Презентация по лабораторной работе № 7

Информационная безопасность

Адебайо Р. А.

20.10.2023

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Адебайо Ридвануллахи Айофе
- студент группы НКНбд-01-20
- Факультет физико-математических и естественных наук
- Российский университет дружбы народов
- Страничка на GitHub
- Страничка на LinkedIn

Цель лабораторной работы

Цель лабораторной работы

Освоить на практике применение режима однократного гаммирования

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.

Порядок выполнения работы(1)

Определить вид шифротекста при известном ключе и известном открытом тексте

```
1 text="С Новым Годом, друзья!"
```

```
1 key=""
2 seed(23)
3 for i in range(len(text)):
4     key += random.choice(string.ascii_letters + string.digits)
5 print(key)
```

```
7X8s51fbLtByHwiUmrCaoN
```

Рис. 1: создание ключа той же длины, что и открытый текст

Порядок выполнения работы(2)

Определить ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста.

In [3]:

```python
def cipher_text_function(text, key):
    #condition to check if the key and text have the same length
    if len(key) != len(text):
        return "Key and text must have the same length"
    cipher_text = ""
    for i in range (len(key)):
        cipher_text_symbol=ord(text[i]) ^ ord(key[i])
        cipher_text+=chr(cipher_text_symbol)
    return cipher_text
```

In [9]:

```python
cipher_text = cipher_text_function(text, key)
print(cipher_text)
```

```
ЖхХэЇЮьВцъЎчV[IwЭбVЭРо
```

In [11]:

```python
print(f"Text: {cipher_text_function(cipher_text, key)}")
```

Вывод

Вывод

В ходе выполнения данной лабораторной работы я освоил на практике применение режима однократного гаммирования