Известно, что в V в. 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. Для зашифрования и расшифрования необходимо было иметь абсолютно одинаковые жезлы. На такой предмет наматывалась пергаментная лента. Далее на эту ленту построчно наносился текст. Для расшифрования ленту с передаваемым сообщением нужно было намотать так же, как и при нанесении открытого текста

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. Такие способы шифрования несколько усложняют процесс, однако усиливают криптостойкость шифра.

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: слево направо, сверху вниз;
* шифрограмма выписывается по столбцам в соответствии с их нумерацией (ключом). Ключ может задаваться в виде текста (слова или словосочетания). Лексикографическое местоположение символов в ключевом выражении определяет порядок считывания столбцов.

Шифры множественной перестановки. 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. К ключевой информацию мы можем относить также способы вписывания сообщения и считывания отдельных символов из текущего столбца матрицы.

**Основное задание**

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 (варианты задания в табл. 3.11);

|  |  |  |
| --- | --- | --- |
| Вариант | Алфавит | Шифр |
| 2 | Русский | 1. Маршрутная перестановка (маршрут –по спирали; 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)).

**Задание 1:**

В соответствии с вариантом задания, было разработано приложение, которое выполняет зашифрование и расшифрование текста с помощью маршрутной перестановки (маршрут –по спирали; параметры таблицы – по указанию преподавателя), множественной перестановки, ключевые слова – собственные имя и фамилия. Код приложения предоставлен в листинге 1.1, 1.2 соответственно.

|  |
| --- |
| function spiralEncrypt(text, rows, cols) {  const totalCells = rows \* cols;  const paddedText = text.padEnd(totalCells, ' ');  const table = [];  for (let i = 0; i < rows; i++) {  table.push(paddedText.substr(i \* cols, cols).split(''));}  let result = [];  let top = 0, bottom = rows - 1, left = 0, right = cols - 1;  while (top <= bottom && left <= right) {  for (let i = right; i >= left; i--) {  result.push(table[top][i]);}  top++;  for (let i = top; i <= bottom; i++) {  result.push(table[i][left]);  }  left++;  if (top <= bottom) {  for (let i = left; i <= right; i++) {  result.push(table[bottom][i]);}  bottom--;}  if (left <= right) {  for (let i = bottom; i >= top; i--) {  result.push(table[i][right]);  }right--;}}  return result.join('');  }  function spiralDecrypt(text, rows, cols) {  const paddedText = text.padEnd(rows \* cols, ' ');  const table = Array(rows).fill().map(() => Array(cols).fill(''));  let top = 0, bottom = rows - 1, left = 0, right = cols - 1;  let index = 0;  while (top <= bottom && left <= right) {  for (let i = right; i >= left; i--) {  table[top][i] = paddedText[index++];  }top++;  for (let i = top; i <= bottom; i++) {  table[i][left] = paddedText[index++];  }  left++;  if (top <= bottom) {  for (let i = left; i <= right; i++) {  table[bottom][i] = paddedText[index++];}bottom--;}  if (left <= right) {  for (let i = bottom; i >= top; i--) {  table[i][right] = paddedText[index++];  }right--;}}  return table.map(row => row.join('')).join('');} |

Листинг 1.1 – Реализация маршрутной перестановки

|  |
| --- |
| function multipleEncrypt(text, key1, key2) {  const table1 = createTable(text, key1);  const order1 = getColumnOrder(key1);  const firstPass = readColumns(table1, order1);  const table2 = createTable(firstPass, key2);  const order2 = getColumnOrder(key2);  return readColumns(table2, order2);}  function multipleDecrypt(text, key1, key2) {  const order2 = getColumnOrder(key2);  const table2 = rebuildTable(text, key2.length, order2);  const firstPass = readRows(table2);  const order1 = getColumnOrder(key1);  const table1 = rebuildTable(firstPass, key1.length, order1);return readRows(table1);}  function createTable(text, key) {  const cols = key.length;  const rows = Math.ceil(text.length / cols);  const table = [];  for (let i = 0; i < rows; i++) {const row = text.slice(i \* cols, (i + 1) \* cols).split('');  while (row.length < cols) row.push(' ');  table.push(row);}return table;}  function getColumnOrder(key) {  return key.split('')  .map((char, i) => ({ char, index: i }))  .sort((a, b) => a.char.localeCompare(b.char) || a.index - b.index).map(item => item.index);}  function readColumns(table, order) {  let result = '';  for (let col of order) {  for (let row = 0; row < table.length; row++) {  result += table[row][col] || ' ';}}return result;}  function rebuildTable(text, cols, order) {  const rows = Math.ceil(text.length / cols);  const table = Array(rows).fill().map(() => Array(cols).fill(''));let pos = 0;  for (let col of order) {  for (let row = 0; row < rows; row++) {  table[row][col] = text[pos++] || ' ';}}return table;}  function readRows(table) {  return table.map(row => row.join('')).join('').trim();  } |

