Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение

высшего профессионального образования

«Владимирский государственный университет

имени Александра Григорьевича и Николая Григорьевича Столетовых»

(ВлГУ)

Кафедра информационных систем и программной инженерии

Лабораторная работа №4

по дисциплине "Администрирование и безопасность информационных систем"

ТЕМА РАБОТЫ:

Алгоритм Виженера

Выполнил:

студент гр. ПРИ-120

Парахин К.В.

Принял:

Доцент кафедры ИСПИ

Курочкин С.В.

Владимир 2023 г.

Цель работы:

Реализовать криптографический алгоритм шифрования с использованием открытого текста в качестве ключа по таблице Виженера:

Выполнение работы:

Индивидуальный вариант № 9.

1. Зашифровать последовательность с помощью алгоритма Виженера:

«Ей рано нравились романы Они ей заменяли все Она влюблялася в обманы И Ричардсона и Руссо»

Для шифрования используйте ключ «идеал»:

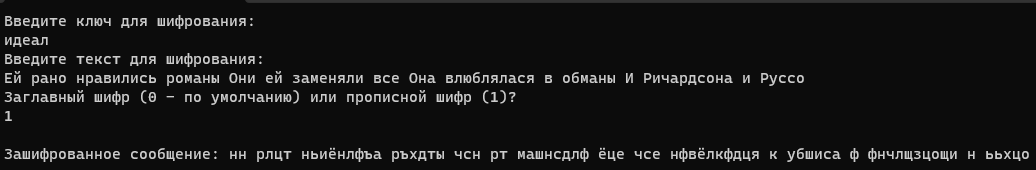
****

Рисунок 1. Шифрование сообщения с помощью алгоритма Виженера

**Результат шифрования:**

Зашифрованное сообщение: нн рлцт ньиёнлфъа ръхдты чсн рт машнсдлф ёце чсе нфвёлкфдця к убшиса ф фнчлщзцощи н ььхцо

1. Расшифровать (дешифровать) последовательность с помощью алгоритма Виженера:

«Фу эъцё сйу дюсягм ьръгм С аяцшффжмм схщм зпаэпдпьйс Ню т щхитрд хе сщтзл сбула».

Для дешифрования используйте ключ «проза»;

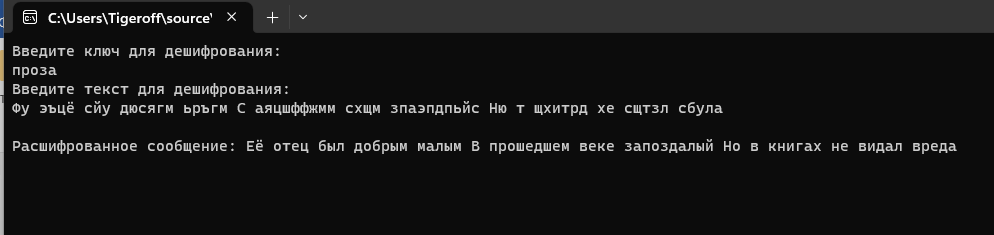


Рисунок 2. Дешифрование сообщения с помощью алгоритма Виженера

**Результат дешифрования:**

Расшифрованное сообщение: Её отец был добрым малым В прошедшем веке запоздалый Но в книгах не видал вреда

1. Написать алгоритм и программу для шифрования/дешифрования строк алгоритмом Виженера.

Вариант m = mynumber – 2 = **9** – 2 = 7, key = кирилл

m = 7, key = парахин (длина равна m)

Листинг программы на языке C#:

public class Program

{

public static void Main(string[] args)

{

Console.WriteLine("Введите ключ для шифрования: ");

var key = Console.ReadLine();

Console.WriteLine("Введите текст для шифрования:");

var text = Console.ReadLine();

Console.WriteLine("Заглавный шифр (0 - по умолчанию) или прописной шифр? ");

var letter = Console.ReadLine();

var isUpperCase = letter switch

{

"1" => false,

\_ => true

};

if (isUpperCase)

