Элементы криптографии. Однократное гаммирование

Гурбангельдиев Мухаммет НФИбд-03-18

Информационная безопасность, 11 декабря, 2021, Москва, Россия

RUDN University

Цель лабораторной работы

Цель лабораторной работы

Освоить на практике применение режима однократного гаммирования

Процесс выполнения лабораторной работы

Выполнение работы

1. Блок функции для расчетов
2. Получение шифротекста
3. Вариант прочтения открытого текста

Блок функции для расчетов

Результат

```
In [23]: import string
         import random

In [24]: 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(text, key):
             return ''.join(chr(a^b) for a, b in zip(text, key))

         def compute_key(text, encrypt):
             return ''.join(chr(a^b) for a,b in zip(text, encrypt))
```

Рис. 1: Блок функции для расчетов

Получение шифротекста

Результат

```
In [25]: message= 'С Новым Годом, друзья!'

         key=gen_key(len(message))
         hex_key=hexx(key)
         print("Используемый ключ:", key)
         print("Ключ в шестнадцатиричном виде:", hex_key)
         encrypt = encrypted([ord(i) for i in message], [ord(i) for i in key])
         hex_encrypt=hexx(encrypt)
         print("Зашифрованное сообщение:", hex_encrypt)
         decryptt = encrypted([ord(i) for i in encrypt], [ord(i) for i in key])
         print("Расшифрованное сообщение:", decryptt)

         Используемый ключ: BuFNEGBLdBPrpd6v5bE0xi
         Ключ в шестнадцатиричном виде: 4275464e4547424c6442507270643676356245307869
         Зашифрованное сообщение: 4635545b47047740c47e6c47747c46444c44c481644247542147247c43748
         Расшифрованное сообщение: С Новым Годом, друзья!

In [26]: compute_key = compute_key([ord(i) for i in message], [ord(i) for i in encrypt])
         decrypt_compute_key= encrypted([ord(i) for i in encrypt], [ord(i) for i in key])
         print("Вариант прочтения открытого тескта:", decrypt_compute_key)

         Вариант прочтения открытого тескта: С Новым Годом, друзья!
```

Рис. 2: Получение шифротекста

Вариант прочтения открытого текста

```
In [26]: compute_key = compute_key([ord(i) for i in message], [ord(i) for i in encrypt])
         decrypt_compute_key= encrypted([ord(i) for i in encrypt], [ord(i) for i in key])
         print("Вариант прочтения открытого тескта:", decrypt_compute_key)

         Вариант прочтения открытого тескта: С Новым Годом, друзья!
```

Рис. 3: Прочтение открытого текста

Выводы

Выводы

Освоил на практике применение режима однократного гаммирования.