Лабораторная работа №8

Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом

Ван И

28 октября 2023

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Ван И
- студент НФИбд-02-20
- Российский университет дружбы народов
- 1032198069@pfur.ru
- https://github.com/WangYi157

Вводная часть

Цели

Освоить на практике применение режима однократного гаммирования

Цели

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

Создаем функцию шифрования (@fig:001).

```
def encr(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

Введем данные из условия (@fig:002).

```
P1 = "НаВашисходящийот1204"
P2 = "ВСеверныйфилиалБанка"

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

Рис. 2: Данные из условия

Зашифруем текст с помощью ключа K. Создадим последовательность, с помощью которой будем расшифровывать текст. Передадим ее в функцию шифрования вместе с зашифрованным текстом. (@fig:003).

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

decr = encr(C1, C2)
```

Рис. 3: Шифрование текста

Запустим программу и получим результат (@fig:004).

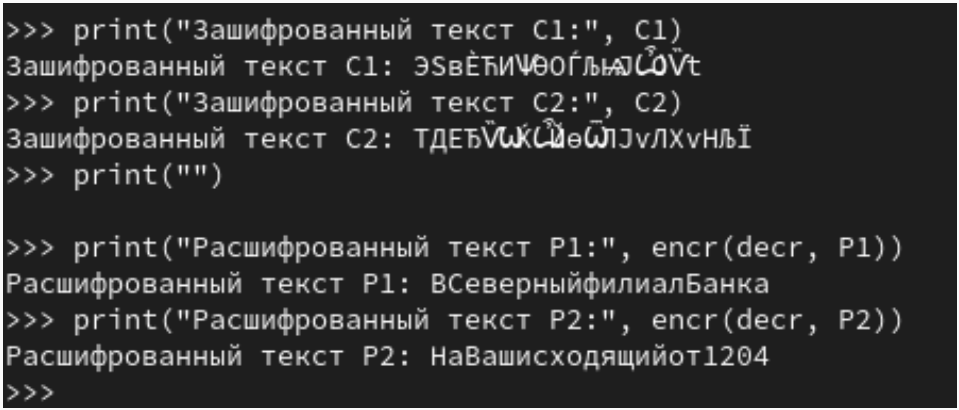

Рис. 4: Результат выполнения программы

Вывод

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