{

text = text.ToUpper();

key = key.ToUpper();

}

else

{

text = text.ToLower();

key = key.ToLower();

}

var myCrypter = new VigenerCrypter(isUpperCase);

var encryptedText = myCrypter.Encrypt(text, key);

Console.WriteLine();

Console.WriteLine($"Зашифрованное сообщение: {encryptedText} \n");

Console.WriteLine($"Расшифрованное сообщение: {myCrypter.Decrypt(encryptedText, key)}");

Console.ReadLine();

}

}

public class Crypter

{

private const string upperCaseAlphabet = "АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ";

private readonly List<char> alphabet;

public Crypter(bool isUpperCase = true)

{

alphabet = isUpperCase

? upperCaseAlphabet.ToList()

: upperCaseAlphabet.ToLower().ToList();

}

private string ProcessCrypting(string message, string key, bool flag = true)

{

var temp = new StringBuilder(key);

while (temp.Length < message.Length)

{

temp.Append(temp);

}

var subString = temp.ToString().Substring(0, message.Length);

var outputMessage = new StringBuilder("");

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

{

var messageIndex = alphabet.IndexOf(message[i]);

var keyIndex = alphabet.IndexOf(subString[i]);

var cryptOdd = flag

? keyIndex

: -keyIndex;

var targetIndex = (alphabet.Count + messageIndex + cryptOdd) % alphabet.Count;

\_ = messageIndex < 0

? outputMessage.Append(message[i])

: outputMessage.Append(alphabet[targetIndex]);

}

return outputMessage.ToString();

}

public string Encrypt(string plainMessage, string password)

=> ProcessCrypting(plainMessage, password, true);

public string Decrypt(string encryptedMessage, string password)

=> ProcessCrypting(encryptedMessage, password, false);

}

Результат шифрования первой части сообщения (первого абзаца):

Не мысля гордый свет забавить, Вниманье дружбы возлюбя, Хотел бы я тебе представить Залог достойнее тебя, Достойнее души прекрасной, Святой исполненной мечты, Поэзии живой и ясной, Высоких дум и простоты; Но так и быть - рукой пристрастной Прими собранье пестрых глав, Полусмешных, полупечальных, Простонародных, идеальных, Небрежный плод моих забав, Бессонниц, легких вдохновений, Незрелых и увядших лет, Ума холодных наблюдений И сердца горестных замет

Зашифрованное сообщение: ЭЕ МРЪЩО УОЁМИЩ ВВЪЫ ЧАСАЧСАЛ, ВГСЪПНМЕ МЮГЖСЫ КЬЧЛОБФ, ЕОГЕБ ОК П ЗНОФ АРЪМЯВАТИЗЕ ЧАЬОШ СЮСГОЯЦТФ ГЕЦЗ, ДЯСЗЧЧЭЕХ ЩЬЁШ АРЪУЮПСЮОЯ, БВПТДТ ШСАОБЦТЭНЯЙ ХТЖТЛ, ШЬМЗЩИ ПЦСОЪ Ю МБНЯЙ, ПКСЯКЮЮ УУЭ Ю ЭАОВТДЫИ; ЮО ЫНЪ Щ ЦДАЛ - ЁЬШЮЙ ПЁСЯВРРСЗЦЬЩ АРЮХЦ СЯБЁИЫЛЕ ПЪЪААЫЁ ШФНС, ПДФББМХШГДГ, АОБЬЭФЧРЛСЦИЕ, ПЁЧЯВОЮАЁЧСЭЫЁ, ССФАЬЬГДГ, ЮЕЦЩТЦНЛЙ ШЩЮД МДСГ ЗРБХК, БХСЖЧЫЭИЖ, ФТТКЩХ КСЮХЮОЧНЫШЙ, ГНХАЕЬЫК Ц УТЯЩБЦЕ ЬЕЗ, ГМР КЧЩЮДЮЫК ЫПБЬЮЩНЫШЙ И ЪТАДЖА ЛЬАЕВТГДГ ЗРМЪЫ

