Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерных систем и сетей

Кафедра информатики

Дисциплина: Информационные сети. Основы безопасности

**ОТЧЕТ**

к лабораторной работе № 1

на тему «Шифр Цезаря»

Выполнил:

студент гр. 153503

Киселева Е.А.

Проверил:

Лещенко Е.А.

Минск 2023

СОДЕРЖАНИЕ

[1 Постановка задачи 3](file:///C:\Users\Acer\Downloads\Report1.docx#_Toc157353562)

[2 Краткие теоретические сведения 4](file:///C:\Users\Acer\Downloads\Report1.docx#_Toc157353563)

[2.1 Шифр Цезаря 4](file:///C:\Users\Acer\Downloads\Report1.docx#_Toc157353564)

[2.2 Шифр Виженера 5](file:///C:\Users\Acer\Downloads\Report1.docx#_Toc157353565)

[3 Результаты выполнения лабораторной работы 7](file:///C:\Users\Acer\Downloads\Report1.docx#_Toc157353566)

[3.1 Шифрование (дешифрование) текста при помощи шифра Цезаря 7](file:///C:\Users\Acer\Downloads\Report1.docx#_Toc157353567)

[3.2 Шифрование (дешифрование) текста при помощи шифра Виженера 7](file:///C:\Users\Acer\Downloads\Report1.docx#_Toc157353568)

[Выводы 9](file:///C:\Users\Acer\Downloads\Report1.docx#_Toc157353569)

Приложение А [(обязательное) Листинг исходного кода 10](file:///C:\Users\Acer\Downloads\Report1.docx#_Toc157353570)

Приложение Б [(обязательное) Блок схема алгоритма, реализуюшего   
                           шифр Цезаря 13](file:///C:\Users\Acer\Downloads\Report1.docx#_Toc157353573)

Приложение В (обязательное) [Блок схема алгоритма, реализующего   
                           шифр Виженера 14](file:///C:\Users\Acer\Downloads\Report1.docx#_Toc157353577)

## 1 ПОСТАНОВКА ЗАДАЧИ

Целью выполнения лабораторной работы является изучения теоретических сведений о шифре Цезаря и шифре Виженера, а также создание программ, читающих данные из файла и шифрующие (дешифрующие) их с помощью шифра Цезаря и шифра Виженера.

## 2 КРАТКИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

## 2.1 Шифр Цезаря

Шифр Цезаря, также известный, как шифр сдвига, код Цезаря или сдвиг Цезаря – один из самых простых и наиболее широко известных методов шифрования.

Шифр Цезаря – это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется символом, находящимся на некотором постоянном числе позиций левее или правее него в алфавите. Например, в шифре со сдвигом 4 «А» была бы заменена на «Г», «Б» станет «Д», и так далее.

Шифр назван в честь римского императора Гая Юлия Цезаря, использовавшего его для секретной переписки со своими генералами.

Шаг шифрования, выполняемый шифром Цезаря, часто включается как часть более сложных схем, таких как шифр Виженера, и все ещё имеет современное приложение в системе ROT13. Как и все моноалфавитные шифры, шифр Цезаря легко взламывается и не имеет практически никакого применения на практике.



Рисунок 1 – Шифр Цезаря

Если сопоставить каждому символу алфавита его порядковый номер (нумеруя с 0), то шифрование и дешифрование можно выразить формулами модульной арифметики:

y=(x+k)\ \mod\ n

x=(y-k+n)\ \mod\ n,

где ~x – символ открытого текста, ~y – символ шифрованного текста, ~n – мощность алфавита, а ~k – ключ.

С точки зрения математики шифр Цезаря является частным случаем аффинного шифра.

## 2.2 Шифр Виженера

Шифр Виженера состоит из последовательности нескольких шифров Цезаря с различными значениями сдвига. Для зашифровывания может использоваться таблица алфавитов, называемая tabula recta или квадрат (таблица) Виженера. Применительно к латинскому алфавиту таблица Виженера составляется из строк по 26 символов, причём каждая следующая строка сдвигается на несколько позиций. Таким образом, в таблице получается 26 различных шифров Цезаря. На каждом этапе шифрования используются различные алфавиты, выбираемые в зависимости от символа ключевого слова. Например, предположим, что исходный текст имеет такой вид:

ATTACKATDAWN

Человек, посылающий сообщение, записывает ключевое слово («LEMON») циклически до тех пор, пока его длина не будет соответствовать длине исходного текста:

