Отчет по лабораторной работе №7

Элементы криптографии. Однократное гаммирование

Каримов Зуфар НПИ-01-18

Содержание

1 Цель работы

Освоить на практике применение режима однократного гаммирования

2 Последовательность выполнения работы

1. Блок функции для расчетов. (рис. 2.1)

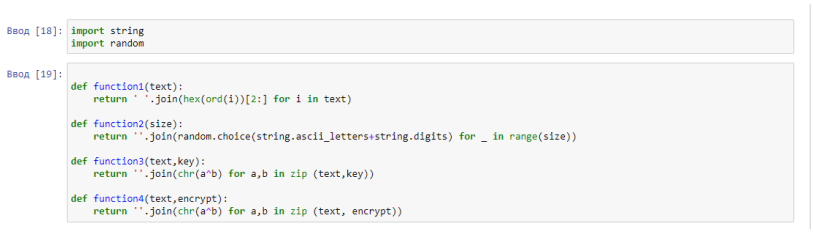

Figure 2.1: Блок функции для расчетов

2. Определил вид шифротекста при известном ключе и известном открытом тексте. (рис. 2.2)

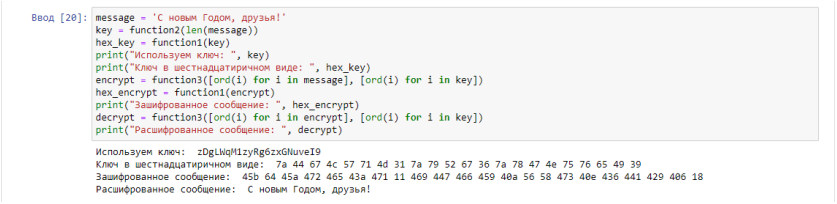

Figure 2.2: Получение шифротекста

3. Определил ключ,с помощью которого шифротекст может быть преобразован в некоторый фрагменттекста,представляющий собой один из возможных вариантов прочтения открытого текста. (рис. 2.3)

```
Ввод [23]: compute_key = function4([ord(i) for i in message], [ord(i) for i in encrypt])
           decrypt_compute_key = function3([ord(i) for i in encrypt], [ord(i) for i in key])
           print("Исходный ключ: ", key)
           print("Вариант прочтения открытого текста: ", decrypt_compute_key)

           Исходный ключ:  zDgLWqM1zyRg6zxGNuveI9
           Вариант прочтения открытого текста:  С новым Годом, друзья!
```

Figure 2.3: Прочтение открытого текста

3 Контрольные вопросы

1. Поясните смысл однократного гаммирования.

Гаммирование—метод симметричного шифрования,заключающийся в «наложении» последовательности,состоящей из случайных чисел,на открытый текст. Последовательность случайных чисел называется гаммапоследовательностью и используется для зашифровывания и расшифровывания данных.

2. Перечислите недостатки однократного гаммирования.

Ключ одного размера с сообщением,на один ключ используется только один текст.

3. Перечислите преимущества однократного гаммирования.

Простота и криптостойкость.

4. Почему длина открытого текста должна совпадать с длиной ключа?

Каждый символ текста попарно складывается с символом ключа.

5. Какая операция используется в режиме однократного гаммирования,назовите её особенности?

Сложение по модулю 2.Особенность в симметричности–оерация при повторном применении дает исходний результат.

6. Как по открытому тексту и ключу получить шифротекст?

Сложить по модулю 2 каждый символ открытого текста и ключа.

7. Как по открытому тексту и шифротексту получить ключ?

Сложить по модулю 2 каждый символ открытого текста и шифротекста.

8. В чем заключаются необходимые и достаточные условия абсолютной стойкости шифра?

- полная случайность ключа;
- равенство длин ключа и открытого текста;
- однократное использование ключа.

4 Выводы

Освоил на практике применение режима однократного гаммирования.