Лабораторная работа №8. Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом.

Alexander S. Baklashov

29 October, 2022

RUDN University, Moscow, Russian Federation

Цель работы

Цель работы

Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

Выполнение лабораторной работы

Выполнение

Создадим функцию для шифрования и дешифрования, а также импортируем необх. библиотеки.

```
In [1]: import string

In [2]: def en_de (text1, text2):
            t1=[ord(i) for i in text1]
            t2=[ord(i) for i in text2]
            return ''.join (chr(a^b) for a,b in zip(t1,t2))
```

Figure 1: Функция

Выполнение

Создадим код для выполнения поставленной задачи.

In [3]:
```
P1 = "НаВашисходящийот1204"
P2 = "ВСеверныйфилиалБанка"

hex_key =  "05 0C 17 7F 0E 4E 37 D2 94 10 09 2E 22 57 FF C8 OB B2 70 54"

C1 = en_de (P1, hex_key)
C2 = en_de (P2, hex_key)

print ("Шифорванный текст 'НаВашисходящийот1204':", C1)
print ("Шифорванный текст 'ВСеверныйфилиалБанка':", C2)

decr = en_de (C1, C2)

print ("Расшифорванный текст P1:", en_de (decr, P1))
print ("Расшифорванный текст P2:", en_de (decr, P2))
```

```
Шифорванный текст 'НаВашисходящийот1204': ЭSвÈЋИѰѲОЃЉЖJЎОЎt□□□
Шифорванный текст 'ВСеверныйфилиалБанка': ТДЕЂЎѠЌЎЙѳѼЛJvЛXvНЉЇ
Расшифорванный текст P1: ВСеверныйфилиалБанка
Расшифорванный текст P2: НаВашисходящийот1204
```

Figure 2: Код

Выводы

Выводы

В результате выполнения работы я освоил на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.