ДНІПРОВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМ. О.ГОНЧАРА

ФАКУЛЬТЕТ ПРИКЛАДНОЇ МАТЕМАТИКИ

КАФЕДРА КОМП’ЮТЕРНИХ ТЕХНОЛОГІЙ

**Лабораторна робота №2**

**з курсу «Захист інформації»**

Виконав:

студент групи ПА-19-2

Овсов Михайло

Дніпро, 2022

Постановка задачі:

Програмно реалізувати 2 найпростіших алгоритмів шифрування.

Хід роботи:

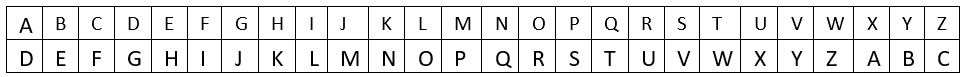
Для виконання лабораторної роботи №2 я обрав шифр Цезаря та шифр Полібія.

Шифр Цезаря:

Шифр Цезаря – найпростіший із шифрів підстановки і є одноалфавітним шифром. Для цих видів шифру замість кожного символу відкритого тексту підставляється символ того ж алфавіту, який залежить від ключа.

В залежності від конкретного шифру ключ обирається по різному. Конкретно для шифру Цезаря ключем k є певне ціле число від 1 до 25. Замість літери незашифрованого тексту підставляється літера, яка стоїть в алфавіті на k позицій праворуч.

Якщо k=3, то латинська літера A заміниться на D, B на E тощо. Таблиця підстановки для даного ключа буде така:



Слово CIPHER зашифрується як C(‘CIPHER’, 3) = ’FLSKHU’.

Для розшифровування достатньо кожну літеру зашифрованого тексту замінити на літеру, яка стоїть на k позицій ліворуч:

D(’FLSKHU’,3) = (‘CIPHER’).

Програмний код:

alphabet = "ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ"

def **cezar\_cipher**(text, size, decipher=False):

    try:

        size = int(size)

        if size < 1 or size > 25:

            raise MyError

    except ValueError:

        return ValueError

    except MyError:

        return MyError

    text = text.upper()

    if decipher:

        size \*= (-1)

    result = ''

    for i in text:

        place = alphabet.**find**(i)

        new\_letter = place + size

        if i in alphabet:

            result += alphabet[new\_letter]

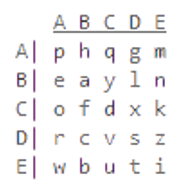
        else:

            result += i

    return result

Шифр Полібія:

Ще один шифр підстановки. Ключем шифру є квадрат розміром 5 \* 5 (для англійської мови), що містить всі літери алфавіту, крім J.



При шифруванні кожна літера вихідного тексту заміщається парою символів, що представляють номер рядка і номер стовпця, в яких розташована буква, яка заміщується. Буква a буде заміщена в шифр тексту парою BB, буква b - парою EB і так далі. Так як ключ не містить букву J, перед шифруванням в початковому тексті J слід замінити на I.

Наприклад, зашифруємо слово HABRAHABR. C ( 'HABRAHABR') = 'AB BB EB DA BB AB BB EB DA'.

Програмний код:

alphabet = {

    'p': 'AA',

    'h': 'AB',

    'q': 'AC',

    'g': 'AD',

    'm': 'AE',

    'e': 'BA',

    'a': 'BB',

    'y': 'BC',

    'l': 'BD',

    'n': 'BE',

    'o': 'CA',

    'f': 'CB',

    'd': 'CC',

    'x': 'CD',

    'k': 'CE',

    'r': 'DA',

    'c': 'DB',

    'v': 'DC',

    's': 'DD',

    'z': 'DE',

    'w': 'EA',

    'b': 'EB',

    'u': 'EC',

    't': 'ED',

    'i': 'EE',

}

def **polibiy\_cipher**(text):

    result = ''

    text = text.lower().replace('j', 'i')

    for i in text:

        result += alphabet[i.lower()]

        result += ' '

    return result

def **get\_key**(d, value):

        for k, v in d.items():

            if v == value:

                return k

def **polibiy\_decipher**(text):

    result = ''

    text = text.split(' ')

    for i in text:

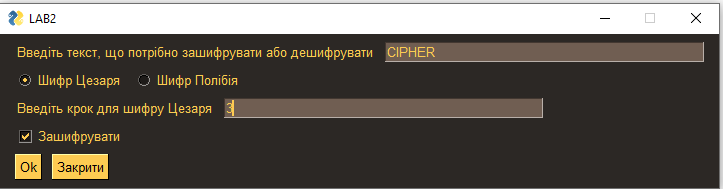
        result += **get\_key**(alphabet, i)

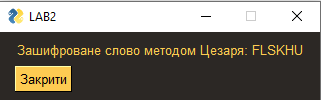
    return result.**upper**()

Результат роботи:

