Федеральное государственное автономное

образовательное учреждение

высшего образования

«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

|  |
| --- |
| Институт космических и информационных технологий |
| институт |
| Информатика |
| кафедра |

**ОТЧЕТ ПО ПРАКТЧЕСКОЙ РАБОТЕ №1**

|  |
| --- |
| по Информационной безопасности и защите информации |
| наименование дисциплины  Простые симметричные шифры |
| тема |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Преподаватель | |  |  |  |  |
|  | |  | подпись, дата |  | инициалы, фамилия |
| Студент | КИ19-16/1Б |  |  |  | Горовенко Н. М,  Горячкин А.Д  Рубникович С. О.  Непомнящий А.Д. |
|  | номер группы, зачетной книжки |  | подпись, дата |  | инициалы, фамилия |

Красноярск 2021

**СОДЕРЖАНИЕ**

Цель и задачи 3

1 Ход работы 4

1.1 Алгоритмы шифрования и дешифрования 4

1.2 Усовершенствованные алгоритмы шифрования и дешифрования 8

ЗАКЛЮЧЕНИЕ 13

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ 14

## Цель и задачи

**Цель:**

Ознакомиться с основами симметричного шифрования, ознакомиться с простыми симметричными криптографическими шифрами на основе методов подстановок, перестановок и гаммирования, освоить основные этапы проектирования и реализации симметричных шифров.

**Задачи:**

Согласно вашему персональному варианту или индивидуальному заданию преподавателя разработайте и составьте в виде блоксхемы алгоритмы шифрования и дешифрования текста. Убедитесь в правильности составления алгоритмов и затем на языке программирования составьте программу, которая реализует данные алгоритмы.

На ряде контрольных примеров (не менее 10) открытого текста, состоящего из различного количества символов, проверьте правильность работы алгоритмов шифрования и дешифрования.

Самостоятельно или с помощью преподавателя придумайте оригинальный способ модификации шифра с целью повышения его криптостойкости. Внесите изменения в исходный алгоритм и программу. Проверьте работоспособность алгоритма на тестовых примерах.

Докажите, что предложенный Вами способ модификации действительно повышает криптостокость.

Разработанная Вами программа должна содержать графический интерфейс пользователя.

