МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Отчет по лабораторной работе №3

Исследование криптологических шифров на основе

перестановки символов

Выполнил студент: Плюто Э. В.

ФИТ 3 курса, 5 группа

Проверил: Савельева М. Г.

Минск 2024

**Практическое задание:**

**1)** Разработать авторское приложение, которое должно выполнять зашифрование/расшифрование текстовых документов, созданных на основе алфавита языка (белорусский), используя маршрутную перестановку (маршрут: запись – по строкам, считывание – по столбцам таблицы; параметры таблицы – по указанию преподавателя).

Реализация зашифрования представлена ниже.

|  |
| --- |
| public static void EncryptFile(string text, char[,] table)  {  string encryptedText = "";  bool isFind = false;  foreach (char symbol in text)  {  if (belarus.Contains(symbol))  {  for (int i = 0; i < table.GetUpperBound(0) + 1; i++)  {  if (isFind)  break;  for (int j = 0; j < table.GetUpperBound(0) + 1; j++)  {  if (isFind)  break;  if (table[i, j] == symbol)  {  encryptedText += table[j, i];  isFind = true;  }  }  }  isFind = false;  }  else  encryptedText += symbol;  }  File.WriteAllText(@"C:\Users\Erik\Desktop\3course\IB\LABA5\Encrypted.txt", encryptedText);  } |

Листинг 1 – Реализация функции шифрования маршрутной перестановки

Для расшифрования использовалась аналогичная функция.

Время выполнения шифрования и расшифрования файла представлено на рисунке 1.

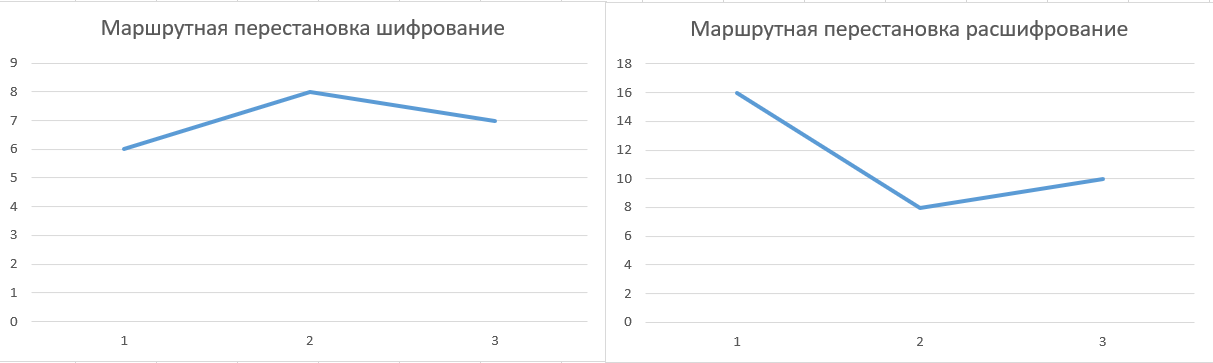


Рисунок 1 – Время выполнения операций шифрования и расшифрования

Гистограмма частоты появления символов файла представлена ниже.

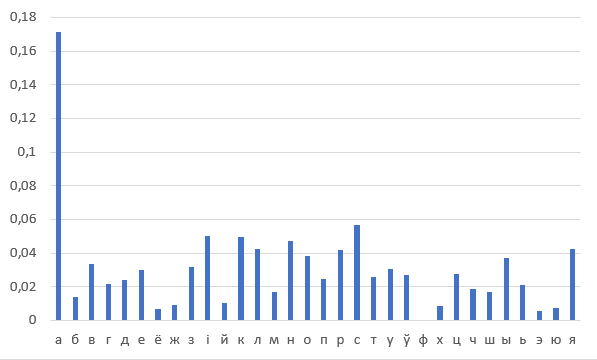


Рисунок 2 – Частота появления символов

**2)** Разработать авторское приложение, которое должно выполнять зашифрование/расшифрование, используя множественную перестановку, ключевые слова – собственные имя и фамилия.

Для шифрования была реализована функция, представленная ниже.

