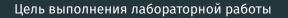
Защита лабораторной работы №8. Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом

Бармина Ольга Константиновна 2022 Sep 22th

RUDN University, Moscow, Russian Federation

Результат выполнения

лабораторной работы №8



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

Результат выполнения лабораторной работы

```
import string
import random

def f1(text):
    return ' '.join(hex(ord(i))[2:] for i in text)

def f2(size):
    return ' '.join(random.choice(string.ascii_letters+string.digits) for _ in range(size))

def f3(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: рис 1. функции

Результат выполнения лабораторной работы

```
p1 = "HaBaшисходящийот1204"
p2 = "BCeepHaNdynmanБанка"
key = f2(len(p1))
key
'i W P V 1 n o k 7 f p e u J Z r 4 r l 6'
hex_key = f1(key)
hex_key
'69 20 57 20 50 20 56 20 31 20 66 20 6f 20 6b 20 37 20 66 20 70 20 65 20 75 20 4a 20 5a 20 72 20 34 20 72 20 6c 20 36'
```

Figure 2: рис 2. создание ключа

Результат выполнения лабораторной работы

ecr1 = f3(p1, key)

```
ecr2 = f3(p2, key)
ecr1, ecr2

('VAXAUN3кЦДСМІЙЅБ\X06\X12V\X14', 'ФЁБВКШЖЖЈКІЛЇАѐбЇНЌА')

decr = f3(ecr1, ecr1)
f3(decr, p1), f3(decr, p2)
```

Figure 3: рис 3. шифрование

('НаВашисходящийот1204', 'ВСеверныйфилиалБанка')

В ходе работы мы освоили на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.