Отчёт по лабораторной работе №8

Серегин Денис Алексеевич

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

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

2 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.

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. 3.2)

```
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. Взял два текста и зашифровал их друг другом (рис. **??**)
5. Попробовал расшифровать полученный текст используя изначальные тексты. Как итог расшифровывая одним текстом я получал другой исходный. (рис. 3.3)

```
Изначальный текст1 С Новым Годом, друзья!
Изначальный текст2 Съешь ещё этих мягких!
tашифрованный текст ⍰Ӂ(v~ӂ  ѩBOy|ѩ p
⍰
Получм первый текст С Новым Годом, друзья!
Получм второй текст Съешь ещё этих мягких!
```

Рис. 3.3: Вывод работы программы

4 Выводы

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