МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

ІМЕНИ СЕМЕНА КУЗНЕЦЯ

Лабораторна робота №8

з дисципліни «Математичні основи криптології»

Виконав:

Студент групи 6.04.125.010.21.2

факультету Інформаційних технологій

спеціальності 125

П.І.П. Бойко В.В.

Перевірив:

Чугай А.М.

Харків – 2022

Завдання

Виконати шифрування тексту наступними методами

1. Шифр Віженера

2. Подвіййний квадрат Уітсона

Я написав код для шифрування Вінжера

*def* form\_dict():  
 d = {}  
 iter = 0  
 *for* i *in* range(0,127):  
 d[iter] = chr(i)  
 iter = iter +1  
 *return* d  
  
*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  
  
*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  
  
*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  
  
  
*if* \_\_name\_\_ == "\_\_main\_\_":  
 word = 'simple phrase'  
 key = 'qwerty'  
  
 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))

Приклад роботи



