Міністерство освіти і науки України

Національний університет «Львівська політехніка»

Інститут комп'ютених наук та інформаційних технологій

Кафедра «Системи штучного інтелекту»

Лабораторна робота №3

з курсу "Технології захисту інформації"

Виконала:

студентка групи КН-308

Ріжко Марія

Перевірив:

Яковина В.С.

Львів 2020 р.

Тема роботи

Створення програмного засобу для забезпечення конфідеційності інформації

Завдання

Згідно до варіанту, наведеного в таблиці, створити прикладну програму для шифрування інформації за алгоритмом RC5. Програма повинна отримувати від користувача парольну фразу і, на її основі, шифрувати файли довільного розміру, а результат зберігати у вигляді файлу з можливістю подальшого дешифрування (при введенні тієї самої парольної фрази).

Програмна реалізація

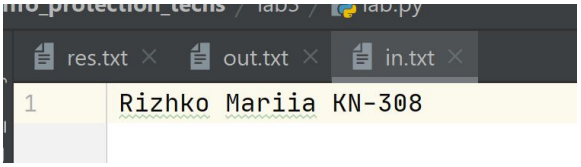
```
from hashlib import md5

w = 16
r = 16
b = 64

key = 'password'

# prepare key
key = md5(key.encode()).digest()[8:]

# create L
w8 = w // 8
L = [0] * (b // w8)
for i in range(b // 8 - 1, -1, -1):
   L[i // w8] = (L[i // w8] << 8) + key[i]

# create S
p = 0xB7E1
q = 0x9E37
mod = 2 ** w
mask = mod - 1
c = b // w8
t = 2 * (r + 1)
S = [(p + i * q) % mod for i in range(t)]


def lshift(val, n):
   n %= w
   return ((val << n) & mask) | ((val & mask) >> (w - n))


def rshift(val, n):
   n %= w
   return ((val & mask) >> n) | (val << (w - n) & mask)
```

```
        # shuffle
        i, j, a, b = 0, 0, 0, 0
        for k in range(3 * max(c, t)):
            a = S[i] = lshift((S[i] + a + b), 3)
            b = L[j] = lshift((L[j] + a + b), a + b)
            i = (i + 1) % t
            j = (j + 1) % c

        # encrypt file
        with open('in.txt', 'rb') as inp, open('res.txt', 'wb') as out:
            empty = False
            while not empty:
                # read text
                text = inp.read(w // 4)
                print(text)
                if not text:
                    break
                if len(text) != w // 4:
                    empty = True
                    text = text.ljust(w // 4, b'\x00')

                # encrypt text
                a = int.from_bytes(text[:w8], byteorder='little')
                b = int.from_bytes(text[w8:], byteorder='little')
                a = (a + S[0]) % mod
                b = (b + S[1]) % mod
                for i in range(1, r + 1):
                    a = (lshift((a ^ b), b) + S[2 * i]) % mod
                    b = (lshift((a ^ b), a) + S[2 * i + 1]) % mod
                text = a.to_bytes(w8, byteorder='little') + b.to_bytes(w8,
byteorder='little')

                # write text
                out.write(text)

        with open('res.txt', 'rb') as inp, open('out.txt', 'wb') as out:
            empty = False
            while not empty:
                # read text
                text = inp.read(w // 4)
                if not text:
                    break
                if len(text) != w // 4:
                    empty = True

                # decrypt text
                a = int.from_bytes(text[:w8], byteorder='little')
                b = int.from_bytes(text[w8:], byteorder='little')
                for i in range(r, 0, -1):
                    B = rshift(b - S[2 * i + 1], a) ^ a
                    a = rshift(a - S[2 * i], b) ^ b
                b = (b - S[1]) % mod
                a = (a - S[0]) % mod
                text = a.to_bytes(w8, byteorder='little') + b.to_bytes(w8,
byteorder='little')

                # write text
                if empty:
                    text = text.rstrip(b'\x00')
                out.write(text)
```

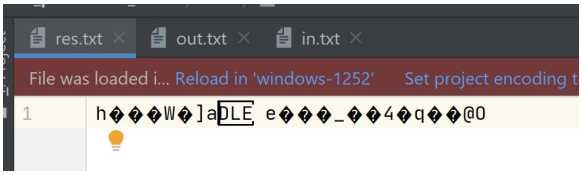
Результати виконання

```
C:\Users\mariz\PycharmProjects\Info_protection_techs\venv\Scripts\python.exe C:/Users/mariz/PycharmProjects/Info_protection_techs/lab3/code.py

Process finished with exit code 0
```

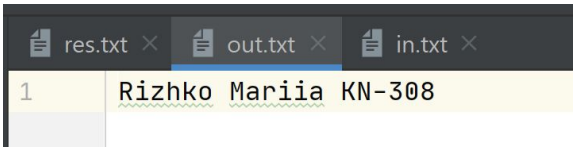
Файл in.txt



Файл res.txt

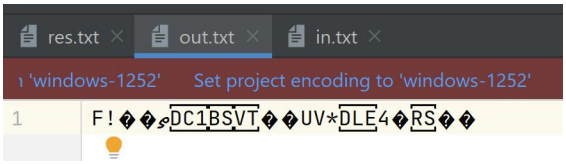


Файл out.txt



RC5 успішно зашиврував і розшиврував дані.

Змінити ключ і попробуємо розшифрувати дані. Результат:



Висновок

На лабораторній роботі я створила програмну реалізацію алгоритму RC5, який успішно закодував і розкодував дані.