МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФГБОУ ВО «Уральский государственный экономический университет»

Часовских В.П.

Интеллектуальные технологии и кибербезопасность цифрового предприятья

38.04.05 – бизнес-информатика направленность интеллектуальное управление цифровыми предприятиями»

Лабораторная работа №2
Простое шифрование и дешифрование - шифр Вижинера

Екатеринбург 2023

Лабораторная работа №2

Простое шифрование и дешифрование - шифр Вижинера

Шифр **Виженера** – метод полиалфавитного шифрования буквенного текста с использованием кодового слова. В этом шифре ключом является фраза или слово. Пароль записывался периодически над буквами открытого текста. Буква пароля, стоящая над соответствующей буквой открытого текста, указывала номер строки в таблице, по которой следует проводить замену (шифрование) это буквы.

		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z
	A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z
	B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A
	C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B
	D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C
	E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D
	F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E
	G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F
	H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G
	I	I	J	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H
	J	J	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I
	K	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
	L	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
	M	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
	N	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
	O	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
	P	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
	Q	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
	R	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
	S	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
	T	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
	U	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
	W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
	X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	W
	Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	W	X
	Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y

Рис. 1 Квадрат Виженера (таблица Виженера)

Исходный текст: **ATTACKATDAWN** - буква определяет строку

Ключ: **LEMON**LEMONLE - буква определяет столбец

Зашифрованный текст: **LXFOPVEFRNHR** - буква на пересечение строки и столбца

Шифр Виженера состоит из нескольких шифров Цезаря (в данном шифре каждая буква сдвигается на несколько позиций). Буквам A-Z соответствуют числам 0-25, то шифрование Виженера можно записать в виде формулы:

$$C_i = (P_i + K_i) \mod 26$$

Расшифровка:

$$P_i = (C_i - K_i + 26) \mod 26$$

Закодируем слова 'Hello world' с ключом 'key'. Программа будет следующая:

```
# Создаем множество (словарь)  символов, которые будут участвовать в шифровании

def form_dict():
    d = {}
    iter = 0
    for i in range(0,127):
        d[iter] = chr(i)
        iter = iter +1
    return d

# подготовка шифротекста -  сопоставляем буквы в нашем слове с буквами в словаре и присваиаем
им соответствующие числовые индексы

def encode_val(word):
    list_code = []
    lent = len(word)
    d = form_dict()

    for w in range(lent):
        for value in d:
            if word[w] == d[value]:
               list_code.append(value)
    return list_code

# И так мы закодировали наше слово и ключ и получили 2 списка индексов:
# Value= [72, 101, 108, 108, 111, 32, 119, 111, 114, 108, 100]
# Key =  [107, 101, 121]
```

Далее сопоставляем индексы ключа с индексами нашего слова функцией full_encode():

```
def comparator(value, key):
    len_key = len(key)
    dic = {}
    iter = 0
    full = 0

    for i in value:
        dic[full] = [i,key[iter]]
        full = full + 1
        iter = iter +1
        if (iter >= len_key):
            iter = 0
    return dic

def full_encode(value, key):
    dic = comparator(value, key)
    print ('Compare full encode', dic)
    lis = []
    d = form_dict()

    for v in dic:
        go = (dic[v][0]+dic[v][1]) % len(d)
        lis.append(go)
    return lis

def decode_val(list_in):
    list_code = []
    lent = len(list_in)
    d = form_dict()

    for i in range(lent):
        for value in d:
```

```
            if list_in[i] == value:
                list_code.append(d[value])
    return list_code

# Получаем наш индексы шифра и переводим их в строку функцией decode_val():
# {0: [72, 107], 1: [101, 101], 2: [108, 121], 3: [108, 107], 4: [111, 101], 5: [32, 121], 6:
[119, 107], 7: [111, 101], 8: [114, 121], 9: [108, 107], 10: [100, 101]}
# Индексы: [52, 75, 102, 88, 85, 26, 99, 85, 108, 88, 74]
# Получаем закодированное суперсекретное послание: 4KfXUcUlXJ

# Раскодировать же все это можно с помощью функции full_decode(), первым аргументом которой
есть список числовых индексов шифра, а вторым — список индексов ключа:


def full_decode(value, key):
    dic = comparator(value, key)
    print ('Deshifre=', dic)
    d = form_dict()
    lis =[]

    for v in dic:
        go = (dic[v][0]-dic[v][1]+len(d)) % len(d)
        lis.append(go)
    return lis

# Все так же получаем индексы шифра и переводим их в строку уже знакомой функцией decode_val():
# [72, 101, 108, 108, 111, 32, 119, 111, 114, 108, 100]
# Наше зашифрованное слово: Hello world
#
********************************************************************************************

# Исполнительная часть программы

if __name__ == "__main__":

    word = 'Hello world'
    key = 'key'

    print ('Слово: '+ word)
    print ('Ключ: '+ key)

    key_encoded = encode_val(key)
    value_encoded = encode_val(word)

    print ('Value= ',value_encoded)
    print ('Key= ', key_encoded)

    shifre = full_encode(value_encoded, key_encoded)
    print ('Шифр=', ''.join(decode_val(shifre)))

    decoded = full_decode(shifre, key_encoded)
    print( 'Decode list=', decoded)
    decode_word_list = decode_val(decoded)

    print ('Word=',''.join(decode_word_list))
```

ЗАДАНИЯ РАБОТЫ

1. Создать проект в среде Visual Studio 2019 с использование языка программирования Python.
2. Сформировать необходимое окружения языка Python из библиотек, необходимых для выполнения лабораторной работы.
3. Создать два файла-программы в языке python для шифровки и дешифровки.
4. Сформировать тексты программ, в соответствие с методическими указаниями, для шифровки и дешифровки. Дополнительно к английскому алфавиту добавить алфавит русского языка (кириллица). Программ может быть две, отдельно для английского и отдельно для русского.
5. Подготовить 4 примера – 2 на русском языке и 2 на английском для подготовки шифротекста. Примеры должны содержать правильные тексты (символы алфавита) и ошибочные.
6. Сформировать шифротексты.
7. Выполнить дешифровку шифротекстов.

Оформить отчет по работе с указанием описания алгоритма Вижинера, описания программ шифровки и дешифровки, описание примеров и указания недостатков и достоинств алгоритма Вижинера.