|  |
| --- |
| public static string MultiplePermutationEncrypt(string text, string key1, string key2)  {  int[] X = GetNumbers(key1, belarus);  int[] Y = GetNumbers(key2, belarus);  Console.Write("X: ");  for (int i = 0; i < X.Length; i++)  {  Console.Write(X[i]);  }  Console.WriteLine();  Console.Write("Y: ");  for (int i = 0; i < Y.Length; i++)  {  Console.Write(Y[i]);  }  Console.WriteLine();  char[,] textTable = new char[key1.Length, key2.Length];  int position = 0;  for (int i = 0; i < key1.Length; i++)  {  for (int j = 0; j < key2.Length; j++)  {  textTable[i, j] = text[position];  Console.Write(textTable[i, j] + "\t");  position++;  }  Console.WriteLine();  }  char[] buff = new char[int.Max(key1.Length, key2.Length)];  int buffInt = 0;  for (int i = 0; i < X.Length; i++)  {  if (X[i] != i + 1)  {  for (int j = 0; j < Y.Length; j++)  {  buff[j] = textTable[i, j];  textTable[i, j] = textTable[X[i] - 1, j];  textTable[X[i] - 1, j] = buff[j];  }  buffInt = X[i];  X[i] = i + 1;  X[buffInt - 1] = buffInt;  }  }  for (int i = 0; i < Y.Length; i++)  {  if (Y[i] != i + 1)  {  for (int j = 0; j < X.Length; j++)  {  buff[j] = textTable[j, i];  textTable[j, i] = textTable[j, Y[i] - 1];  textTable[j, Y[i] - 1] = buff[j];  }  buffInt = Y[i];  Y[i] = i + 1;  Y[buffInt - 1] = buffInt;  }  }  string result = "";  for (int i = 0; i < X.Length; i++)  {  for (int j = 0; j < Y.Length; j++)  {  result += textTable[i, j];  }  }  return result;  } |

Листинг 2 – Реализация функции шифрования множественной перестановкой

Результат выполнения данной функции представлен ниже.

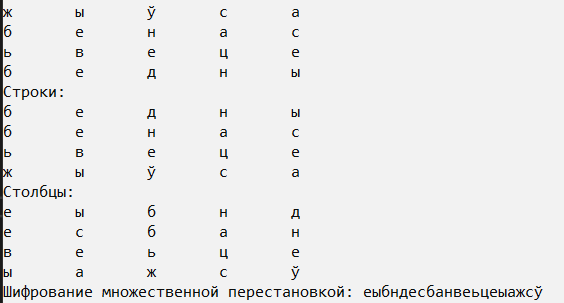


Рисунок 3 – Результат выполнения шифрования и расшифрования

Время выполнения шифрования и расшифрования файла представлено на рисунке 4.

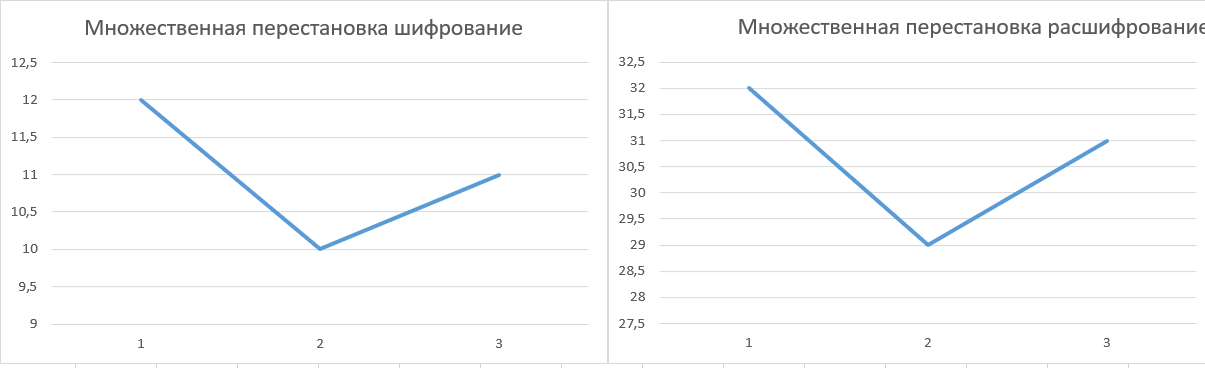


Рисунок 4 – Время выполнения шифрования и расшифрования

Гистограмма частоты появления символов зашифрованного и расшифрованного текста представлена на рисунке 5.

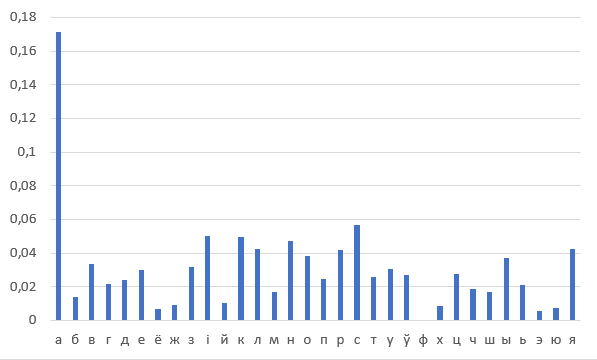


Рисунок 5 – Частота появления символов зашифрованного и расшифрованного текста

При шифровании и расшифровании текста при помощи множественной перестановки получим одинаковые гистограммы частот появления символов.

**Вывод:**

Были приобретены практические навыки разработки и использования приложений для реализации перестановочных шифров. Реализованы функции для шифрования и расшифрования текстов с использованием шифров маршрутной перестановки и множественной перестановки, замерено время выполнения этих функций, а также построены гистограммы частот появления символов.