Лабораторная работа № 8.

Серегин Д.А.

28 октября 2023

Российский университет дружбы народов, Москва, Россия

Цель работы

Цель работы

Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

Выполнение работы

Задание

2. Два текста кодируются одним ключом (однократное гаммирование). Требуется не зная ключа и не стремясь его определить, прочитать оба текста. Необходимо разработать приложение, позволяющее шифровать и дешифровать тексты P1 и P2 в режиме однократного гаммирования. Приложение должно определить вид шифротекстов C1 и C2 обоих текстов P1 и P2 при известном ключе ; Необходимо определить и выразить аналитически способ, при котором злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить.

Генерация ключа

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 основываюсь на однократном гаммировании.

```
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. 2: Функция шифрования

5. Попробовал расшифровать полученный текст используя изначальные тексты. Как итог расшифровывая одним текстом я получал другой исходный.

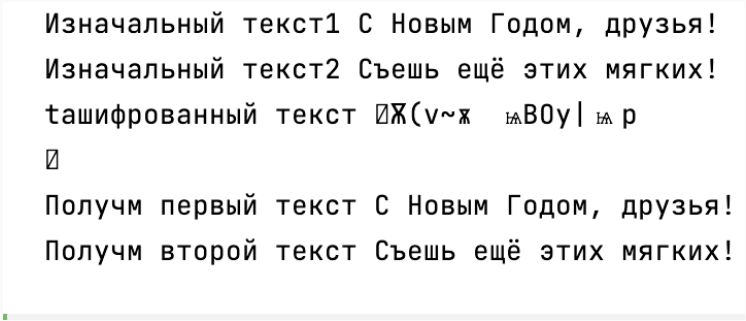

Рис. 3: Вывод работы программы

Вывод

Вывод

В результате выполнения работы я смог освоить метод однократного гаммирования и написать на его основе шифруюшее приложение, чтобы зашифровать два текста.