Листинг 1.2 – Реализация множественной перестановки

Зашифрование и расшифрование текста с помощью маршрутной перестановки представлено на рисунках 1.1, 1.2 соответственно.

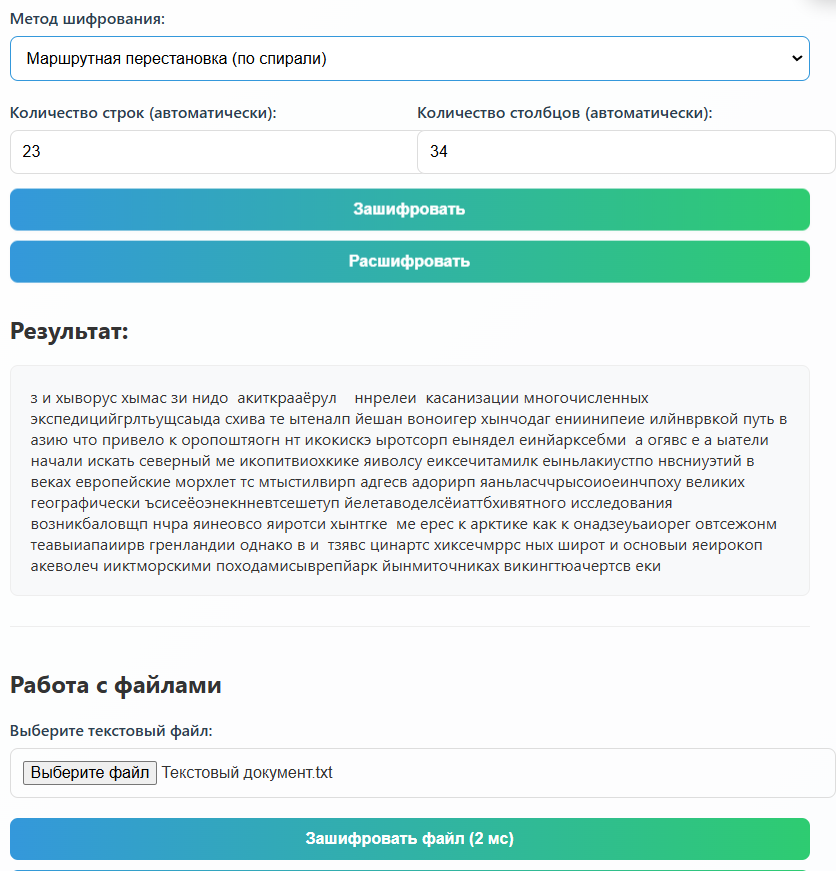


Рисунок 1.1 – Результат зашифрования текста

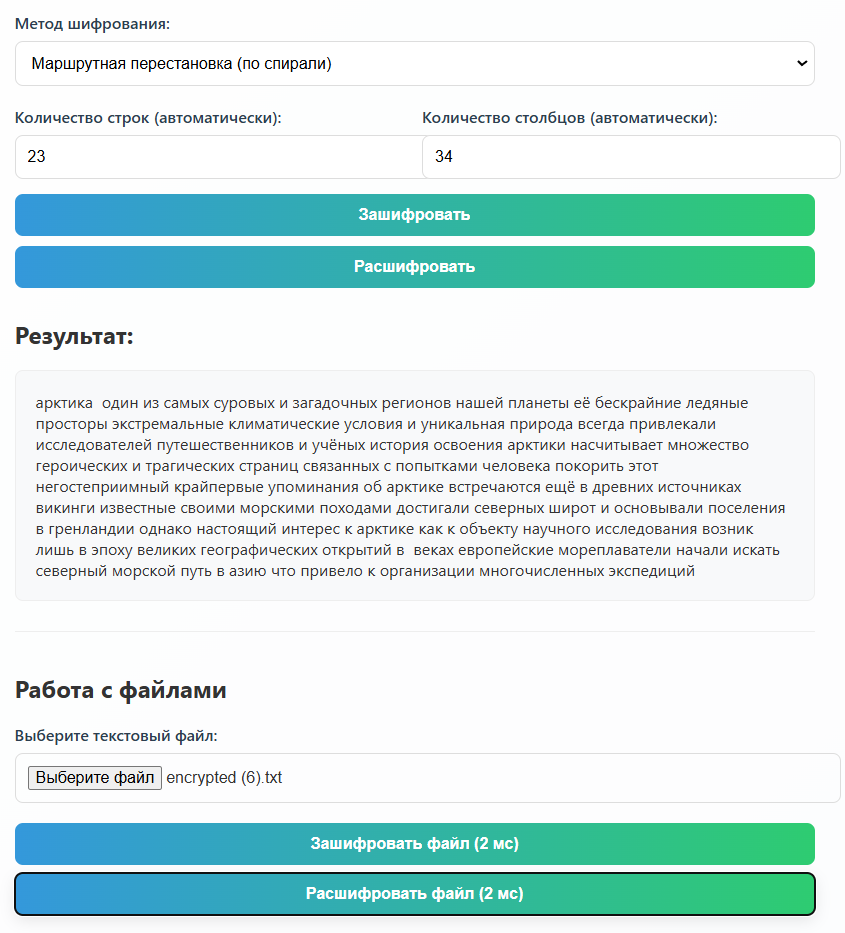


Рисунок 1.2 – Результат расшифрования текста

