

Лабораторная работа № 7.

Серегин Д.А.

21 октября 2023

Российский университет дружбы народов, Москва, Россия

Цель работы

Освоить на практике применение режима однократного гаммирования.

Выполнение работы

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.

1. Изучил указания к лабораторной работе
2. Написал функцию генерации случайного ключа.

```
In 18 1 import secrets
      2
      3 def generate_random_key(length):
      4     key = ''.join([secrets.choice('0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz') for i in range(length)])
      5     return key
```

Рис. 1: Функция генерации ключа

3. Написал функцию шифрования текста основываясь на однократном гаммировании.

```
In 19 1 def encrypt(plaintext, key):  
      2     cyphertext=''  
      3     for i in range(len(plaintext)):  
      4         char = plaintext[i]  
      5         key_char = key[i]  
      6         encrypted_char = chr (ord(char) ^ ord(key_char))  
      7         cyphertext += encrypted_char  
      8     return cyphertext
```

Рис. 2: Функция шифрования

4. Написал функцию нахождения ключа при наличии исходного текста и зашифрованного текста. (рис. (fig:003?))

```
In 20 1 def find_key(plaintext, cyphertext):  
      2     key = ''  
      3     for i in range(len(plaintext)):  
      4         char = plaintext[i]  
      5         encrypted_char = cyphertext[i]  
      6         key_char = chr(ord(char) ^ ord(encrypted_char))  
      7         key += key_char  
      8     return key
```

Рис. 3: Функция нахождения ключа

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

```
Изначальный текст С Новым Годом, друзья!  
Сгенерированный ключ eLS3hE9wc0j6GucGgS1jer  
Зашифрованный текст фЛюЙньЎSWΨψЎJоYCөЧАIЦЪQ  
Найденный ключ eLS3hE9wc0j6GucGgS1jer  
Равенство ключей True
```

Рис. 4: Вывод работы программы

Вывод

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