## Ход работы

### Алгоритмы шифрования и дешифрования

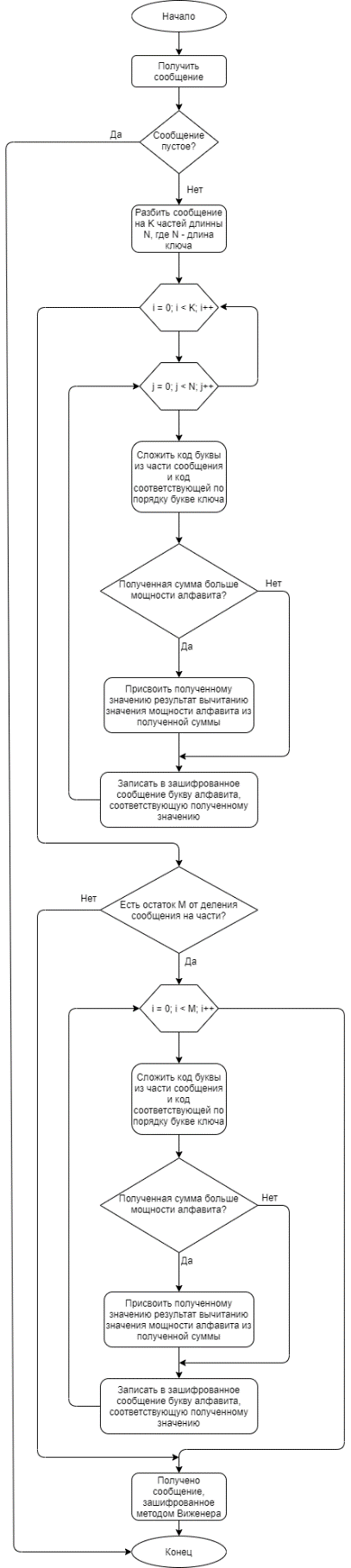


Рисунок 1 – Блок-схема алгоритма шифрования

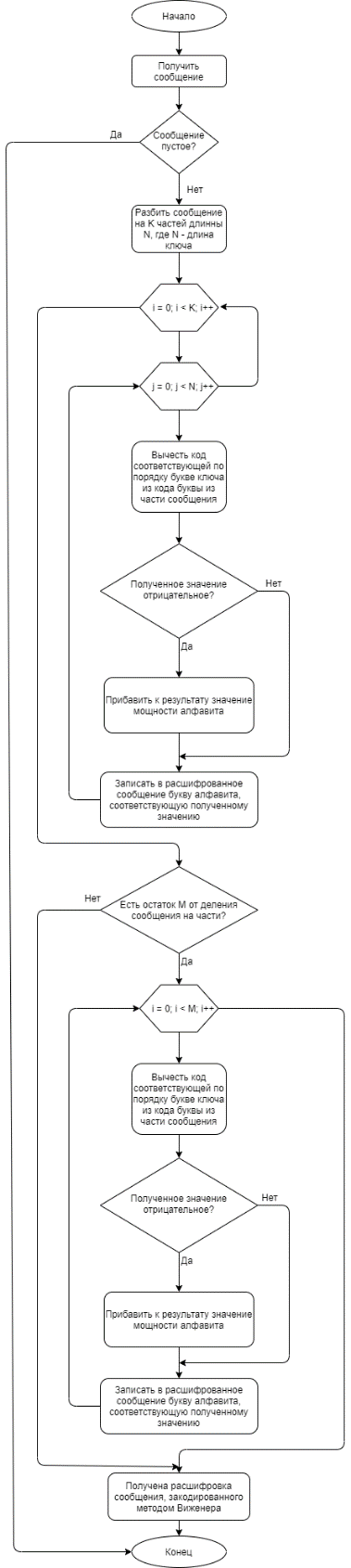


Рисунок 2 – Блок-схема алгоритма дешифрования

Листинг 1 — алгоритм шифрования

public override void Encrypt()

{

\_words = new string(InputString);

string result = "";

// шифрование

if (!string.IsNullOrEmpty(Key))

{

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

{

var index = \_alphabetEn.IndexOf(\_words[i]) + \_alphabetEn.IndexOf(Key[i % Key.Length]);

index %= \_alphabetEn.Length;

result += \_alphabetEn[index];

}

}

OutputString = result;

}

Листинг 2 – алгоритм дешифрования

public override void Decrypt()

{

\_words = new string(InputString);

string result = "";

// дешифрование

if (!string.IsNullOrEmpty(Key))

{

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

{

var index = \_alphabetEn.IndexOf(\_words[i]) - \_alphabetEn.IndexOf(Key[i % Key.Length]) +

\_alphabetEn.Length;

index %= \_alphabetEn.Length;

result += \_alphabetEn[index];

}

}

OutputString = result;

