Лабораторная работа №7

Элементы криптографии. Однократное гаммирование

Валиева Найля Разимовна

Содержание

Список таблиц

Список иллюстраций

1 Цель работы

Освоить на практике применение режима однократного гаммирования [1].

2 Задание

1. Написать программу, которая должна определить вид шифротекста при известном ключе и известном открытом тексте
2. Также эта программа должна определить ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста

3 Выполнение лабораторной работы

1. Написала функцию шифрования, которая определяет вид шифротекста при известном ключе и известном открытом тексте “С Новым Годом, друзья!”. Ниже представлены функция, шифрующая данные (рис - @fig:001), а также работа данной функции (рис - @fig:002).

```
In [2]: import numpy as np

In [3]: def encryption(text):
            print("Open text", text)

            text_array = []
            for i in text:
                text_array.append(i.encode("cp1251").hex())
            print("\nOpen text of 16th format", *text_array)


            key_dec = np.random.randint(0, 255, len(text))
            key_hex = [hex(i)[2:] for i in key_dec]
            print("\nKey of 16th format", *key_hex)

            crypt_text = []
            for i in range(len(text_array)):
                crypt_text.append("{:2x}".format(int(text_array[i], 16) ^ int(key_hex[i], 16)))
            print("\nEncrypted text of 16th format", *crypt_text)

            final_text = bytearray.fromhex("".join(crypt_text)).decode("cp1251")
            print("\nEncrypted text", final_text)
            return key_hex, final_text
```

Рис. 3.1: Функция, шифрующая данные

```
In [5]: a = "С Новым годом, друзья!"

        crypt_key, crypt_text = encryption(a)

        Open text С Новым годом, друзья!

        Open text of 16th format d1 20 cd ee e2 fb ec 20 e3 ee e4 ee ec 2c 20 e4 f0 f3 e7 fc ff 21

        Key of 16th format 65 61 f6 40 ca 4b 94 3 f6 3d 24 15 5d 3b 12 f9 6e b9 42 bf 7f fc

        Encrypted text of 16th format b4 41 3b ae 28 b0 78 23 15 d3 c0 fb b1 17 32 1d 9e 4a a5 43 80 dd

        Encrypted text rA;®(°x#ⅢУАы±Ⅲ2ⅢhJГСЪЭ
```

Рис. 3.2: Результат работы функции, шифрующей данные

2. Написала функцию дешифровки, которая определяет ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент

текста, представляющий собой один из возможных вариантов прочтения открытого текста (рис - @fig:003). А также представила результаты работы программы (рис - @fig:004).

```
In [4]: def decryption(text, final_text):
            print("Open text", text)
            print("\nEncrypted text", final_text)

            text_hex = []
            for i in text:
                text_hex.append(i.encode("cp1251").hex())
            print("\nOpen text of 16th format", *text_hex)

            final_text_hex = []
            for i in final_text:
                final_text_hex.append(i.encode("cp1251").hex())
            print("\nEncrypted text of 16th format", *final_text_hex)

            key = [hex(int(i, 16) ^ int(j, 16))[2:] for (i,j) in zip(text_hex, final_text_hex)]
            print("\nKey we needed with 16th format", *key)
            return key
```

Рис. 3.3: Функция, дешифрующая данные

```
In [6]: key = decryption(a, crypt_text)
Open text С Новым годом, друзья!

Encrypted text rA;®(°x#ⅢУАы±Ⅲ2ⅢhJГСЪЭ

Open text of 16th format d1 20 cd ee e2 fb ec 20 e3 ee e4 ee ec 2c 20 e4 f0 f3 e7 fc ff 21

Encrypted text of 16th format b4 41 3b ae 28 b0 78 23 15 d3 c0 fb b1 17 32 1d 9e 4a a5 43 80 dd

Key we needed with 16th format 65 61 f6 40 ca 4b 94 3 f6 3d 24 15 5d 3b 12 f9 6e b9 42 bf 7f fc
```

Рис. 3.4: Результат работы функции, дешифрующей данные

Сравнение ключей, полученных с помощью первой и второй функций (рис - @fig:005).

```
In [7]: print("Answer is right!") if crypt_key == key else print("Answer isnt right")
Answer is right!
```

Рис. 3.5: Сравнение ключей

4 Выводы

Освоила на практике применение режима однократного гаммирования.

5 Ответы на контрольные вопросы

1. Одократное гаммирование - выполнение операции XOR между элементами гаммы и элементами подлежащего сокрытию текста. Если в методе шифрования используется однократная вероятностная гамма (однократное гаммирование) той же длины, что и подлежащий сокрытию текст, то текст нельзя раскрыть. Даже при раскрытии части последовательности гаммы нельзя получить информацию о всём скрываемом тексте.

2. Недостатки однократного гаммирования: Абсолютная стойкость шифра доказана только для случая, когда однократно используемый ключ, длиной, равной длине исходного сообщения, является фрагментом истинно случайной двоичной последовательности с равномерным законом распределения.

3. Преимущества однократного гаммирования: во-первых, такой способ симметричен, т.е. двойное прибавление одной и той же величины по модулю 2 восстанавливает исходное значение; во-вторых, шифрование и расшифрование может быть выполнено одной и той же программой. Наконец, Криптоалгоритм не даёт никакой информации об открытом тексте: при известном зашифрованном сообщении C все различные ключевые последовательности K возможны и равновероятны, а значит, возможны и любые сообщения P.

4. Длина открытого текста должна совпадать с длиной ключа, т.к. если ключ

короче текста, то операция XOR будет применена не ко всем элементам и конец сообщения будет не закодирован, а если ключ будет длиннее, то появится неоднозначность декодирования.

5. Операция XOR используется в режиме однократного гаммирования. Наложение гаммы по сути представляет собой выполнение побитовой операции сложения по модулю 2, т.е. мы должны сложить каждый элемент гаммы с соответствующим элементом ключа. Данная операция является симметричной, так как прибавление одной и той же величины по модулю 2 восстанавливает исходное значение.
6. Получение шифротекста по открытому тексту и ключу: $C_i = P_i \oplus K_i$

7. Получение ключа по окрытому тексту и шифротексту: $K_i = P_i \oplus C_i$

8. Необходимы и достаточные условия абсолютной стойкости шифра: полная случайность ключа; равенство длин ключа и открытого текста; однократное использование ключа.

6 Список литературы

1. Кулябов Д. С., Королькова А. В., Геворкян М. Н. Информационная безопасность компьютерных сетей. Лабораторная работа № 7. Элементы криптографии. Однократное гаммирование.