Лабораторная работа №8

Информационная безопасность

Тейшейра Боа Морте Селмилтон.

20 Октябрья 2023

Докладчик

- Тейшейра Боа Морте Селмилтон
- Студент Группы НКНбд-01-20
- Факультет Физико-Математических и Естественных Наук
- Российский Университет Дружбы Народов
- https://github.com/Celmilton

Цель работы

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

Выполнение лабораторной работы

Два текста кодируются одним ключом (однократное гаммирование). Требуется не зная ключа и не стремясь его определить, прочитать оба текста. Необходимо разработать приложение, позволяющее шифровать и дешифровать тексты P1 и P2 в режиме однократного гаммирования. Приложение должно определить вид шифротекстов C1 и C2 обоих текстов P1 и P2 при известном ключе ; Необходимо определить и выразить аналитически способ, при котором злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить.

```
[15] import random
     import string
```

```
def hextext(text):
  t=''.join(hex(ord(i))[2:]for i in text)
  return t

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


def encrypt(plaintext ,ciphertext):
    plaintext=[ord(i) for i in plaintext]
    ciphertext=[ord(i) for i in ciphertext]
    create=''.join(chr(a^b)for a,b in zip(ciphertext,plaintext))
    return create

# Textos originais
P1 = "НаВашисходящийот1204"
P2 = "ВСеверныйфилиалБанка"

key = ger_key(len(P1))
print(key)
hex_key=hextext(key)
print("Key in:  {}".format(hex_key))

c1=encrypt(P1,key)
c2=encrypt(P2,key)
print("Encrypt text: {}".format(c1))
print("Encrypt text: {}".format(c2))
```

```
key = ger_key(len(P1))
print(key)
hex_key=hextext(key)
print("Key in:  {}".format(hex_key))

c1=encrypt(P1,key)
c2=encrypt(P2,key)
print("Encrypt text: {}".format(c1))
print("Encrypt text: {}".format(c2))

descrypt=encrypt(c1,c2)
print("Descrypt text: {}".format(encrypt(descrypt,P1)))
print("Descrypt text: {}".format(encrypt(descrypt,P2)))
```

```
DlUODE36UxpcrqtZQ6eB
Key in:  446c554f4445333655787063727174 5a51366542
Encrypt text: ьќчщЌѽѲѳжьпЪьшъИ`Uv
Encrypt text: iэѠѽѱSЎѽѫмшjьсяыwЋџѲ
Descrypt text: ВСеверныйфилиалБанка
Descrypt text: НаВашисходящийот1204
```

Выводы

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