МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное автономное бюджетное образовательное учреждение высшего образования

«**Севастопольский государственный университет**»

кафедра Информационных систем

Институт информационных технологий и управления в технических системах

Лисянский Александр Игоревич

курс 4 группа ИС/б-42-о

09.03.02 Информационные системы (уровень бакалавриата)

**ОТЧЁТ**

о лабораторном практикуме №1

ШИФРОВАНИЕ ДАННЫХ МЕТОДАМИ ПОДСТАНОВКИ, ПЕРЕСТАНОВКИ И ПОЛИАЛФАВИТНЫМИ ШИФРАМИ

по дисциплине «Основы защиты информации»

Отметка о зачёте \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_

(дата)

Руководитель практикума

\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(должность) (подпись) (инициалы, фамилия)

Севастополь

2016

**Цель работы**: Приобретение навыков шифрования информации с использованием простейших методов шифрования.

**Вариант задания**:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 13 | Подстановка | 2 | 5 | Английский алфавит |
| 15 | Перестановка | 3 | 5 | ASCI-код |

Таблица перестановки

|  |  |
| --- | --- |
| 5 |  |

**Метод подстановки**: Наиболее простой вид преобразований, заключающийся в замене символов исходного текста на другие (того же алфавита) по более или менее сложному правилу. Для обеспечения высокой криптостойкости требуется использование больших ключей. В основе метода лежит принцип кодировочной таблицы. Простые подстановки широко используются в качестве головоломок. Ключом к шифрованию является перестановочный алфавит. Это позволяет заменять буквы в словах буквами из такого алфавита. Рассмотрим метод подстановки на примере. Перестановочный алфавит составлен по следующему правилу:

А(2К-1)=В(2К); А(2К)=В(33-2К),

где А - перестановочный алфавит;

В - исходный алфавит;

1≤ К ≤ 16.

Воспользуемся новым алфавитом для шифрования фразы:

ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

Каждая буква в этой фразе имеет порядковый номер в исходном алфавите. При шифровании методом подстановки необходимо заменить буквы исходного алфавита соответствующими буквами перестановочного алфавита (О - П, С - О, Н - Т и т.д.).

В шифрованном виде эта фраза примет следующий вид:

ПОТПГЭ ШБЖЙУЭ ЙТХПСНБЧЙЙ.

Шифрование простой подстановкой на коротких алфавитах обеспечивает слабую защиту открытого текста. Подстановочные криптограммы можно раскрыть, составляя частотные таблицы для букв, пар букв (биграмм) и троек букв (триграмм). Большие частоты появления одних букв и малые других, а также частые ассоциации гласных с согласными позволяют найти буквы открытого текста. С увеличением размера алфавита применение частотного анализа становится все более дорогим, однако, принцип подстановки теряет свою практическую значимость.

**Метод перестановки**: Также несложный метод криптографического преобразования. Используется, как правило, в сочетании с другими методами. При шифровании этим методом переставляются не буквы алфавита, а буквы открытого текста. Например, сообщение разбито на 4 группы знаков, включая пробелы, и в каждой группе буквы переставлены в соответствии с правилом:

⎡1 2 3 4 ⎤

⎣2 4 1 3⎦

В этом случае фраза:

ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

будет представлена в следующем виде:

СООНЫЗВ ЩТАИ НЫИОМФРИАИ.

В случае перестановки таблицы частот для пар и трех букв показывают наличие стандартных буквенных пар, позволяя реконструировать открытый текст путем поиска тех перестановок, которые их воссоединяют. Следовательно, ключ, используемый для преобразования открытого текста, может быть восстановлен по одной криптограмме.

**Ход работы**: В соответствии с вариантом задания был разработан алгоритм шифрования сообщений пользователя несколькими методами.

В результате было принято решение о создании графического интерфейса программы с возможностью выбора вида шифрования сообщения. По каждому из методов была определена своя вкладка.

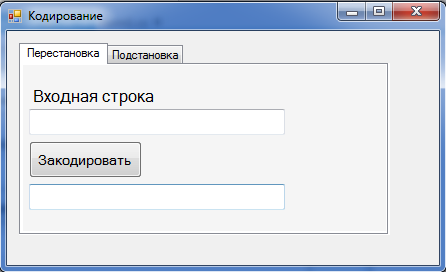


Рисунок 1 – интерфейс программы

Проверяем работу программы. Введем самое простое выражение для двух видов кодировки

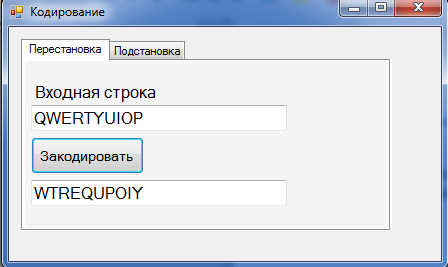


Рисунок 2 – кодирование перестановкой

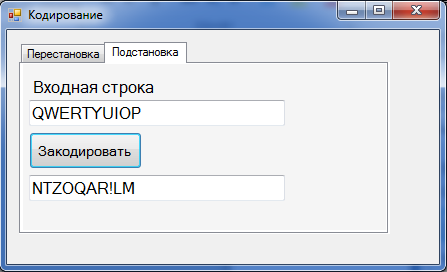


Рисунок 3 – кодирование подстановкой

В результате проверки было получено заключение, что программа работает правильно, кодировка удается.

Код программы:

using System;

using System.Collections.Generic;

using System.ComponentModel;

using System.Data;

using System.Drawing;

using System.Linq;

using System.Text;

using System.Threading.Tasks;

using System.Windows.Forms;

namespace Sasha

{

public partial class CodingForm : Form

{

public CodingForm()

{

InitializeComponent();

}

private void codeSubstitution\_Click(object sender, EventArgs e)

{

string result = "";

string alf = "ABCDEFGHIJKLMNOPQRSTUVWXYZ .,!:;?-";

string alfres = "VWXYZ .,!:;?-KLMNOPQRSTUABCDEFGHIJ";

foreach (char c in inStringSubstitution.Text)

{

result += alfres[alf.IndexOf(c)];

}

outStringSubstitution.Text = result;

}

private void codeRearrange\_Click(object sender, EventArgs e)

{

int[] permutation = {2, 5, 4, 3, 1};

string result = "";

for (int i = 0; i < inStringRearrange.TextLength; i+=5)

{

if (inStringRearrange.TextLength - i > 5)

{

for (int k = 0; k < 5; k++)

{

result += inStringRearrange.Text[permutation[k] + i - 1];

}

}

else

{

if (inStringRearrange.TextLength - i > 2)

for (int k = 0; k < inStringRearrange.TextLength - i; k++)

{

result += inStringRearrange.Text[permutation[k] + i - 1];

}

else

{

result += inStringRearrange.Text[inStringRearrange.TextLength - 1];

}

}

}

outStringRearrange.Text = result;

}

}

}

Вывод: В результате выполнения лабораторной работы были получены навыки по разработке алгоритмов кодирования методами подстановки и перестановки, на основе полученных алгоритмов разработаны функции кодирования, а так же написана и отлажена программа с полученными функциями. Результаты тестирования программы показали, что алгоритмы разработаны верно, программа работает правильно.