МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №4 НА ТЕМУ:**

**Исследование криптографических шифров на основе подстановки (замены) символов**

Выполнила студентка 3 курса 5 группы

Авсюкевич Полина Вадимовна

Минск 2024

**Задание 1:** Разработать авторское приложение в соответствии с целью лабораторной работы. Приложение должно реализовывать следующие операции: выполнять зашифрование/расшифрование текстовых документов (объемом не менее 5 тысяч знаков), созданных на основе алфавита Исследование криптографических шифров на основе подстановки (замены) символов 37 языка в соответствии с нижеследующей таблицей вариантов задания;

Реализация данной функциональности представлена в листинге 1:

|  |
| --- |
| static string GetPrimeFactors(int n)  {  List<int> factors = new List<int>();  int divisor = 2;  while (divisor \* divisor <= n){  if (n % divisor == 0){  factors.Add(divisor);  n /= divisor;}  else  divisor++;}  if (n > 1)  factors.Add(n);  string canonicalForm = $"{n} = {factors[0]}";  for (int i = 1; i < factors.Count; i++){  canonicalForm += $" \* {factors[i]}"; }  return canonicalForm;  } |

Листинг 1 – Реализация функции зашифрования на основе соотношения

Надо было замерить время шифрования и дешифрования представлено на рисунке 1, 2 представлены графики времени выполнения для шифрования дешифрования.

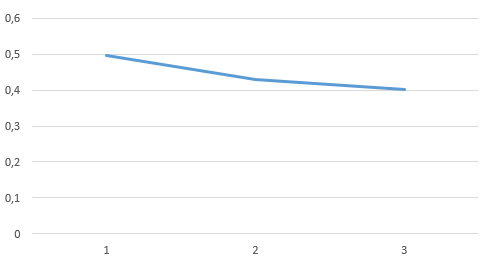


Рисунок 1 – Время для шифрования

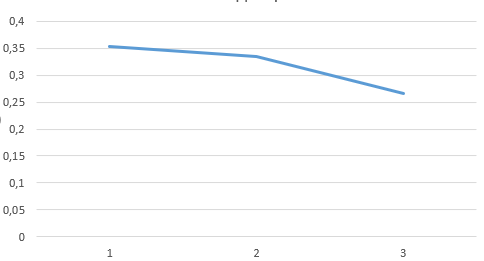


Рисунок 2 – Время для дешифрования

Задание 2. Зашифровать/расшифровать текстовые документы (объем не менее 5 тысяч знаков), созданных на основе алфавита языка в соответствии с заданным вариантом (английский), используя шифр Виженера, ключевое слово – собственная фамилия. Код реализации представлен на листинге 2.

|  |
| --- |
| public string Encrypt(string input)  {  StringBuilder result = new StringBuilder();  input = input.ToLower(); // Приводим все буквы к нижнему регистру  for (int i = 0; i < input.Length; i++)  {  char symbol = input[i];  int x = Alphabet.IndexOf(symbol);  if (x < 0)  {  result.Append(symbol);  }  else  {  int k = Alphabet.IndexOf(\_key[i % \_key.Length]);  int y = (x + k) % \_n;  result.Append(Alphabet[y]);  }  }  return result.ToString();  } |

Листинг 2 – Реализация функции зашифрования на шифра Виженера

Надо было замерить время шифрования и дешифрования представлено на рисунке 3, 4.

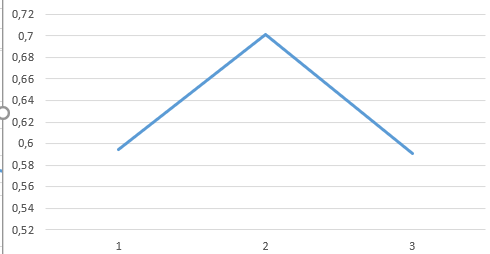


Рисунок 3 – Время для шифрования

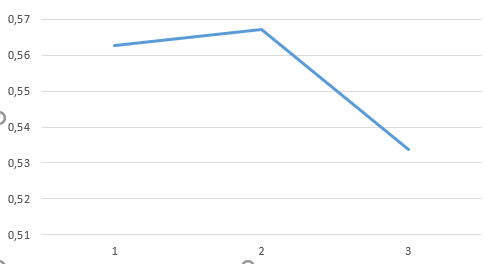


Рисунок 4 – Время для дешифрования

Задание 3. Сформировать частоты появления символов для исходного и зашифрованного сообщений.

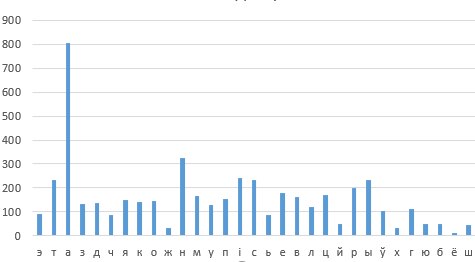


Рисунок 5 – Частота появления символов исходного текста

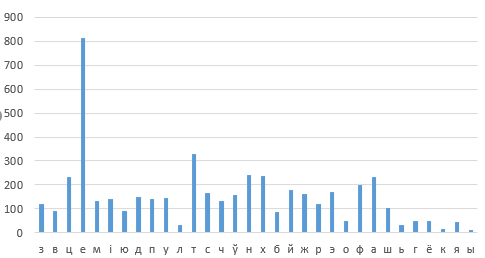


Рисунок 6 – Частота появления символов на основе соотношения

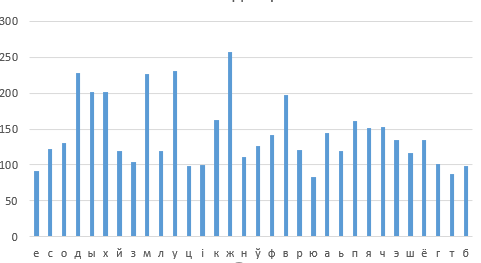


Рисунок 7 – Частота появления символов таблицы Виженера

В процессе выполнения лабораторной работы были освоены навыки создания и применения приложений для реализации подстановочных шифров. Также проведена оценка скорости операций шифрования и расшифрования, реализованных методов шифрования.