Отчёт по лабораторной работе №7. Элементы криптографии. Однократное гаммирование.

Предмет: информационная безопасность

Александр Сергеевич Баклашов

Содержание

List of Figures

1 Цель работы

Освоить на практике применение режима однократного гаммирования. [1]

2 Теоретическое введение

Информационная безопасность – это защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры.

3 Выполнение лабораторной работы

1. Создадим функции для перевода в 16-ричный вид, шифрования и дешифрования, а также импортируем необх. библиотеки. (рис. 3.1)

```
In [1]: import string
        import random

In [2]: def hex_16(txt):
            return ' '.join(hex(ord(i))[2:] for i in txt)
        def cypher(size):
            return ''.join(random.choice(string.ascii_letters+string.digits) for _ in range(size))
        def decypher (txt, key):
            return ''.join(chr(a^b) for a,b in zip (txt,key))
```

Figure 3.1: Функции

2. Создадим код для получения шифротекста. (рис. 3.2)

```
In [3]: msg = "С Новым Годом, друзья!"
        key = cypher (len(msg))
        hex_key = hex_16(key)
        print ("Ключ:", key)
        print ("Ключ в 16-ричном виде:", hex_key)
        encr = decypher ([ord(i) for i in msg], [ord(i) for i in key])
        hex_encr = hex_16 (encr)
        print ("Зашифр. сообщение:", hex_encr)
        decr=decypher ([ord(i) for i in encr], [ord(i) for i in key])
        print ("Расшифр. сообщ.:", decr)

Ключ: Cjy9C184jA8QkVWihuKrmr
Ключ в 16-ричном виде: 43 6a 79 39 43 31 38 34 6a 41 38 51 6b 56 57 69 68 75 4b 72 6d 72
Зашифр. сообщение: 462 4a 464 407 471 47a 404 14 479 47f 40c 46f 457 7a 77 45d 428 436 47c 43e 422 53
Расшифр. сообщ.: С Новым Годом, друзья!
```

Figure 3.2: Шифротекст

3. Создадим код для получения варианта прочтения открытого текста. (рис. 3.3)

```
In [4]: decr1=decypher ([ord(i) for i in encr], [ord(i) for i in key])
        print ("Ключ:", key)
        print ("Вариант прочтения откр. текста:", decr1)

Ключ: Cjy9C184jA8QkVWihuKrmr
Вариант прочтения откр. текста: С Новым Годом, друзья!
```

Figure 3.3: Открытый текст

4 Вывод

В результате выполнения работы я освоил на практике применение режима однократного гаммирования.

5 Контрольные вопросы

1. Поясните смысл однократного гаммирования.

Гаммирование - выполнение операции сложения по модулю 2 (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. Перечислите недостатки однократного гаммирования.

Абсолютная стойкость шифра доказана только в случае, когда однократно используемый ключ, длиной, равной длине исходного сообщения, является фрагментом истинно случайной двоичной последовательности с равномерным законом распределения.

3. Перечислите преимущества однократного гаммирования.

Такой метод шифрования является симметричным, так как двойное прибавление одной и той же величины по модулю 2 восстанавливает исходное значение, а шифрование и расшифрование выполняется одной и той же программой. 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. Почему длина открытого текста должна совпадать с длиной ключа?

Если ключ длиннее текста - появится неоднозначность декодирования, а если короче - операция XOR будет применена не ко всем элементам.

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

Используется операция XOR, которая является симметричной.

6. Как по открытому тексту и ключу получить шифротекст?

Если известны ключ и открытый текст, то задача нахождения шифротекста заключается в применении к каждому символу открытого текста следующего правила: Ci = Pi (+) Ki где Ci — i-й символ получившегося зашифрованного послания, Pi — i-й символ открытого текста, Ki — i-й символ ключа, i = 1, m.

7. Как по открытому тексту и шифротексту получить ключ?

Если известны шифротекст и открытый текст, то обе части равенства необходимо сложить по модулю 2 с Pi: Ci (+) Pi = Pi (+) Ki (+) Pi = Ki, Ki = Ci (+) Pi.

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

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

6 Библиография

1. Лабораторная работа № 7. Элементы криптографии. Однократное гаммирование. - 3 с. [Электронный ресурс]. М. URL: Лабораторная работа №6 (Дата обращения: 18.10.2022).