Лабораторная работа № 8

Байрамгельдыев
Довлетмурат
28 октября 2023, Москва

Цели

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

Задачи

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.

Ход работы

Создаем функцию шифрования.

```
In [3]: def ecncrypt(t1, t2):
            t1 = [ord(i) for i in t1]
            t2 = [ord(i) for i in t2]
            return ''.join(chr(a^b) for a, b in zip(t1, t2))
```

Рис. 1: Функция шифрования

Ход работы

Введем данные из условия.

```
In [4]: P1 = "НаВашисходящийот1204"
        P2 = "ВСеверныйфилиалБанка"

        K = "05 0C 17 7F 0E 4E 37 D2 94 10 09 2E 22 57 FF C8 0B B2 70 54"
```

Рис. 2: Данные из условия

Ход работы

Зашифруем текст с помощью ключа K.

```
C1 = ecncrypt(P1, K)
C2 = ecncrypt(P2, K)

print("Зашифрованный текст C1:", C1)
print("Зашифрованный текст C2:", C2)
```

Рис. 3: Шифрование текста

Ход работы

Создадим последовательность, с помощью которой будем расшифровывать текст. Передадим ее в функцию шифрования вместе с зашифрованным текстом.

```
decr = ecncrypt(C1, C2)

print("Расшифрованный текст P1:", ecncrypt(decr, P1))
print("Расшифрованный текст P2:", ecncrypt(decr, P2))
```

Рис. 4: Расшифровка текста

Ход работы

Запустим программу и получим результат.

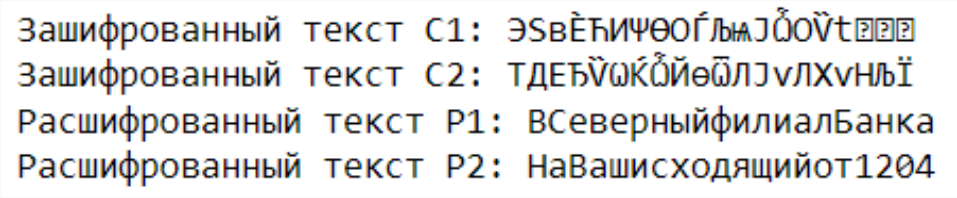

Рис. 5: Результат

Результаты

В рамках данной лабораторной работы было освоено на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.