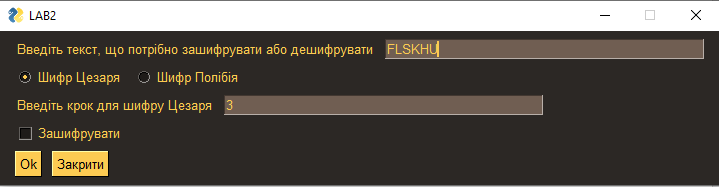
Шифр Цезаря:

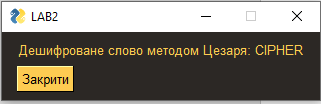
Шифрування:



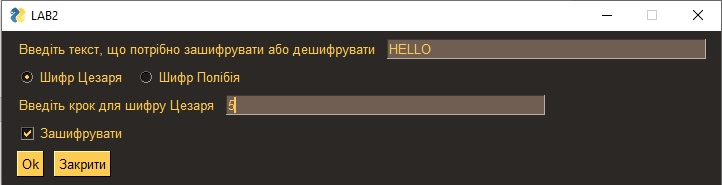


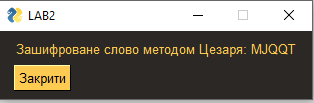
Дешифрування:



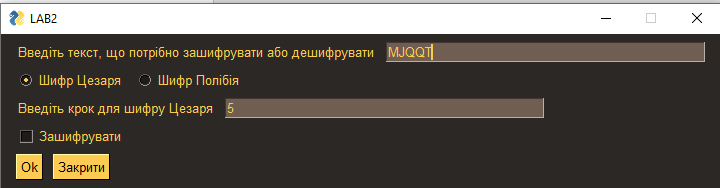


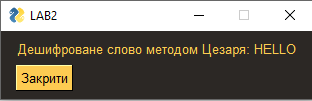
Шифрування:





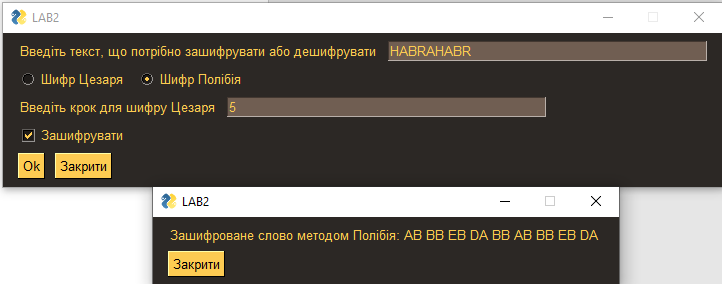
Дешифрування:



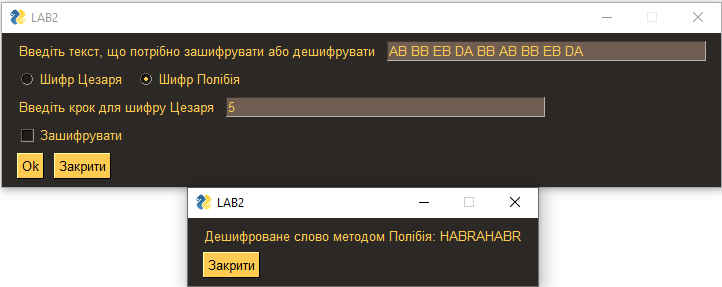


Шифр Полібія:

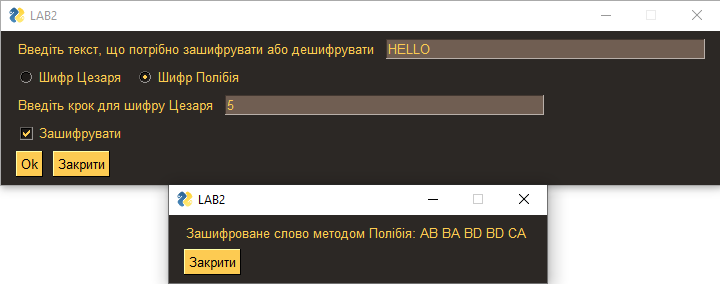
Шифрування:



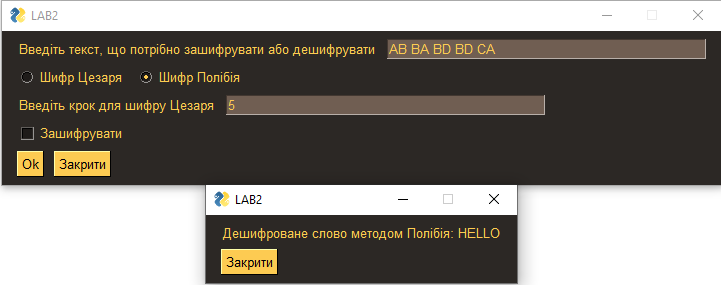
Дешифрування:



Шифрування:



Дешифрування:



Висновок: в цій лабораторні роботі №2 я ознайомився з різними видами шифрування та реалізував два із них, такі як метод Цезаря та метод Полібія із графічним інтерфейсом та їх дешифратори.