LEMONLEMONLE

Первый символ исходного текста A зашифрован последовательностью L, которая является первым символом ключа. Первый символ L шифрованного текста находится на пересечении строки L и столбца A в таблице Виженера. Точно так же для второго символа исходного текста используется второй символ ключа; то есть второй символ шифрованного текста X получается на пересечении строки E и столбца T. Остальная часть исходного текста шифруется подобным способом:

1 Исходный текст:  ATTACKATDAWN

2 Ключ:  LEMONLEMONLE

3 Зашифрованный текст: LXFOPVEFRNHR

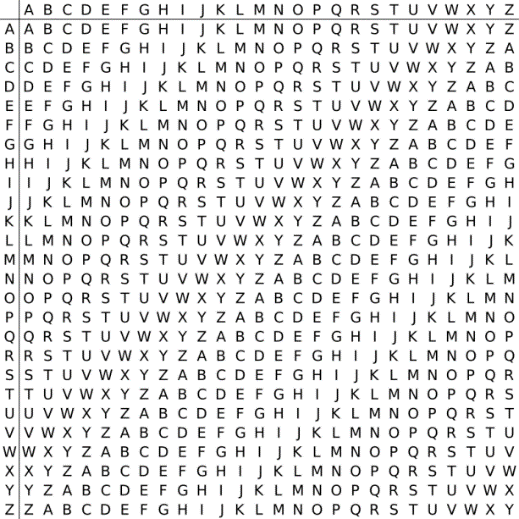


Рисунок 2 – Квадрат Виженера

Расшифровывание производится следующим образом: находим в таблице Виженера строку, соответствующую первому символу ключевого слова; в данной строке находим первый символ зашифрованного текста. Столбец, в котором находится данный символ, соответствует первому символу исходного текста. Следующие символы зашифрованного текста расшифровываются подобным образом.c j = m j + k j ( mod n )

m j = c j − k j ( mod n )

В компьютере такая операция соответствует сложению кодов ASCII символов сообщения и ключа по некоторому модулю. Кажется, что если таблица будет более сложной, чем циклическое смещение строк, то шифр станет надежнее. Это действительно так, если ее менять чаще, например, от слова к слову. Но составление таких таблиц, представляющих собой латинские квадраты, где любая буква встречается в строке или столбце один раз, трудоемко и его стоит делать лишь на ЭВМ. Для ручного же многоалфавитного шифра полагаются лишь на длину и сложность ключа, используя приведенную таблицу, которую можно не держать в тайне, а это упрощает шифрование и расшифровывание

## 3 РЕЗУЛЬТАТЫ ВЫПОЛНЕНИЯ ЛАБОРАТОРНОЙ             РАБОТЫ

В ходе выполнения лабораторной работы были реализованы два приложения, которые шифруют текст из файла при помощи шифра Цезаря и шифра Виженера, а после выводят результаты шифровки и дешифровки обратно в файлы. Блок схемы алгоритмов, реализующих шифр Цезаря и шифр Виженера, представлены в приложения Б и В соответственно.

## 3.1 Шифрование (дешифрование) текста при помощи шифра Цезаря

При запуске программы пользователю предоставляется возможность ввести числовой ключ, по которому будет происходить сдвиг. Ключ может быть как положительным, так и отрицательным. При положительном ключе сдвиг будет происходить вправо на указанное число позиций. При отрицательном ключе сдвиг будет происходить влево. При ключе, равном нулю, сдвига не будет происходить. Результат работы программы предоставлен на рисунке 3.1.

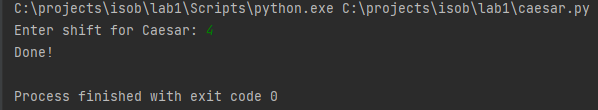


Рисунок 3.1 – Результат работы программы, реализующей шифр Цезаря

## 3.2 Шифрование (дешифрование) текста при помощи шифра                 Виженера

При запуске программы пользователю предоставляется возможность ввести ключ, который является словом или набором символов. Результат работы программы представлен на рисунке 3.2.

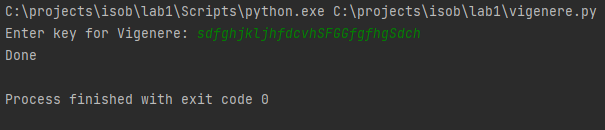


Рисунок 3.2 – Результат работы программы, реализующей шифр Виженера

## ВЫВОДЫ

В ходе выполнения лабораторной работы были изучены теоретические сведения о шифре Цезаря и шифре Виженера, а также были созданы программы, читающие данные из файла и шифрующие (дешифрующие) их с помощью шифры Цезаря и шифра Виженера, а также предоставляющие результат в выходные файлы.

