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

Гаджиев Нурсултан НПИбд-01-18

Информационная безопасность, 18 декабря, 2021, Москва, Россия

RUDN University

Цель лабораторной работы

Цель лабораторной работы

Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом. # Процесс выполнения лабораторной работы

Выполнение работы

1. Блок функции для расчетов
2. Написал блок обработки данных
3. Итоговый результат

Блок функции для расчетов

Результат

Ввод [24]:
```
import string
import random
```

Ввод [25]:
```
#Перевод в шестнадцатиричную систему:
def hexx(text):
    return ' '.join(hex(ord(i))[2:] for i in text)
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

Блок обработки данных

Результат

Ввод [27]:

```
#Исходный текст:
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("Зашифрованный текст:", C1)
print("Зашифрованный текст:", C2)

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

```
thZq8pz0STYn6DpSETLw
Ключ в шестнадцатиричном виде:  74 68 5a 71 38 70 7a 30 53 54 59 6e 36 44 70 53 45 54 4c 77
Зашифрованный текст: ыjшсΨшлvыЩЖЧЎЬЮБtf|C
Зашифрованный текст: АщЂуЙачоЖAwsЎVытvыЎч
Расшифрованный текст: НаВашисходящийот1204
Расшифрованный текст: ВСеверныйфилиалБанка
```

Figure 2: Чтение текста

Выводы

Выводы

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