Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом

Гебриал Ибрам [1]

2021 Moscow, Russia

[1]RUDN University, Moscow, Russian Federation

Цель работы

Цель работы

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

Результаты

Результаты

1.Написал блок функции для расчетов. (рис. 1)

```
In [1]: import string
        import random

In [3]: #перевод в шестнадцатиричную систему.
        def hexx(text):
            return ' '.join(hex(ord(i))[2:] for i in text)
        #генерирует рандомный ключ.
        def gen_key(size):
            return ''.join(random.choice(string.ascii_letters + string.digits) for _ in range(size))

        def encrypted(firstText,secondText):
            first_text=[ord(i) for i in firstText]
            second_text=[ord(i) for i in secondText]
            return ''.join(chr (a^b) for a,b in zip(first_text,second_text))
```

Figure 1: Блок функции для расчетов

Результаты

Написал блок обработки данных (рис. 2)

```
In [9]: #Исходные тексты
P1 = "НаВашисходящийот1204"
P2 = "ВСеверныйфилиалБанка"

key=gen_key(len(P1))
print(key)
hex_key=hexx(key)
print("Ключ в шестнадцатиричном виде: ",hex_key)

C1= encrypted(P1,key)
C2= encrypted(P2,key)

print("щифрованное текст: ",C1 )
print("щифрованное текст: ",C2 )

decrypt=encrypted(C1,C2)
print("Расщифрованное текст: ",encrypted(decrypt,P2) )
print("Расщифрованное текст: ",encrypted(decrypt,P1) )
```

```
LqLlTYEKn130tUUlTt9R
Ключ в шестнадцатиричном виде:  4c 71 4c 6c 54 59 45 4b 6e 31 33 30 74 55 55 6c 54 74 39 52
щифрованное текст:  ёсўќMwЄЎèSѼџыѪѫЮeF  f
щифрованное текст:  ўèџўwЙџÈïvЋЋыєѮѼЄщЃЂ
Расщифрованное текст:  НаВашисходящийот1204
Расщифрованное текст:  ВСеверныйфилиалБанка
```

Figure 2: Блок данных и вывод результата

Вывод

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

Спасибо за внимание