Текст, зашифрованный шифром множественной перестановки с ключевыми словами «мария» и «сосновец» предоставлен на рисунке 1.3.

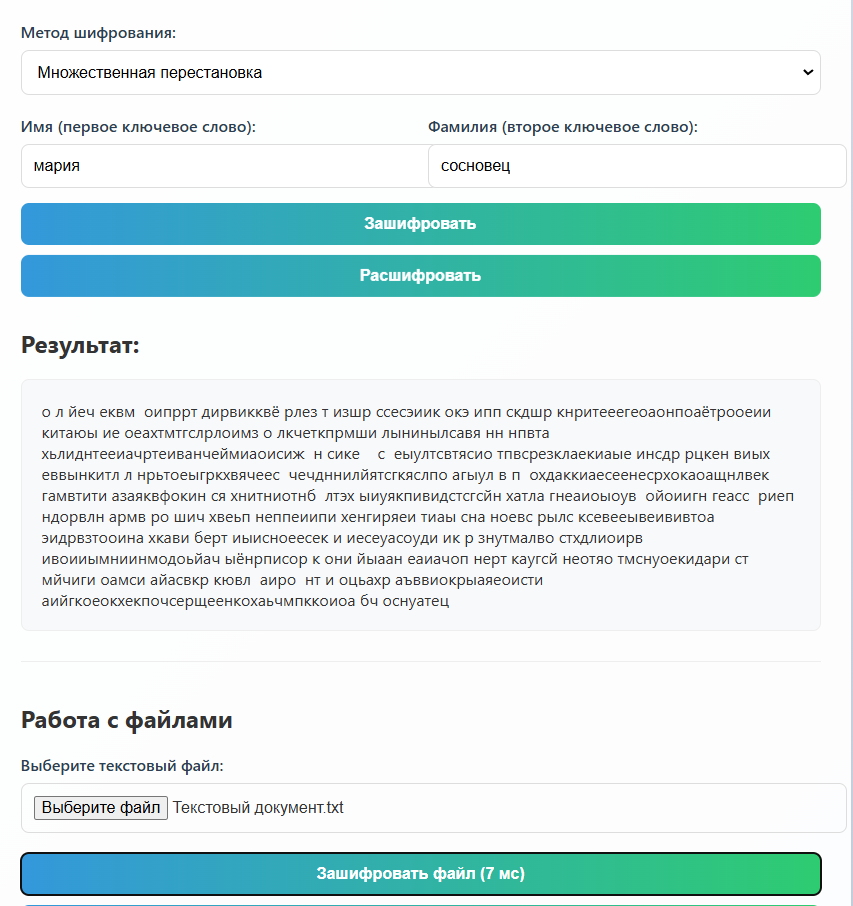


Рисунок 1.3 – Результат зашифрования текста с ключевыми словами «мария» и «сосновец»

Текст, расшифрованный шифром множественной перестановки с ключевыми словами «мария» и «сосновец» предоставлен на рисунке 1.4.

