Учреждение образования

Белорусский государственный университет

информатики и радиоэлектроники

Лабораторная работа №1 по дисциплине

«Информационные сети. Основы безопасности»

Выполнил: Проверил:

студент группы 753502 Протько М.И.

Клишевич И.Д.

Минск 2020

**Введение**

В данной лабораторной работе необходимо реализовать программные средства шифрования и дешифрования текстовых файлов при помощи Шифра Цезаря, (шифра сдвига, кода Цезаря) и шифра Виженера.

**1. Шифр Цезаря**

**Шифр Цезаря** – один из наиболее простых и широко известных алгоритмов шифрования текстовых данных. Этот метод назван в честь римского полководца Гая Юлия Цезаря, который применял шифр для личной переписки с подчиненными.

Алгоритм шифрования Цезаря заключается в замене каждого символа входящего сообщения на символ, который находится на некотором константном расстоянии с правой или левой стороны. Расстояние при этом называют – ключом.



Рис.1(шифр Цезаря)

Например для ключа 5 получаем последовательность:

* Русский алфавит:
  + *А Б В Г Д Е Ё Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я*
* Шифр:
  + *Е Ё Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я А Б В Г Д*

То есть *А* заменяем на *Е*, *Б* на *Ё*, и т. д.

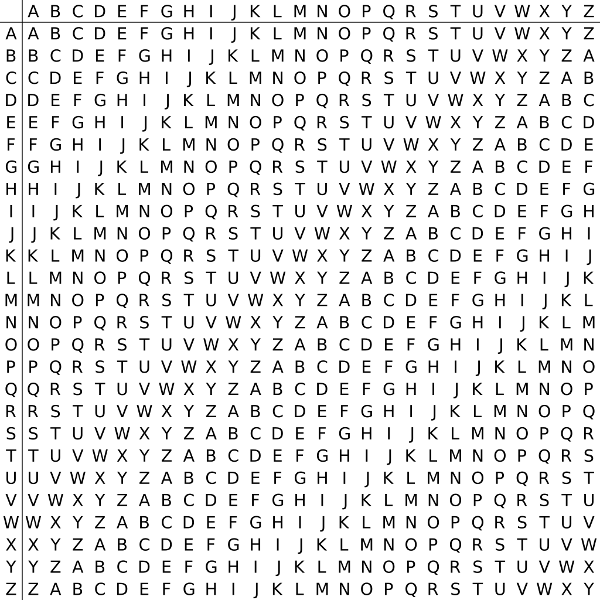
Математически шифр Цезаря можно описать следующими формулами:

* *Encrypt(mn) = (Q + mn + k) % Q*;
* *Decrypt(cn) = (Q + cn - k) % Q*.

где *m* - открытый текст, *k* - ключ шифрования, *Q* - количество символов в алфавите, *c* - зашифрованный текст.

**2. Шифр Виженера**

**Шифр Виженера** – алгоритм шифрования текстовых данных с помощью ключевого слова.Шифрование Виженера можно представить как несколько шифров Цезаря с различными ключами. Проще всего шифры представить в виде таблицы, для английского алфавита мы получим 26 строк шифра Цезаря, в каждой строке сдвиг на единицу больше предыдущей:



Математически шифр Виженера можно описать следующими формулами:

* *Encrypt(mn) = (Q + mn + kn) % Q*;
* *Decrypt(cn) = (Q + cn - kn) % Q*.

где *mn* - позиция символа открытого текста, *kn* - позиция символа ключа шифрования, *Q* - количество символов в алфавите, *cn* - позиция символа зашифрованного текста.

**Блок-схема**

**1. Шифр Цезаря**

**Program.cs:**

Ввод(myKey)

Вывод(text)

Var task = new CoderAndDecoder

Var codText = task.Cod(text,myKey)

Var decText = task.Decode(codText,myKey)

Вывод(codText, decText)

CoderAndDecoder.cs:

alphabet, fullAlphabet,

fullAlphabetLenght, result

Symbol, index

result += symbol.ToString()

Index < 0

Да

Нет

codeIndex

codeIndex < 0

Да

Нет

codeIndex += fullAlphabetLenght

result += fullAlphabet[codeIndex]

**2.** **Шифр Виженера**

Main.cs:

Ввод(key)

Вывод(text)

var task = new Vigener();

var codText = task.Cod(text, key);var decText = task.Dec(codText, key);

Вывод(codText, decText)

