**Лабораторная работа № 2**

Тема: Базовые алгоритмы шифрования данных

Цель работы: изучение основных принципов шифрования информации, знакомство с широко известными алгоритмами шифрования, приобретение навыков их программной реализации.

**Задание: Реализовать в программе шифрование и дешифрацию содержимого файла по методу Цезаря с ключевым словом.**

На С#:

using System;

using System.Collections.Generic;

using System.Linq;

using System.Text;

using System.Threading.Tasks;

namespace CaesarWithKnife

{ class Caesar

{ private static string alpha = "abcdefghijklmnopqrstuvwxyz";

private static char[] newAlpha = new char[26];

public static string encrypt(string Message)

{ string res = "";

foreach (char ch in Message)

{ for (int i = 0; i < alpha.Length; i++)

{ if (ch == alpha[i])

{res += newAlpha[i];

break; } } }

return res; }

public static string decrypt(string Message)

{string res = "";

foreach (char ch in Message)

{ for (int i = 0; i < newAlpha.Length; i++)

{ if (ch == newAlpha[i])

{ res += alpha[i];

break; } } }

return res; }

public static void createNewAlpha(string keyWord, int key) // создаёт новый алфавит с помощью ключа

{

bool findSame = false;

key--;

int beg = 0, current = key;

// добавить ключевое слово в новый алфавит

for (int i = key; i < keyWord.Length + key; i++)

{ for (int j = key; j < keyWord.Length + key; j++)

{ if (keyWord[i - key] == newAlpha[j])

{ findSame = true;

break; } }

if (!findSame)// если повторений нет, то буква добавляется в новый алфавит

{ newAlpha[current] = keyWord[i - key];

current++; }

findSame = false; } // добавить буквы после ключевого слова

for (int i = 0; i < alpha.Length; i++)

{ for (int j = 0; j < newAlpha.Length; j++)

{ if (alpha[i] == newAlpha[j])

{ findSame = true;

break; } }

if (!findSame)

{ newAlpha[current] = alpha[i];

current++; }

findSame = false;

if (current == newAlpha.Length)

{ beg = i;

break; } } // добавить буквы после ключевого слова

current = 0;

for (int i = beg; i < alpha.Length; i++)

{ for (int j = 0; j < newAlpha.Length; j++)

{ if (alpha[i] == newAlpha[j])

{ findSame = true;

break; } }

if (!findSame)

{ newAlpha[current] = alpha[i];

current++; }

findSame = false; } }

public static string getNewAlpha()

{ string strNewAlpha = new string(newAlpha);

return strNewAlpha; } } }

**Контрольные вопросы:**

1. *Дайте определение следующим понятиям: шифр, криптография, криптоанализ, ключ.*

* Шифр — система обратимых преобразований, зависящая от некоторого секретного параметра (ключа) и предназначенная для обеспечения секретности передаваемой информации.
* Криптография — это наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним), целостности данных (невозможности незаметного изменения информации), аутентификации (проверки подлинности авторства или иных свойств объекта).
* Криптоана́лиз — наука о методах дешифровки зашифрованной информации без предназначенного для этого ключа, а также сам процесс такой дешифровки.
* Ключ — секретная информация, используемая криптографическим алгоритмом при шифровании/расшифровке сообщений, постановке и проверке цифровой подписи, вычислении кодов аутентичности.

1. *Чем отличаются одно- и многоалфавитные методы шифрования?*

* Одноалфавитный метод шифрования.

В его основе лежит простой способ шифрования: отправитель и получатель зашифрованного документа заранее договариваются об определенном смешении букв относительно их обычного местоположения в алфавите.

* Многоалфавитный метод шифрования.

В многоалфавитных подстановках для замены символов исходного текста используется не один, а несколько алфавитов. Обычно алфавиты для замены образованы из символов исходного алфавита, записанных в другом порядке.

1. *В чем заключается основной принцип частотного криптоанализа? В чем заключается основной принцип частотного криптоанализа?*

Частотный анализ, частотный криптоанализ — один из методов криптоанализа, основывающийся на предположении о существовании нетривиального статистического распределения отдельных символов и их последовательностей, как в открытом тексте, так и в шифротексте, которое, с точностью до замены символов, будет сохраняться в процессе шифрования и дешифрования.