Министерство образования Республики Беларусь

Учреждение образования

Белорусский государственный университет

информатики и радиоэлектроники

Кафедра информатики

Лабораторная работа №1 по дисциплине

«Информационные сети. Основы безопасности»

Выполнил: Проверил:

студент группы 753502 Протько М.И.

Горбачев Д.А.

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.

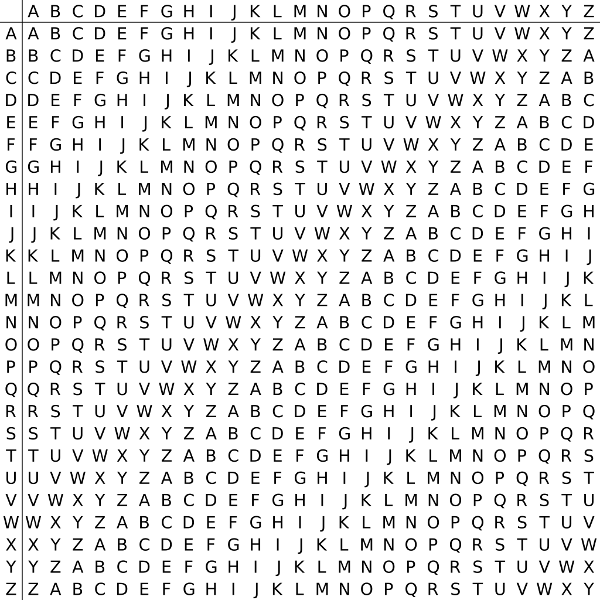
Математически шифр Цезаря можно описать следующими формулами:

* *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:

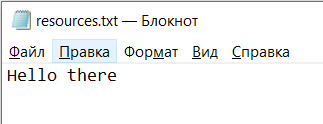
* *Encrypt(mn) = (Q + mn + kn) % Q*;
* *Decrypt(cn) = (Q + cn - kn) % Q*.

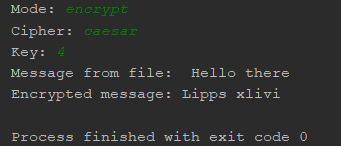
где *mn* - позиция символа открытого текста, *kn* - позиция символа ключа шифрования, *Q* - количество символов в алфавите, *cn* - позиция символа зашифрованного текста.

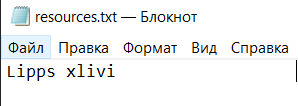
**Демонстрация работы программы**

**1.Шифр Цезаря**

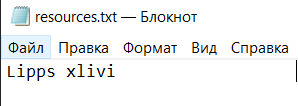
- шифрование:

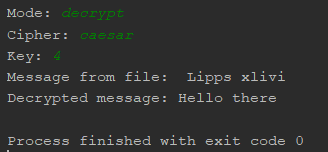


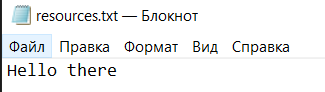




-расшифрование:

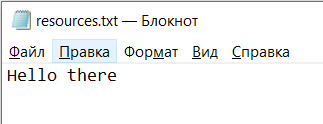


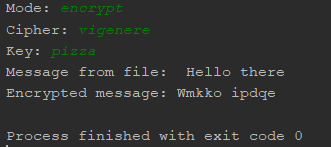


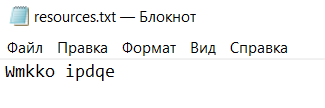
****

**2. Шифр Виженера**

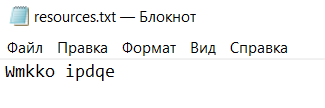
- шифрование:

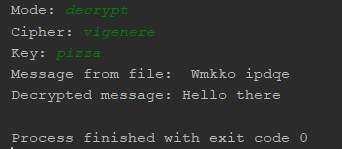
****

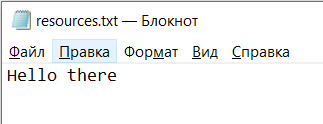




- расшифрование:







**Программный код**

LETTERS = 'ABCDEFGHIJKLMNOPQRSTUVWXYZ'  
  
def main():  
 file = open("resources.txt")  
 message = file.read()  
 mode = input("Mode: ")  
 cipher = input("Cipher: ")  
 key = input("Key: ")  
 print("Message from file: ", message)  
 if cipher == 'vigenere':  
 translated = VigenereCipher(key, message, mode)  
 else:  
 translated = CaesarCipher(key, message, mode)  
  
  
 print('%sed message:' % (mode.title()),end=" ")  
 print(translated)  
 file.close()  
 file = open("resources.txt","w")  
 file.write(translated)  
 file.close()  
  
def CaesarCipher(key, message, mode):  
 result = []  
 key = int(key)  
 if mode == "decrypt":  
 key = key \* -1;  
  
 for symbol in message:  
 if LETTERS.find(symbol.upper()) != -1:  
 if symbol.isupper():  
 result.append(LETTERS[(LETTERS.index(symbol) + key) % len(LETTERS)])  
 else:  
 result.append(LETTERS[(LETTERS.index(symbol.upper()) + key) % len(LETTERS)].lower())  
 else:  
 result.append(symbol)  
  
 return "".join(result)  
  
def VigenereCipher(key, message, mode):  
 result = []  
  
 keyIndex = 0  
 key = key.upper()  
  
 for symbol in message:  
 num = LETTERS.find(symbol.upper())  
 if num != -1:  
 if mode == 'encrypt':  
 num += LETTERS.find(key[keyIndex])  
 elif mode == 'decrypt':  
 num -= LETTERS.find(key[keyIndex])  
  
 num %= len(LETTERS)  
  
 if symbol.isupper():  
 result.append(LETTERS[num])  
 elif symbol.islower():  
 result.append(LETTERS[num].lower())  
  
 keyIndex += 1  
 if keyIndex == len(key):  
 keyIndex = 0  
 else:  
 result.append(symbol)  
  
 return ''.join(result)  
  
if \_\_name\_\_ == '\_\_main\_\_':  
 main()

**Вывод**

В ходе данной лабораторной работы я познакомился с шифрованием и дешифровыванием данных при помощи шифра Цезаря и шифра Виженера. Повторил работу с файлами и строками на языке Python.