Отчет по лабораторной работе №8

по дисциплине: Информационная безопасность

Го Чаопэн

Содержание

Список иллюстраций

1 Цель работы

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

2 Задание

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 Теоретическое введение

- Шифрование – это технология кодирования и раскодирования данных.Зашифрованные данные -это результат применения алгоритма для кодирования данных с целью сделать их недоступными для чтения. Данные могут быть раскодированы в исходную форму только путем применения специальный ключа [1].
- Гаммирование — это наложение (или снятие при расшифровке сообщений) на открытое (или зашифрованное) сообщение так называемой криптографической гаммы. Криптографическая гамма — это последовательность элементов данных, которая вырабатывается с помощью определенного алгоритма. [2].

4 Выполнение лабораторной работы

1. Создаем функцию шифрования (4.1).

```
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. 4.1: Функция шифрования

2. Введем данные из условия (4.2).

```
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. 4.2: Данные из условия

3. Зашифруем текст с помощью ключа K (4.3).

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

Рис. 4.3: Шифрование текста

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

```
decr = ecncrypt(C1, C2)
```

5. Запустим программу и получим результат (4.4).

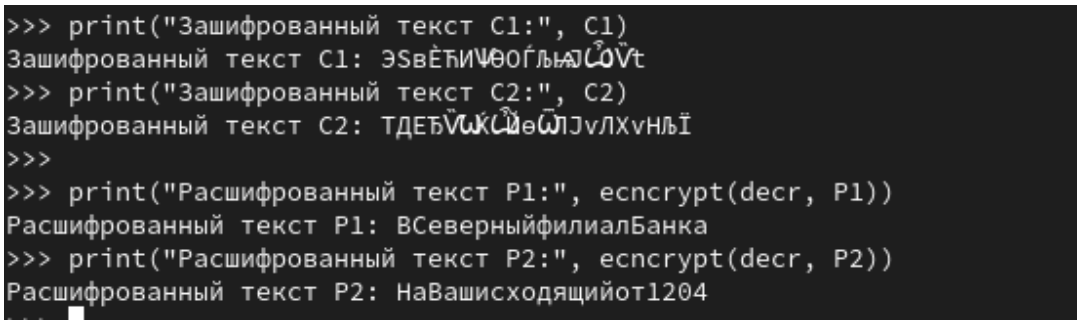

Рис. 4.4: Результат выполнения программы

5 Выводы

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

6 Список литературы

1. Шифрование информации: как защитить свои данные [Электронный ресурс]. URL: https://gb.ru/blog/shifrovanie-informatsii/.

2. Гаммирование [Электронный ресурс]. URL: https://science.fandom.com/ru/wiki/%D0%93%D0%B0%D0%BC%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5.