}

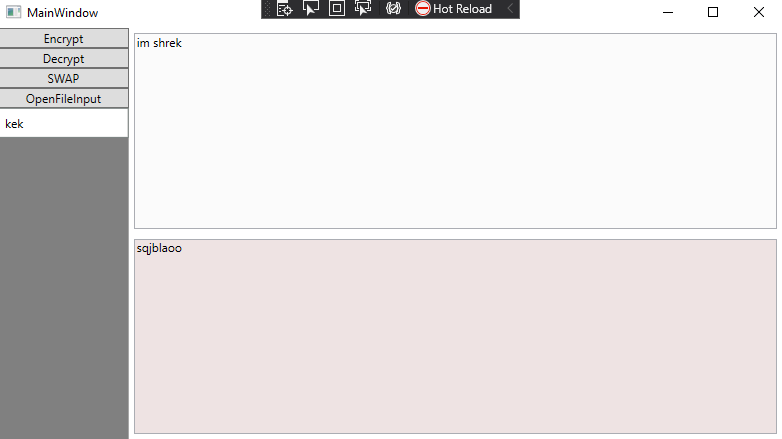


Рисунок 3 — Пример работы алгоритма шифрования

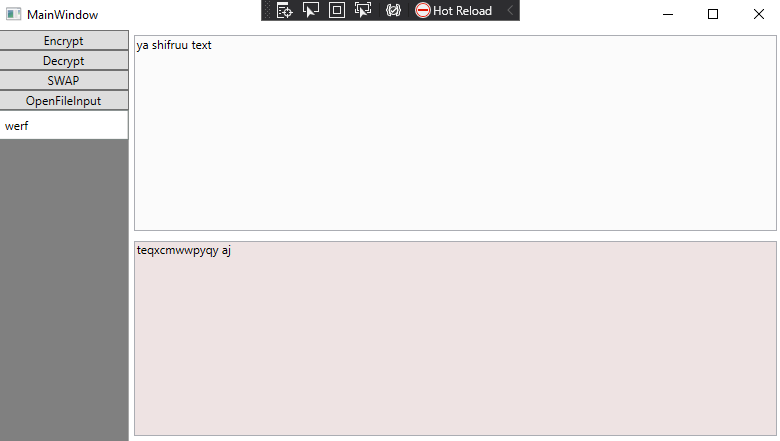


Рисунок 4 — Пример работы алгоритма шифрования

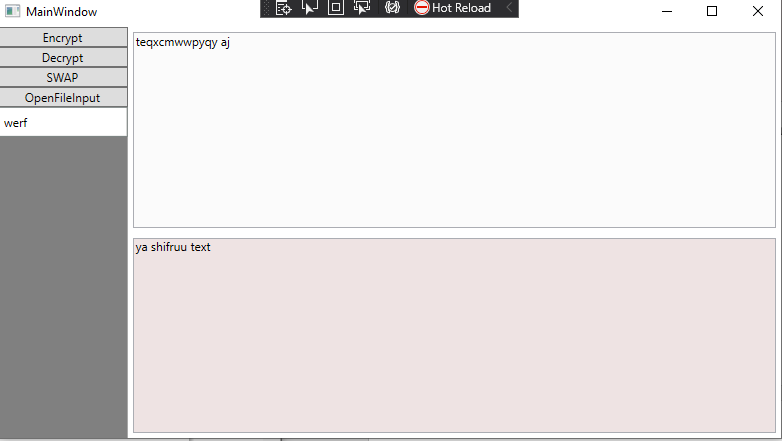


Рисунок 5 — Пример работы алгоритма дешифрования

### Усовершенствованные алгоритмы шифрования и дешифрования

Шифр Вижинера был усовершенствован путем добавления постоянно инкрементирующегося сдвига к ключу. Те самым наш ключ стал изменяться с каждой итерацией на 1. Таким образом для взлом шифра Вижинера уже недостаточно найти ключ, нужно еще понять, что ключ постоянно изменяется, а также понять насколько изменяется ключ, что естественно повысит затраты на взлом шифра.

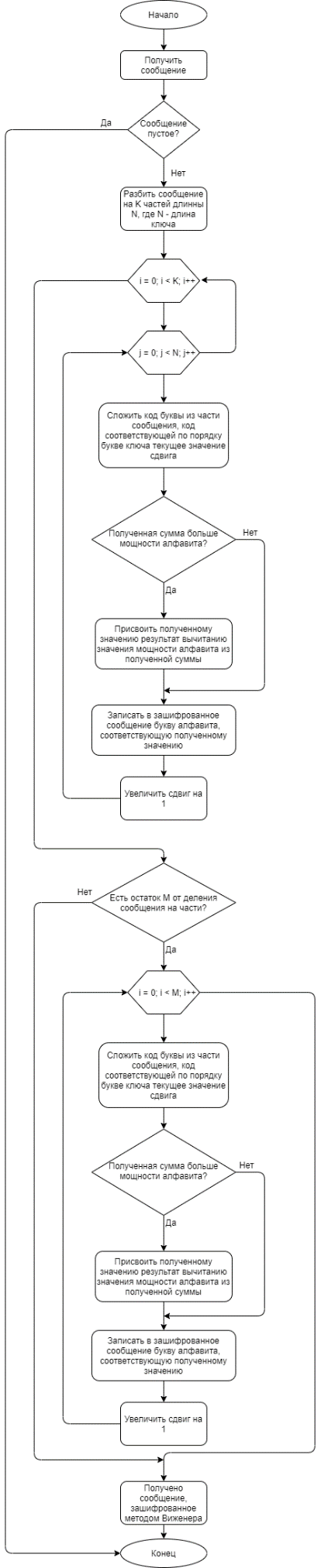


Рисунок 6 – блок-схема усовершенствованного алгоритма шифрования

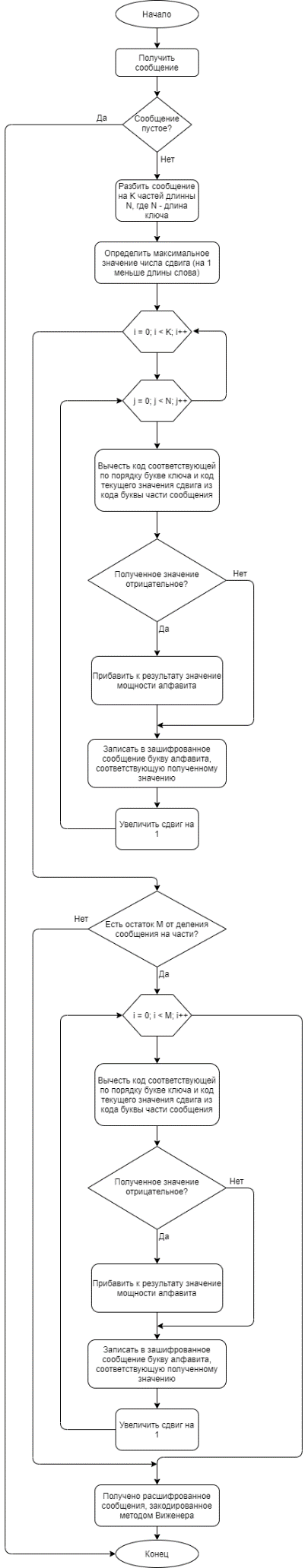


Рисунок 7 – блок-схема усовершенствованного алгоритма дешифрования

Листинг 3 – усовершенствованный алгоритм шифрования

// усовершенствованный алгоритм шифрования

public override void EncryptImprove()

