Отчёт по лабораторной работе №7

Режим Однократного Гарммирования

Вакутайпа Милдред

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Научиться применять режим однократного гарммирования.

2 Задание

Подобрать ключ, чтобы получить сообщение “С Новым Годом”. Требуется разработать приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования.

3 Выполнение лабораторной работы

На языке программирования python, создала функцию для генерации случайного ключа.

```
import string
import random

def generate_key (text):
    return ''.join(random.choice(string.ascii_letters + string.digits) for _ in text)
```

Рис. 3.1: Функция для генерации ключа

Делала одну функцию для шифрования и дешифрования текста.

```
def crypt (text, key):
    return ''.join(chr(ord(c)^ord(k)) for c, k in zip(text, key))
```

Рис. 3.2: Функция для шифрования и дешифрования

Нужно определить ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста. Для этого создала функцию для нахождения возможных ключей для фрагмента текста.

```
def find_keys(cipher, fragment):
    return [''.join(chr(ord(cipher[i+j])^ord(f)))
            for i in range(len(cipher)-len(fragment)+1)
            for j, f in enumerate(fragment)]
```

Рис. 3.3: функция для нахождения возможных ключей

Далее проверила работы программы. Шифрирование и дешифрирование происходит верно, как и нахождение ключей, с помощью которых можно расшифровать верно кусок текста.

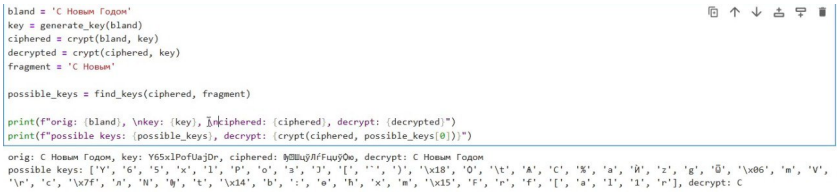

Рис. 3.4: Проверка

4 Выводы

При выполнении данной работы я научилась применять режим однократного гарммирования.

Список литературы