Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий

Кафедра информационных систем и технологий

**Лабораторная работа № 4**

«Исследование криптографических шифров на основе подстановки (замены) символов»

Выполнил:

Студент: Герман А.Е.

ФИТ 3 курса 5 группы

Преподаватель: Савельева М.Г.

Минск 2024

# **1 Описание приложения**

Данное консольное приложение, разработанное на языке программирования C#, предназначено для анализа текстового файла и шифрования его в соответствии с двумя алгоритмами замены.

Основные функциональности приложения:

* Чтение текстового файла;
* Конвертация содержимого текстового файла в сплошной текст;
* Шифрование текста с помощью аффинного преобразования Цезаря;
* Шифрование текста с помощью шифра Порта.

# **2 Методика выполнения расчетов**

В данной лабораторной работе была поставлена цель создания приложения, позволяющее конвертировать текст и шифровать его. На листингах 2.1 и 2.2 представлен классы, реализующий данную функциональность.

|  |
| --- |
| class EncoderK  {  public string alphabet;  public int a, b;  public string editedAlphabet;  public EncoderK(string alphabet, int a, int b)  {  this.alphabet = alphabet;  this.a = a;  this.b = b;  this.editedAlphabet = editAlphabet(alphabet, a, b);  }  public string editAlphabet(string alphabet, int a, int b)  {  StringBuilder newAlphabet = new StringBuilder();  for (int iter = 0; iter < alphabet.Length; iter++)  {  int newPos = (a \* iter + b) % alphabet.Length;  newAlphabet.Append(alphabet[newPos]);  }  return newAlphabet.ToString();  }  public string encode(string text)  {  StringBuilder encodedText = new StringBuilder();  for (int iter = 0; iter < text.Length; iter++)  {  int pos = this.alphabet.IndexOf(text[iter]);  int newPos = (a \* pos + b) % alphabet.Length;  char encSymbol = this.editedAlphabet[newPos];  encodedText.Append(encSymbol);  }  return encodedText.ToString();  }  public string decode(string text)  {  StringBuilder decodedText = new StringBuilder();  int aInverse = ModInverse(a, alphabet.Length);  for (int iter = 0; iter < text.Length; iter++)  {  int pos = this.editedAlphabet.IndexOf(text[iter]);  int newPos = (aInverse \* (pos - b + alphabet.Length)) % alphabet.Length;  char decSymbol = this.alphabet[newPos];  decodedText.Append(decSymbol);  }  return decodedText.ToString();  }  private int ModInverse(int a, int m)  {  a = a % m;  for (int x = 1; x < m; x++)  {  if ((a \* x) % m == 1)  return x;  }  return 1;  }  } |

Листинг 2.1 – Класс **EncoderK**, реализующий функционал для работы аффинного шифрования Цезаря

|  |
| --- |
| public class EncoderPorta  {  private readonly Dictionary<char, int> letterToNumber;  private readonly Dictionary<int, char> numberToLetter;  public EncoderPorta()  {  letterToNumber = new Dictionary<char, int>();  numberToLetter = new Dictionary<int, char>();  string polishAlphabet = "AĄBCĆDEĘFGHIJKLŁMNŃOÓPRSŚTUWYZŹŻ";  for (int i = 0; i < polishAlphabet.Length; i++)  {  letterToNumber[polishAlphabet[i]] = i + 1;  numberToLetter[i + 1] = polishAlphabet[i];  }  }  public string Encrypt(string plaintext)  {  plaintext = plaintext.ToUpper();  List<int> encryptedNumbers = new List<int>();  foreach (char c in plaintext)  {  if (letterToNumber.ContainsKey(c))  {  int number = letterToNumber[c];  encryptedNumbers.Add(number);  }  }  return string.Join(" ", encryptedNumbers);  }  public string Decrypt(string ciphertext)  {  string[] numbers = ciphertext.Split(' ');  List<char> decryptedLetters = new List<char>();  foreach (string number in numbers)  {  if (int.TryParse(number, out int num))  {  if (numberToLetter.ContainsKey(num))  {  char letter = numberToLetter[num];  decryptedLetters.Add(letter);  }  }  }  return string.Join("", decryptedLetters);  } |

Листинг 2.2 – Класс **EncoderPorta**, реализующий функционал для шифрования Порта

# **3 Результаты работы приложения**

Для выполнения расчетов достаточно необходимо запустить приложение. Рисунки 3.1 - 3.3 показывают необходимые расчеты и вызовы методов, требуемые в данной лабораторной работе.