{

\_words = new string(InputString);

string result = "";

// шифрование

try

{

if (!string.IsNullOrEmpty(Key))

{

int shift = 0;

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

{

var index = \_alphabetEn.IndexOf(\_words[i]) + \_alphabetEn.IndexOf(Key[i % Key.Length]);

index += shift; // делаем сдвиг по индексу

index %= \_alphabetEn.Length;

result += \_alphabetEn[index];

shift++;

}

}

OutputString = result;

}

catch (IndexOutOfRangeException exception)

{

OutputString = "Ошибка шифрования";

}

}

Листинг 4 – усовершенствованный алгоритм дешифрования

public override void DecryptImprove()

{

\_words = new string(InputString);

string result = "";

try

{

// дешифрование

if (!string.IsNullOrEmpty(Key))

{

int shift = 0;

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

{

var index = \_alphabetEn.IndexOf(\_words[i]) - \_alphabetEn.IndexOf(Key[i % Key.Length]);

index -= shift;

index %= \_alphabetEn.Length;

result += \_alphabetEn[index];

shift++;

}

}

OutputString = result;

}

catch (IndexOutOfRangeException exception)

{

OutputString = "Ошибка шифрования";

}

}

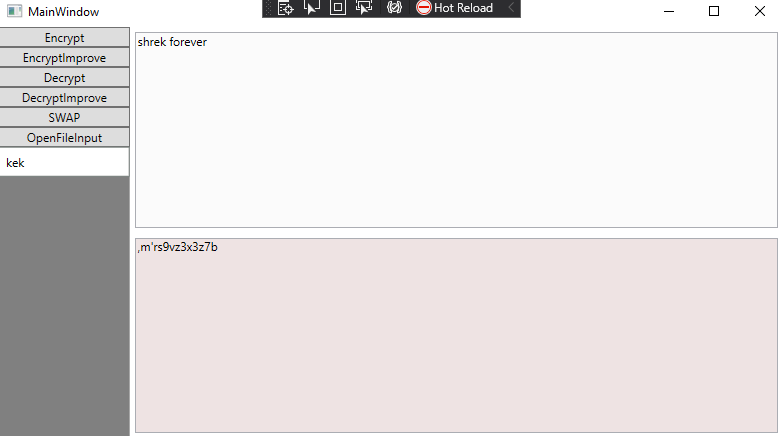


Рисунок 8 — Пример работы усовершенствованного алгоритма шифрования

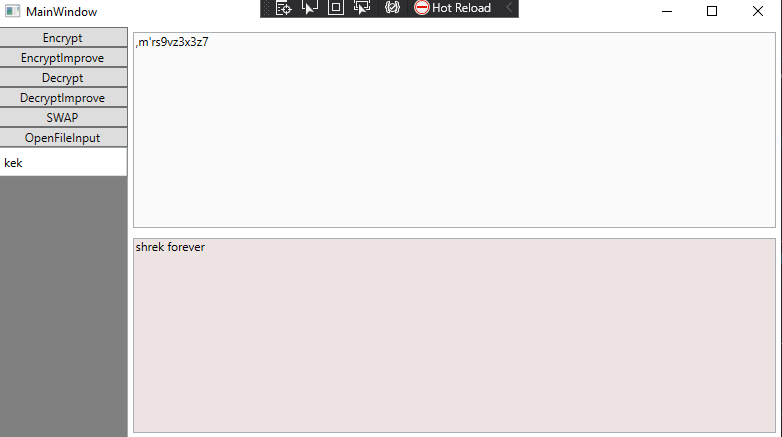


Рисунок 9 – Пример работы усовершенствованного алгоритма дешифрования

# ЗАКЛЮЧЕНИЕ

В ходе выполнения практического задания, мною были получены навыки работы с симметричными шифрами, а также написанию программы для шифрования и дешифрования текста.

# СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

1. СТО – 4.2-07-2014 Система менеджмента качества. Общие требования к построению, изложению и оформлению документов учебной деятельности. – Введ. 30.12.2013г. №1520 – Красноярск : ИПК СФУ, 2013. – 60 с.