Отчет по лабораторной работе №7

Элементы криптографии. Однократное гаммирование

Швец Сергей НФИбд-03-18

Содержание

Цель работы

Освоить на практике применение режима однократного гаммирования

Последовательность выполнения работы

1. Блок функции для расчетов. (рис. -fig. 1)

Ввод [6]:
```
import string
import random
```

Ввод [7]:
```
def scp(text):
    return ''.join(hex(ord(i))[2:] for i in text)
def create_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))
```

Figure 1: Блок функции для расчетов

2. Определил вид шифротекста при известном ключе и известном открытом тексте. (рис. -fig. 2)

Ввод [16]:
```
message= 'С Новым Годом, друзья!'

key=create_key(len(message))
hex_key=scp(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=scp(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: HlUr4voWmpjl1LLeSY0QVy
Ключ в шестнадцатиричном виде: 486c557234766f576d706a6c314c4c65535930515679
Зашифрованное сообщение: 4694c44844c40643d4537747e44e45e45240d606c45141341a40741d41958
Расшифрованное сообщение: С Новым Годом, друзья!
```

Ввод [17]:
```
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!
```

Figure 2: Получение шифротекста

3. Определил ключ,с помощью которого шифротекст может быть преобразо- ван в некоторый фрагменттекста,представляющий собой один из возмож- ных вариантов прочтения открытого текста. (рис. -fig. 3)

```
Ввод [17]: 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!
```

Figure 3: Прочтение открытого текста

Выводы

Освоил на практике применение режима однократного гаммирования.