# Отчет по лабораторной работе №7

**Элементы криптографии. Однократное гаммирование**

Гаджиев Нурсултан НПИ-01-18

# Содержание

1 Цель работы 3

2 Последовательность выполнения работы 4

3 Контрольные вопросы 6

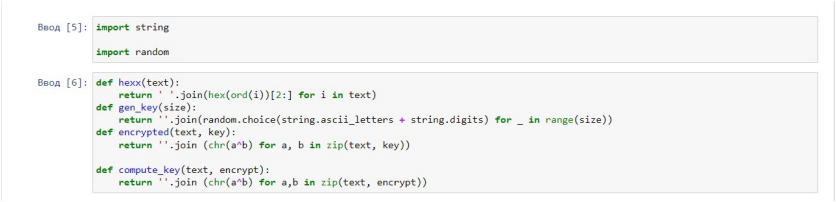
4 Выводы 8

# 1 Цель работы

Освоить на практике применение режима однократного гаммирования

# 2 Последовательность выполнения работы

1. Блок функции для расчетов. (рис. 2.1)

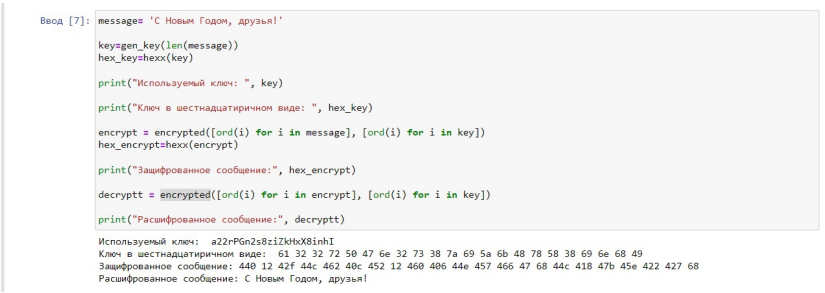


Ввод [5]:
```
import string

import random
```

Ввод [6]:
```
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))
```

Figure 2.1: Блок функции для расчетов

2. Определил вид шифротекста при известном ключе и известном открытом тексте. (рис. 2.2)



Ввод [7]:
```
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:  a22rPGn2s8ziZkHxX8inhI
Ключ в шестнадцатиричном виде:  61 32 32 72 50 47 6e 32 73 38 7a 69 5a 6b 48 78 58 38 69 6e 68 49
Зашифрованное сообщение: 440 12 42f 44c 462 40c 452 12 460 406 44e 457 466 47 68 44c 418 47b 45e 422 427 68
Расшифрованное сообщение: С Новым Годом, друзья!
```

Figure 2.2: Получение шифротекста

3. Определил ключ,с помощью которого шифротекст может быть преобразован в некоторый фрагменттекста,представляющий собой один из возможных вариантов прочтения открытого текста. (рис. 2.3)


Figure 2.3: Прочтение открытого текста

# 3 Контрольные вопросы

1. Поясните смысл однократного гаммирования.

Гаммирование—метод симметричного шифрования,заключающийся в «наложении» последовательности,состоящей из случайных чисел,на открытый текст. Последовательность случайных чисел называется гаммапоследовательностью и используется для зашифровывания и расшифровывания данных.

2. Перечислите недостатки однократного гаммирования.

Ключ одного размера с сообщением,на один ключ используется только один текст.

3. Перечислите преимущества однократного гаммирования.

Простота и криптостойкость.

4. Почему длина открытого текста должна совпадать с длиной ключа?

Каждый символ текста попарно складывается с символом ключа.

5. Какая операция используется в режиме однократного гаммирования,назовите её особенности?

Сложение по модулю 2.Особенность в симметричности–оерация при повторном применении дает исходний результат.

6. Как по открытому тексту и ключу получить шифротекст?

Сложить по модулю 2 каждый символ открытого текста и ключа.

7. Как по открытому тексту и шифротексту получить ключ?

Сложить по модулю 2 каждый символ открытого текста и шифротекста.

8. В чем заключаются необходимые и достаточные условия абсолютной стойкости шифра?

- полная случайность ключа;
- равенство длин ключа и открытого текста;
- однократное использование ключа.

# 4 Выводы

Освоил на практике применение режима однократного гаммирования.