Отчёт по лабораторной работе №7

Серегин Денис Алексеевич

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Освоить на практике применение режима однократного гаммирования.

2 Задание

Нужно подобрать ключ, чтобы получить сообщение **«С Новым Годом, друзья!»**. Требуется разработать приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования. Приложение должно:

1. Определить вид шифротекста при известном ключе и известном открытом тексте.
2. Определить ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста.

3 Выполнение лабораторной работы

1. Изучил указания к лабораторной работе

2. Написал функцию генерации случайного ключа. (рис. **??**)

```
In 18
import secrets

def generate_random_key(length):
    key = ''.join([secrets.choice('0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz') for i in range(length)])
    return key
```

Рис. 3.1: Функция генерации ключа

3. Написал функцию шифрования текста основываюсь на однократном гаммировании. (рис. 3.1)

```
In 19
def encrypt(plaintext, key):
    cyphertext=''
    for i in range(len(plaintext)):
        char = plaintext[i]
        key_char = key[i]
        encrypted_char = chr (ord(char) ^ ord(key_char))
        cyphertext += encrypted_char
    return cyphertext
```

Рис. 3.2: Функция шифрования

4. Написал функцию нахождения ключа при наличии исходного текста и зашифрованного текста. (рис. 3.3)

```
In 20
def find_key(plaintext, cyphertext):
    key = ''
    for i in range(len(plaintext)):
        char = plaintext[i]
        encrypted_char = cyphertext[i]
        key_char = chr (ord(char) ^ ord(encrypted_char))
        key += key_char
    return key
```

Рис. 3.3: Функция нахождения ключа

5. Проверил работу своих методов на фразе «С Новым Годом, друзья!» (рис. 3.4)

```
Изначальный текст С Новым Годом, друзья!
Сгенерированный ключ elS3hE9wcOj6GucGgS1jep
Зашифрованный текст ϕLюЙњЎSWΨψўJ○YCѳЧAIЦЪQ
Найденный ключ elS3hE9wcOj6GucGgS1jep
Равенство ключей  True
```

Рис. 3.4: Вывод работы программы

4 Выводы

В результате выполнения работы я смог освоить метод однократного гаммирования и написать на его основе шифруюшее приложение.