Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Лабораторная работа №4

**ИССЛЕДОВАНИЕ КРИПТОГРАФИЧЕСКИХ ШИФРОВ НА ОСНОВЕ ПОСТАНОВКИ (ЗАМЕНЫ) СИМВОЛОВ**

Студент: Чёрная Я.Р.

ФИТ 3 курс 4 группа

Преподаватель: Нистюк О.А.

Минск 2025

**Задание 1:**

|  |  |  |
| --- | --- | --- |
| 14 | Немецкий | 1. Виженера, ключевое слово–собственная фамилия  2. Шифр Порты |

Шифр Виженера — это метод шифрования, который использует ключевое слово для создания последовательных сдвигов символов в алфавите. Каждый символ текста сдвигается на величину, определяемую соответствующим символом из ключа, что делает шифрование более сложным по сравнению с простыми методами.

Шифр Порты — это простой метод шифрования, который использует фиксированный сдвиг символов в алфавите. Каждый символ текста смещается на заранее заданное число позиций, сохраняя при этом символы, не входящие в алфавит, без изменений. Это легкий для реализации, но уязвимый метод шифрования.

|  |
| --- |
| public static string VigenereEncrypt(string plaintext, string keyword)  {  string result = "";  int keywordIndex = 0;  foreach (char c in plaintext)  {  if (char.IsLetter(c))  {  char offset = char.IsUpper(c) ? 'A' : 'a';  char keyChar = char.ToLower(keyword[keywordIndex % keyword.Length]);  int shift = keyChar - 'a';  // Зашифровка символа  char encryptedChar = (char)((c + shift - offset) % 26 + offset);  result += encryptedChar;  keywordIndex++;  }  else  {  result += c;  }  }  return result;  } |