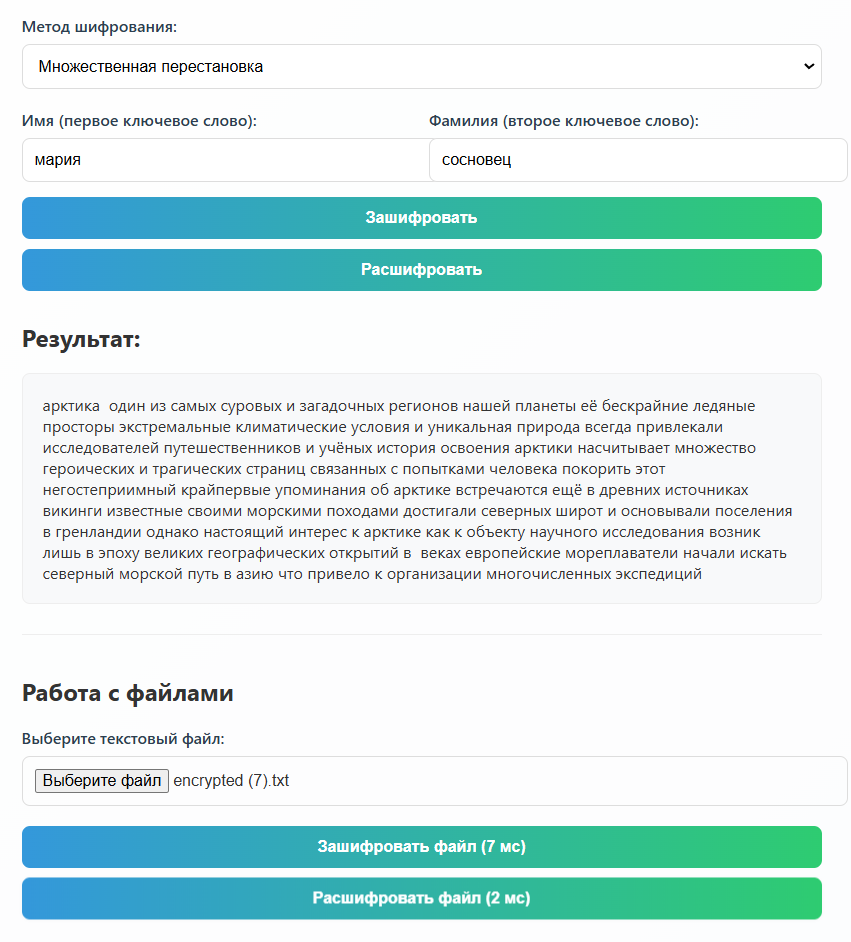
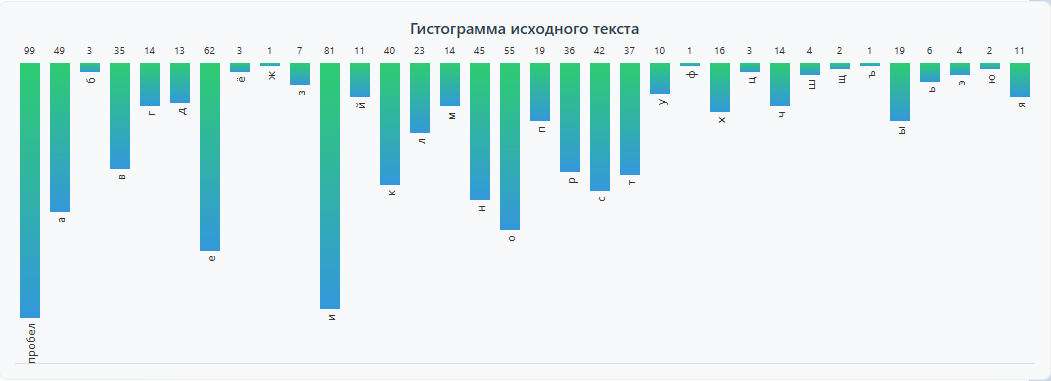