**ПРИЛОЖЕНИЕ А**

## (обязательное)

## Листинг кода

Листинг 1 – Программный код алгоритма шифра Цезаря

def caesar\_cipher\_encrypt(text, shift):

encrypted\_text = ''

for char in text:

if char.isalpha():

shifted = ord(char) + (shift % 26)

if char.islower():

if shifted > ord('z'):

shifted -= 26

elif shifted < ord('a'):

shifted += 26

elif char.isupper():

if shifted > ord('Z'):

shifted -= 26

elif shifted < ord('A'):

shifted += 26

encrypted\_text += chr(shifted)

else:

encrypted\_text += char

return encrypted\_text

def caesar\_cipher\_decrypt(encrypted\_text, shift):

return caesar\_cipher\_encrypt(encrypted\_text, -shift)

def encrypt\_file\_caesar(input\_file, output\_file, shift):

with open(input\_file, 'r') as file:

text = file.read()

encrypted\_text = caesar\_cipher\_encrypt(text, shift)

with open(output\_file, 'w') as file:

file.write(encrypted\_text)

def decrypt\_file\_caesar(input\_file, output\_file, shift):

with open(input\_file, 'r') as file:

encrypted\_text = file.read()

decrypted\_text = caesar\_cipher\_decrypt(encrypted\_text, shift)

with open(output\_file, 'w') as file:

file.write(decrypted\_text)

input\_file = 'files/input.txt'

output\_file = 'files/encrypted\_caesar.txt'

while True:

shift = input("Enter shift for Caesar: ")

try:

shift=int(shift)

break

except ValueError:

print("Error: enter correct number")

encrypt\_file\_caesar(input\_file, output\_file, shift)

decrypt\_file\_caesar(output\_file, 'files/decrypted\_caesar.txt', shift)

print("Done!")

Листинг 2 – Программный код алгоритма шифра Виженера

def vigenere\_cipher\_encrypt(plain\_text, key):

encrypted\_text = ''

key\_length = len(key)

for i, char in enumerate(plain\_text):

if char.isalpha():

key\_shift = ord(key[i % key\_length].lower()) - ord('a')

if char.islower():

shifted = (ord(char) - ord('a') + key\_shift) % 26 + ord('a')

elif char.isupper():

shifted = (ord(char) - ord('A') + key\_shift) % 26 + ord('A')

encrypted\_text += chr(shifted)

else:

encrypted\_text += char

return encrypted\_text

def vigenere\_cipher\_decrypt(encrypted\_text, key):

decrypted\_text = ''

key\_length = len(key)

for i, char in enumerate(encrypted\_text):

if char.isalpha():

key\_shift = ord(key[i % key\_length].lower()) - ord('a')

if char.islower():

shifted = (ord(char) - ord('a') - key\_shift) % 26 + ord('a')

elif char.isupper():

shifted = (ord(char) - ord('A') - key\_shift) % 26 + ord('A')

decrypted\_text += chr(shifted)

else:

decrypted\_text += char

return decrypted\_text

def encrypt\_file\_vigenere(input\_file, output\_file, key):

with open(input\_file, 'r') as file:

text = file.read()

encrypted\_text = vigenere\_cipher\_encrypt(text, key)

with open(output\_file, 'w') as file:

file.write(encrypted\_text)

def decrypt\_file\_vigenere(input\_file, output\_file, key):

with open(input\_file, 'r') as file:

encrypted\_text = file.read()

decrypted\_text = vigenere\_cipher\_decrypt(encrypted\_text, key)

with open(output\_file, 'w') as file:

file.write(decrypted\_text)

input\_file = 'files/input.txt'

output\_file = 'files/encrypted\_vigenere.txt'

key = input("Enter key for Vigenere: ")

encrypt\_file\_vigenere(input\_file, output\_file, key)

decrypt\_file\_vigenere(output\_file, 'files/decrypted\_vigenere.txt', key)

print("Done")

## ПРИЛОЖЕНИЕ Б

## (обязательное)

## Блок схема алгоритма, реализующего шифр Цезаря



## ПРИЛОЖЕНИЕ В

## (обязательное)

## Блок схема алгоритма, реализующего шифр Виженера