Листинг 1.1 – реализация алгоритма Виженера

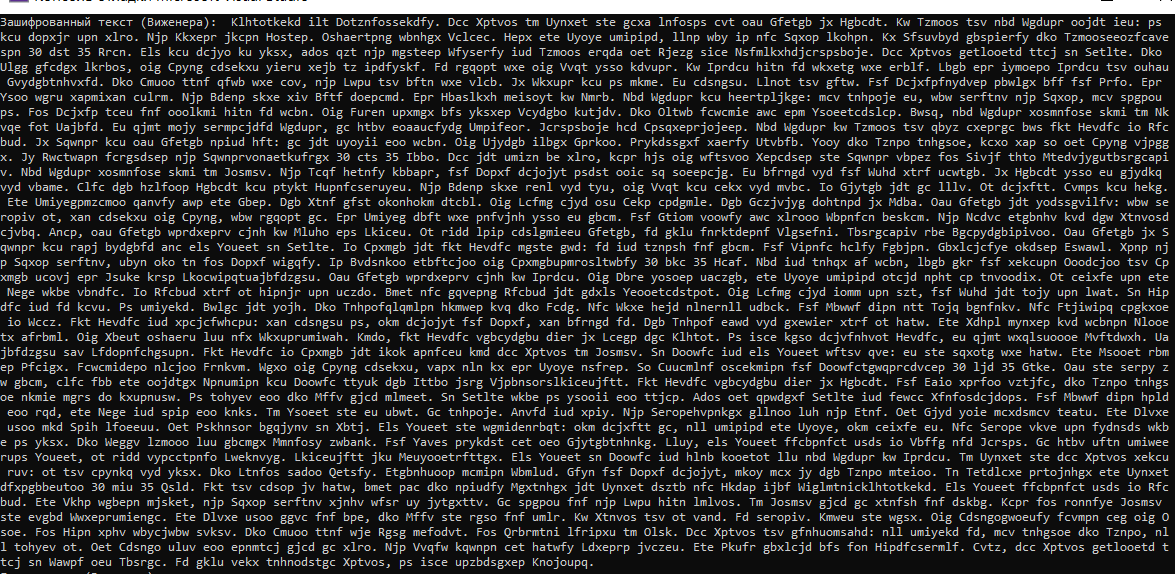


Рисунок 1.1 – Результат зашифрования текста Виженера

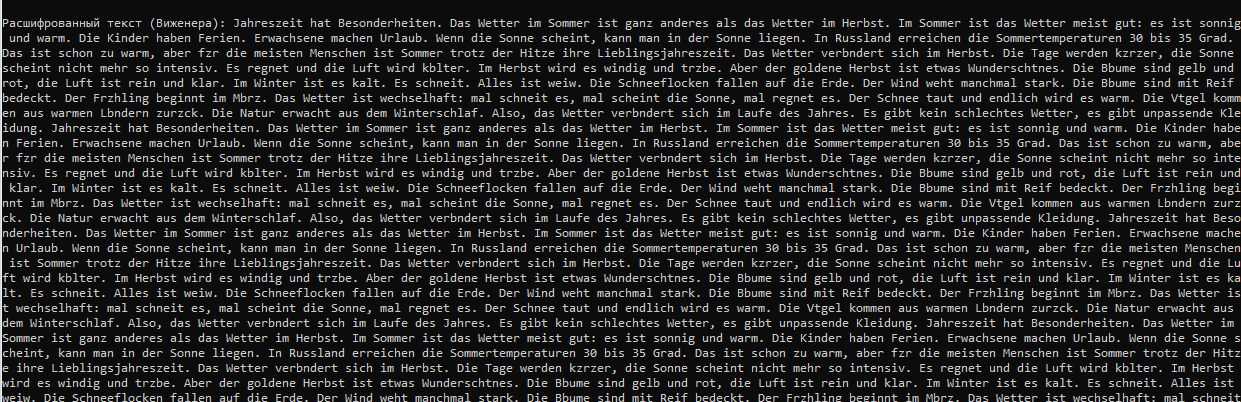
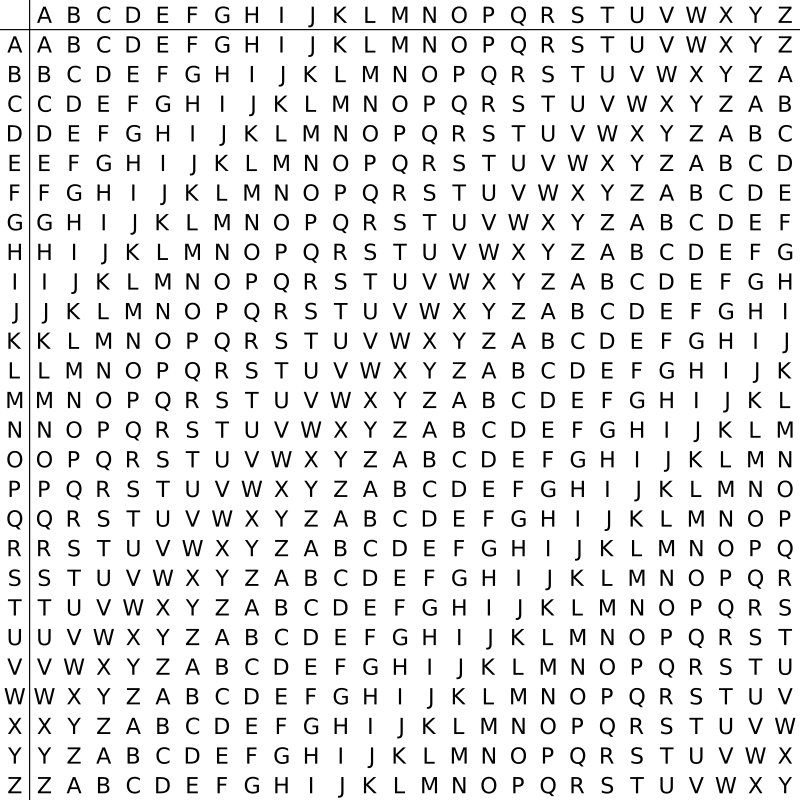