Рисунок 1.4 – Результат расшифрования текста с ключевыми словами «мария» и «сосновец»

На рисунке 1.5 представлены гистограммы частот появления символов для исходного и зашифрованного сообщений;



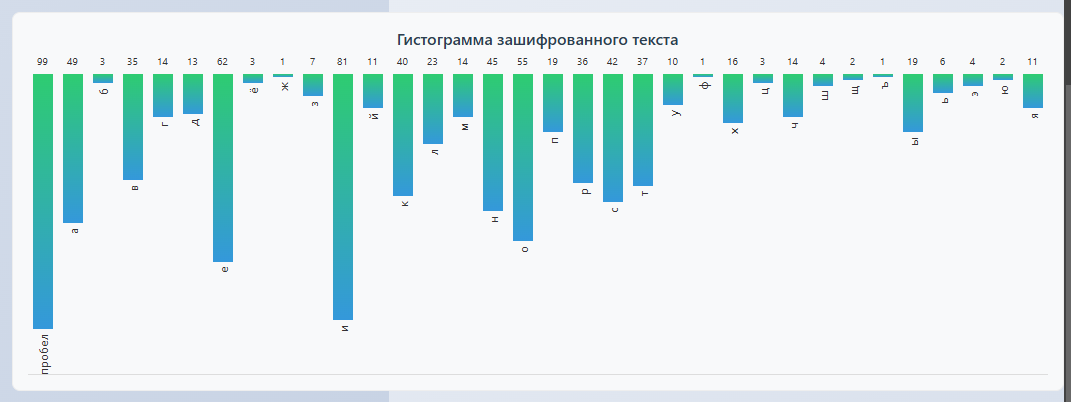
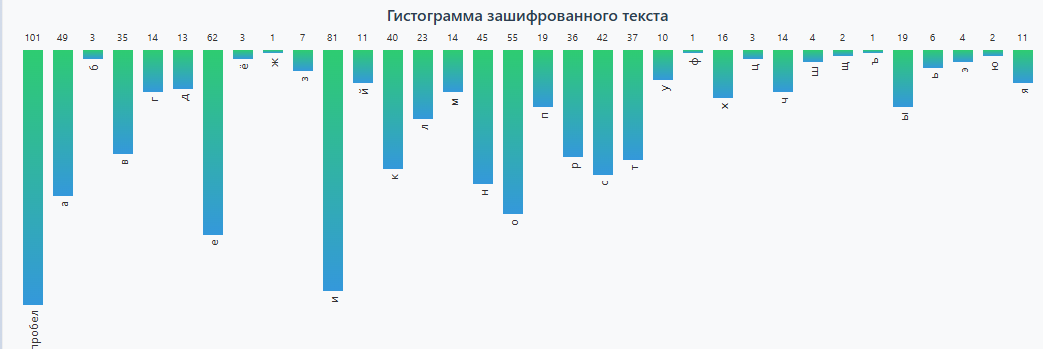


Рисунок 1.5 – Гистограммы частот появления символов для исходного и зашифрованного сообщений (маршрутная)