Vigener.cs:

keyWord, result,

all

textIndex,

keyIndex

result += text[i].ToString();

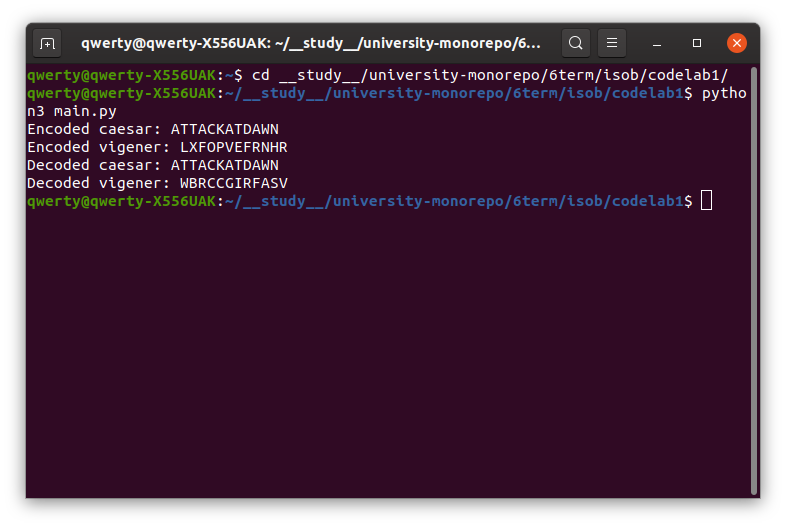
textIndex < 0

Да

Нет

result += alpphbaet[(all + textIndex + ((flag ? 1 : -1) \* keyIndex)) % all].ToString();

**Демонстрация работы программы**



**Программный код**

main.py:

from caesar import Caesar  
from vigener import Vigener  
  
if \_\_name\_\_ == "\_\_main\_\_":  
 text = "ATTACKATDAWN"  
 key\_caesar = 3  
 key\_vigener = "LEMON"  
 encoded\_caesar = Caesar.code(text, key\_caesar)  
 encoded\_vigener = Vigener.code(text, key\_vigener)  
 print("Encoded caesar:", encoded\_caesar)  
 print("Encoded vigener:", encoded\_vigener)  
 print("Decoded caesar:", Caesar.code(encoded\_caesar, key\_caesar))  
 print("Decoded vigener:", Vigener.code(encoded\_vigener, key\_vigener))

caesar.py:

class Caesar:  
 @staticmethod  
 def code\_and\_dec(text, key):  
 alphabet = "АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ"  
 result = ""  
 for char in text:  
 index = alphabet.find(char.upper())  
 if index < 0:  
 result += char  
 else:  
 code\_index = (index + key) % len(alphabet)  
 if code\_index < 0:  
 code\_index += len(alphabet)  
 if char.islower():  
 result += result[code\_index].lower()  
 else:  
 result += alphabet[code\_index]  
 return result  
  
 @staticmethod  
 def code(text, key):  
 return Caesar.code\_and\_dec(text, key)  
  
 @staticmethod  
 def decode(text, key):  
 return Caesar.code\_and\_dec(text, -key)

vigener.py:

class Vigener:  
 @staticmethod  
 def get\_key(text, length):  
 temp = text  
 while len(temp) < length:  
 temp += text  
 return temp[:length]  
  
 @staticmethod  
 def code\_and\_dec(text, key, flag):  
 alphabet = "ABCDEFGHIJKLMNOPQRSTUVWXYZ"  
 password = Vigener.get\_key(key, len(text))  
 result = ""  
 q = len(alphabet)  
  
 index = 0  
  
 for char in text:  
 text\_index = alphabet.find(char.upper())  
 key\_index = alphabet.find(password[index].upper())  
 if text\_index < 0:  
 result += char  
 else:  
 result += alphabet[(q + text\_index + flag \* key\_index) % q]  
 index += 1  
 return result  
  
 @staticmethod  
 def code(text, key):  
 return Vigener.code\_and\_dec(text, key, 1)  
  
 @staticmethod  
 def decode(text, key):  
 return Vigener.code\_and\_dec(text, key, -1)

**Вывод**

В ходе данной лабораторной работы я научился шифровать и дешифровывать данные при помощи шифра Цезаря и шифра Виженера. На мой взгляд, оба шифра очень примитивны и не пригодны для использования в повседневной жизни, т.к. могут быть легко дешифрованы.