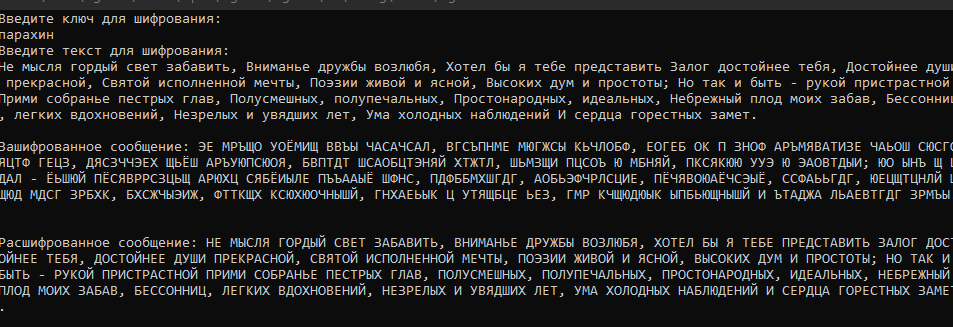


Рисунок 5. Шифрование/дешифрование первого абзаца текста

Мой дядя самых честных правил, Когда не в шутку занемог, Он уважать себя заставил И лучше выдумать не мог. Его пример другим наука; Но, боже мой, какая скука С больным сидеть и день и ночь, Не отходя ни шагу прочь! Какое низкое коварство Полуживого забавлять, Ему подушки поправлять, Печально подносить лекарство, Вздыхать и думать про себя: Когда же черт возьмет тебя

Зашифрованное сообщение: ЬОЪ ЩЗСО ВАВДГ ЧХСЗЦИЕ АРХКЦЫ, КДЛСП ЮЕ К ЗУГКИ ХПНХМДЛ, ОЮ ИКНЦАГЬ ЪТРЯ ЗХЪАПВЩЛ С ЫУЗШЪ ПКДДМХЫЙ НХ ВЧР. ХГД ЭАИЭЕЁ САУУИВ ЫПУЫА; ЫЮ, БДПТ МЯЙ, ШПКРЯ ЪШГКР Ж ОЮЛМНРХ БИФЕЗЕ Ш ФЕГЕ Ш ЮОМЕ, НХ ДЫГЮДП ГС ЗАУУ ШЮЮЧМ! УНЪОХ ГСХЪОХ АЧППРВТЧЧ ЯОЬУЬСПЮГЯ ЭИОПВЬЯЗЕ, ЕЭУ ШЬУУИКЮ ЭЮПБАЧФМВЬ, ЕНЕПЛМНД ЭЮДЮОЖСАЛ ЬЕАИЮБТТО, ПЧДЛХХЫЙ И ДИХНВЬ ПЁЧ БЕСЯ: ШЮГФА ПТ ЧХРЗ ПЮЗММЪЫ ВЕСЯ

Результат шифрования второй части сообщения (второго абзаца):

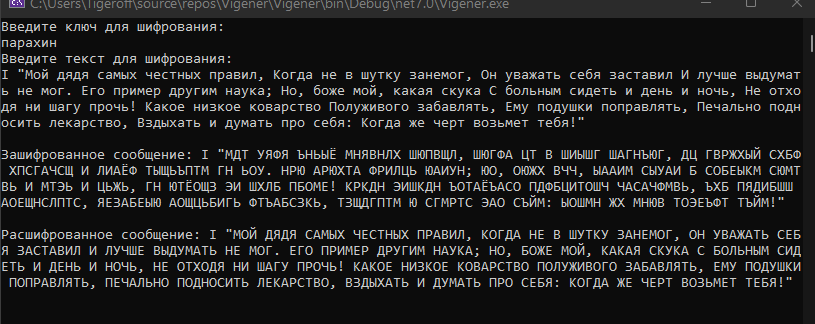


Рисунок 6. Шифрование/дешифрование второго абзаца текста

Вывод

В результате выполнения работы я научился проводить шифрование/дешифрование сообщения алгоритом Виженера как в ручном режиме, так и с помощью программного алгоритма.