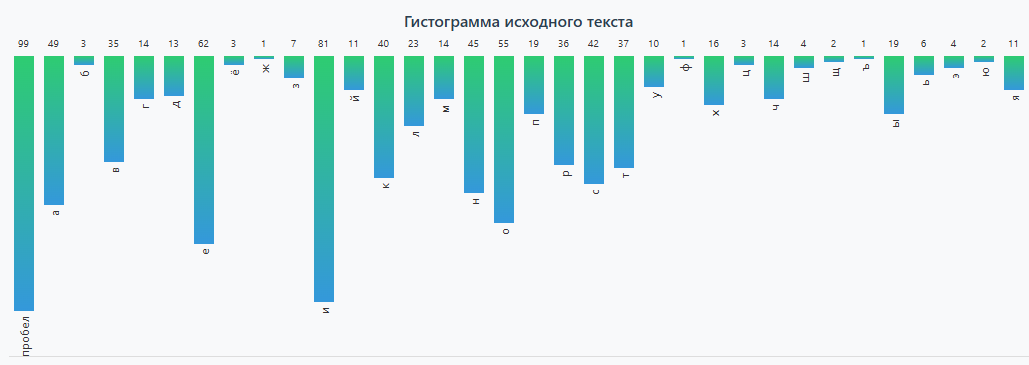


Рисунок 1.5 – Гистограммы частот появления символов для исходного и зашифрованного сообщений (множественная)

Оценка времени выполнения операций зашифрования/расшифрования представлена на рисунке 1.6.

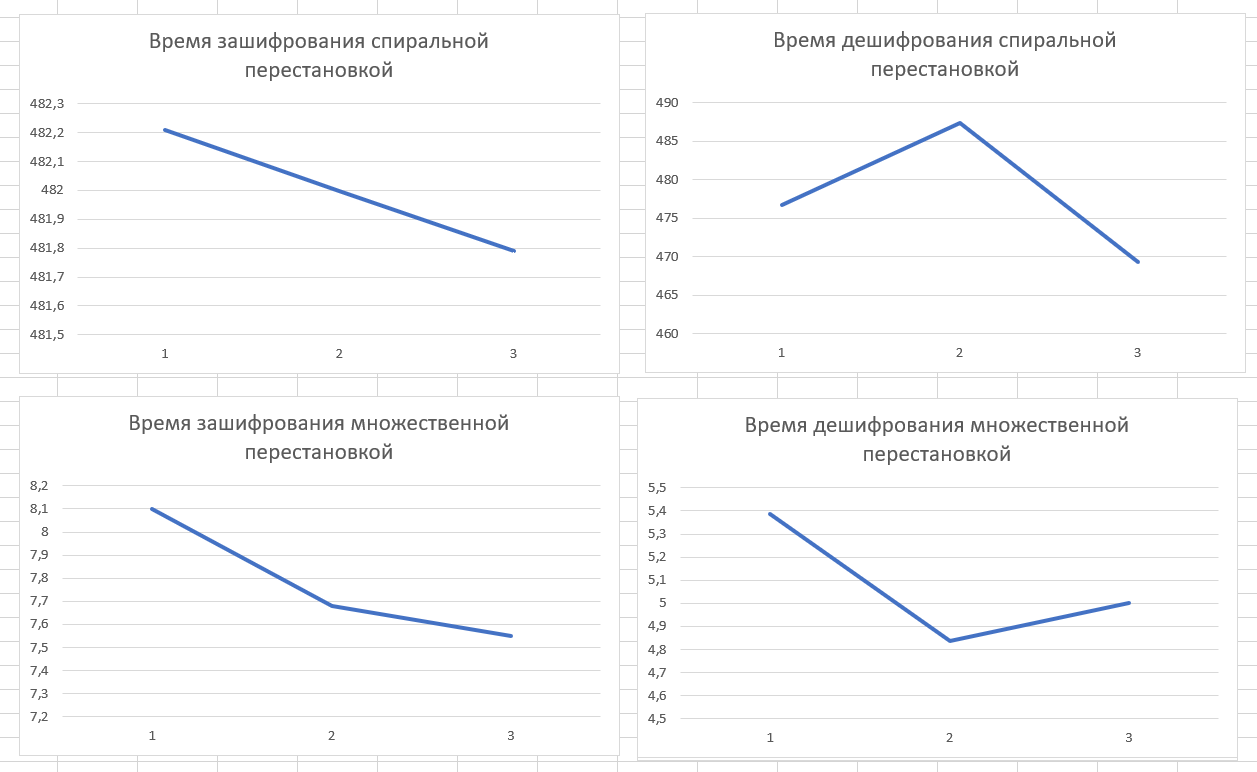


Рисунок 1.6 – Оценка времени выполнения операций зашифрования/расшифрования

**Вывод:**

В данной лабораторной работе мной были изучены и приобретены практических навыков разработки и использования приложений для реализации перестановочных шифров. Были изучены шифры перестановки по спирали и множественной перестановки.