## **3.1 Аффинное шифр Цезаря**

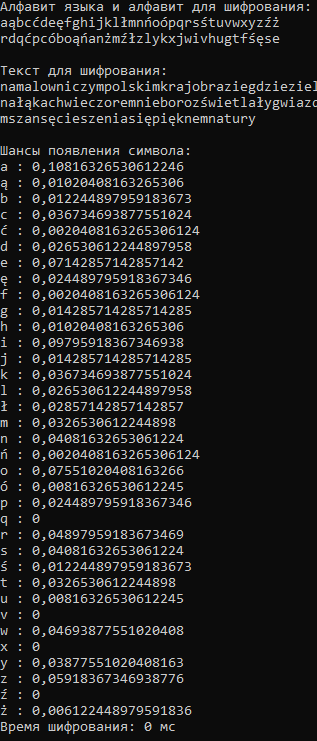
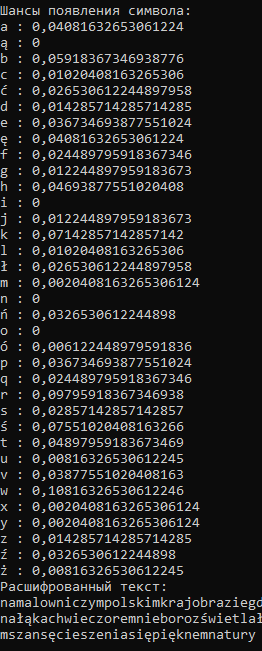
 

Рисунок 3.1 – Результат работы методов класса **EncoderK** с входного файла

В качестве тестового текста было использован файл polish.txt. а = 17, b = 23. Используя аффинный шифр Цезаря был найден зашифрованный алфавит, с помощью которого выполнялось шифрование. Время шифрования меньше, чем 0 мс.

## **3.2 Шифр Порта**

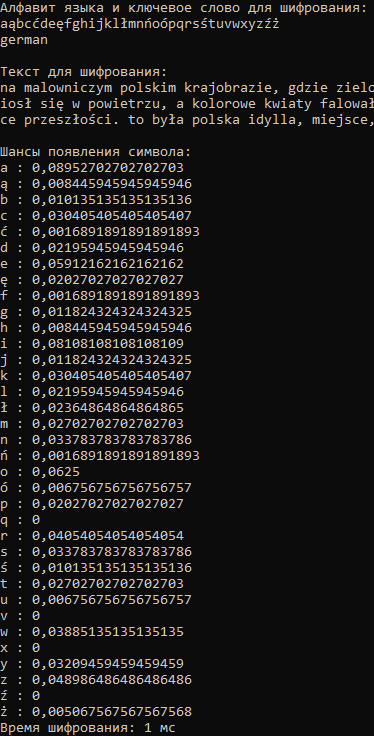
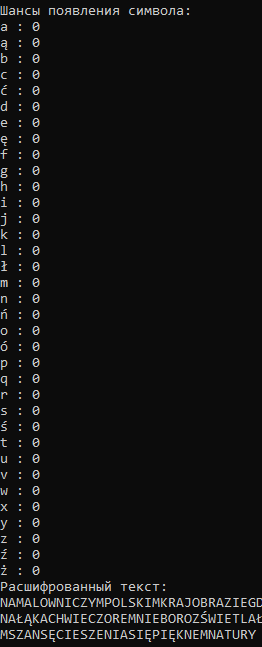
 

Рисунок 3.2 – Результат работы методов класса **EncodedPorta**

Текст расшифровывается корректно, за исключением пробелов. Время шифрования 1 мс.

## **3.3 Гистограммы**

Рисунок 3.3 – Гистограмма вероятностей для исходного текста (шифр Цезаря)

Рисунок 3.4 – Гистограмма вероятностей для зашифрованного текста (шифр Цезаря)

Рисунок 3.5 – Гистограмма вероятностей для зашифрованного текста (шифр Порта)

Рисунок 3.6 – Гистограмма вероятностей для зашифрованного текста (шифр Порта)

## **3.4 График времени**

# **4 Вывод**

В ходе изучения теоретических материалов лабораторной работы и выполнения её практической части были изучены основы теории информации и анализа энтропии. Это консольное приложение, разработанное на языке программирования C#, предоставляет функциональности, направленные на измерение энтропии в различных сценариях, связанных с текстовыми данными.