Рисунок 1.2 – Результат расшифрования текста Виженера

|  |
| --- |
| public static string PortEncrypt(string plaintext)  {  int shift = 3; // Фиксированный сдвиг  string result = "";  foreach (char symbol in plaintext)  {  if (char.IsLetter(symbol))  {  char offset = char.IsUpper(symbol) ? 'A' : 'a';  char encryptedChar = (char)((symbol + shift - offset) % 26 + offset);  result += encryptedChar;  }  else  {  result += symbol;  }  }  return result;  } |

Листинг 1.2 – реализация шифрования Порты

В качестве затлиццы для шифрования методом Порты была взята таблица, приведенная на русунке ниже.



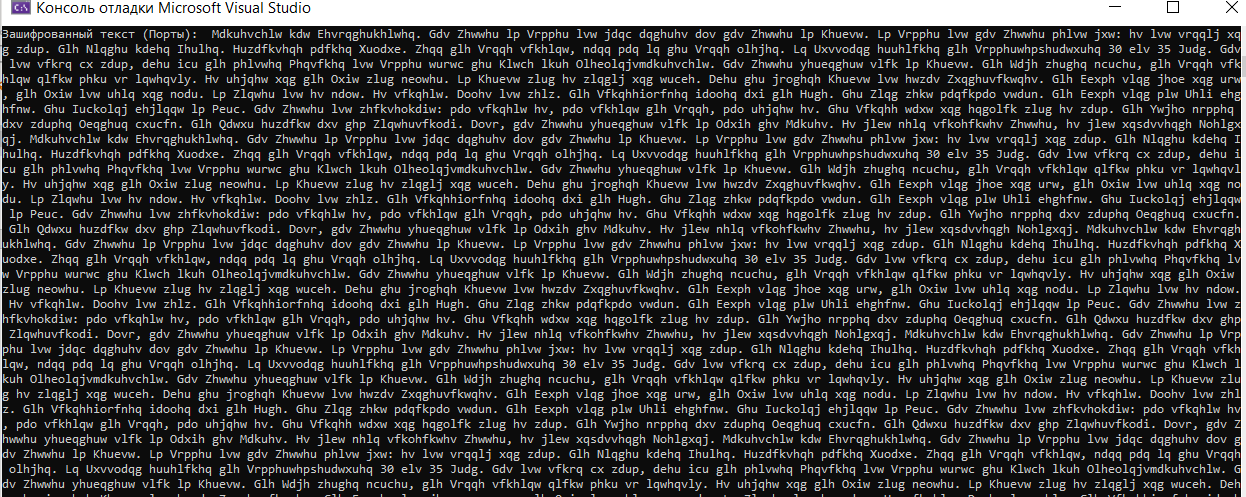


Рисунок 1.3 – Результат зашифрования текста Порты

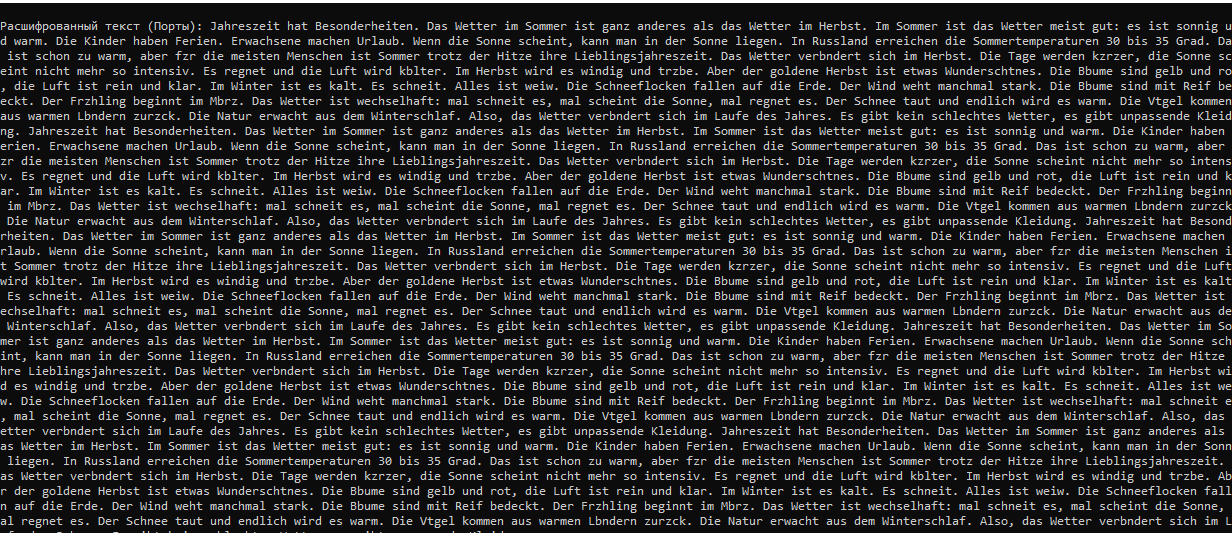
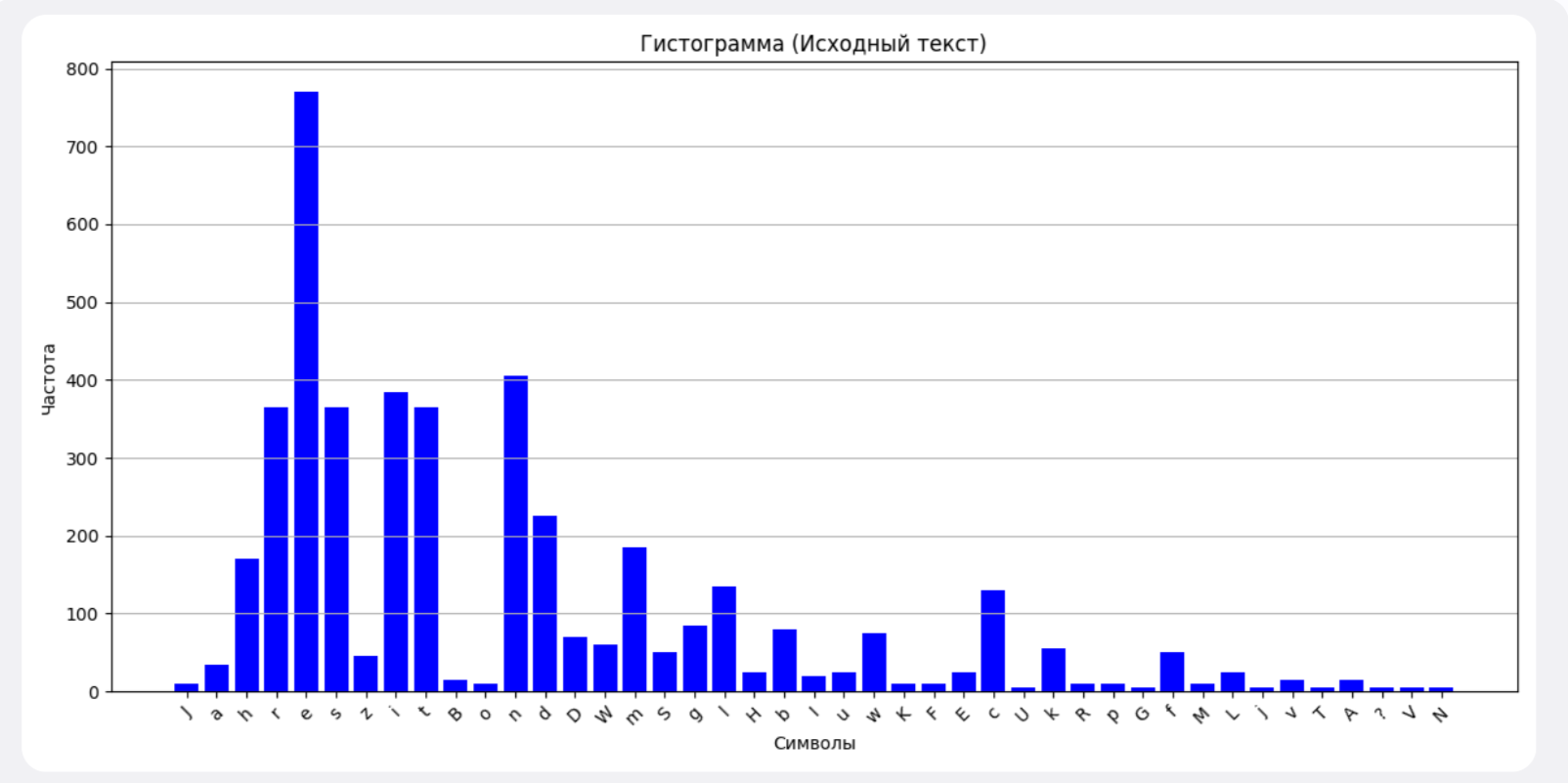


