Отчет по лабораторной работе 7

Радимов Игорь

Содержание

List of Tables

List of Figures

1 Цель работы

Освоить на практике применение режима однократного гаммирования.

2 Задание

Лабораторная работа подразумевает использование языков программирования для создания программы для щифрования и дещифрования в режиме однократного гаммирования.

3 Теория

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

4 Выполнение работы

1. Разработаем приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования.(рис 1)

```
In [57]: import string
         import random

         text='С Новым Годом, друзья!'

         def generator(length,abc):
             return ''.join(random.choice(abc) for i in range(length))
         abc=string.ascii_letters.join(string.digits)
         key=generator(len(text),abc)

In [58]: def gamm(string,key):
             return ''.join(chr(n^m) for n,m in zip ([ord(i) for i in string ],[ord(i) for i in key]))

In [59]: txt1=gamm(text,key)   #закодированная строка

In [60]: key2=generator(len(txt1),abc)
         txt2=gamm(txt1,key2)
         txt2 #расшифрованная строка

Out[60]: "Ш8вжвшЩ\x18ЩвЌЇь\x1b'гшькмь\x00"

In [61]: true_key=gamm(text,txt1)  #настоящий ключ

In [62]: gamm(txt1,true_key) #декодированная строка

Out[62]: 'С Новым Годом, друзья!'
```

Figure 4.1: рис.1. Программа.

5 Контрольные вопросы

1. Поясните смысл однократного гаммирования.

Гаммирование – это наложение (снятие) на открытые (зашифрованные) данные криптографической гаммы, то есть последовательности элементов данных, вырабатываемых с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных.

Однократное гаммирование – это когда каждый символ попарно с символом ключа складываются по модулю 2 (XOR).

2. Перечислите недостатки однократного гаммирования.

Размер ключевого материала должен совпадать с размером передаваемых сообщений. Также необходимо иметь эффективные процедуры для выработки случайных равновероятных двоичных последовательностей и специальную службу для развоза огромного количества ключей. А ещё, если одну и ту же гамму использовать дважды для разных сообщений, то шифр из совершенно стойкого превращается в «совершенно нестойкий» и допускает дешифрование практически вручную.

3. Перечислите преимущества однократного гаммирования.

С точки зрения теории криптоанализа метод шифрования случайной однократной равновероятной гаммой той же длины, что и открытый текст, является невскрываемым. Кроме того, даже раскрыв часть сообщения, дешифровщик не сможет хоть сколько-нибудь поправить положение -

информация о вскрытом участке гаммы не дает информации об остальных ее частях. К достоинствам также можно отнести простоту реализации и удобство применения.

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

Потому что каждый символ открытого текста должен складываться с символом ключа попарно.

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

В режиме однократного гаммирования используется сложение по модулю 2 (XOR) между элементами гаммы и элементами подлежащего сокрытию текста. Особенность заключается в том, что этот алгоритм шифрования является симметричным. Поскольку двойное прибавление одной и той же величины по модулю 2 восстанавливает исходное значение, шифрование и расшифрование выполняется одной и той же программой.

6 Библиография

1. ТУИС РУДН

7 Выводы

Во время выполнения лабораторной работы я освоил на практике применение режима однократного гаммирования.