Рисунок 1.4 – Результат расшифрования текста Порты



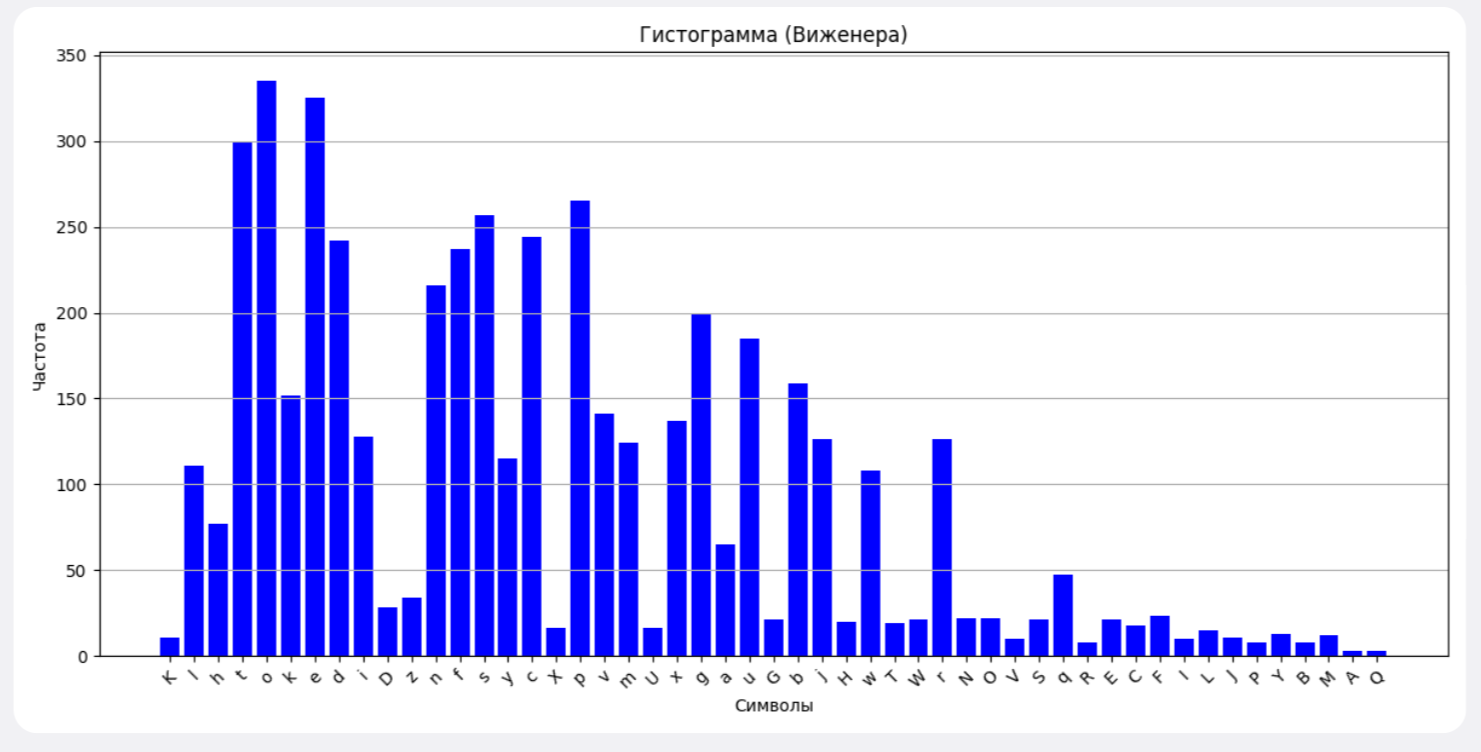


Рисунок 1.5 – Гистограммы частот появления символов для исходного и зашифрованного сообщений

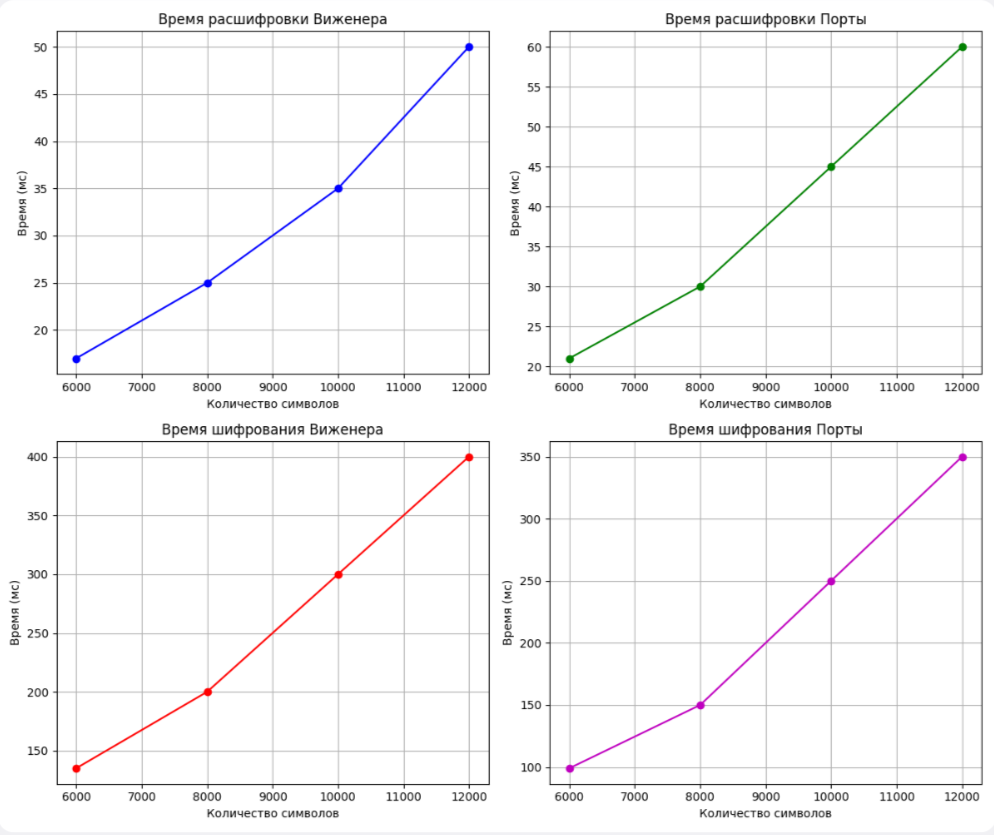


Рисунок 1.6 – Оценка времени выполнения операций зашифрования/расшифрования

**Вывод:**

В данной лабораторной работе мной были изучены и приобретены практических навыков разработки и использования приложений для реализации подстановочных шифров.