Лабораторная работа №7

Дисциплина: основы информационной безопастности

Астраханцева А. А.

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Освоить на практике применение режима однократного гаммирования.

2 Теоретическое введение

Гаммирование представляет собой наложение (снятие) на открытые (зашифрованные) данные последовательности элементов других данных, полученной с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных. Иными словами, наложение гаммы — это сложение её элементов с элементами открытого (закрытого) текста по некоторому фиксированному модулю, значение которого представляет собой известную часть алгоритма шифрования. В соответствии с теорией криптоанализа, 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.Наложение гаммы по сути представляет собой выполнение операции сложения по модулю 2 (XOR) (обозначаемая знаком ⊠) между элементами гаммы и элементами подлежащего сокрытию текста.

3 Выполнение лабораторной работы

Нужно подобрать ключ, чтобы получить сообщение «С Новым Годом, друзья!». Требуется разработать приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования. Приложение должно:

1. Определить вид шифротекста при известном ключе и известном открытом тексте.

2. Определить ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста. (рис. 3.1).

Рис. 3.1: Название рисунка

```
import randomimport string
```

```
def generate_key(message_length):
return [random.choice(string.ascii_letters + string.digits) for _ in range(messag

def encrypt_decrypt(text, key):
    if len(text) != len(key): return "Ключ и сообщение разной длины"
    xor_text = ''
    for i in range(len(text)):
        xor_symbol = ord(text[i]) ^ ord(key[i])
        xor_text += chr(xor_symbol)
        return xor_text

message = "С Новым Годом, друзья!"
key = generate_key(len(message))print(key)
encrypted_messge = encrypt_decrypt(message, key)
encrypt_decrypt(encrypted_messge, key)
```

Листинг 1. Код приложения

4 Контрольные вопросы

1. Поясните смысл однократного гаммирования.

Используется случайный ключ, такой же длины, что и сообщение. Для шифрования каждый символ открытого текста складывается по модулю 2 с соответствующим символом из ключа.

2. Перечислите недостатки однократного гаммирования.

Неудобство в обмене ключами, так как каждый ключ должен быть столь же длинным, как и открытый текст. Один и тот же ключ не должен использоваться более одного раза, иначе это уязвимость.

3. Перечислите преимущества однократного гаммирования.

Так как используется случайный ключ - вероятность подорбать такой же слишком мала. Простота реализации.

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

Потому что шифрование и дешифрование происходит путем применения опрации “сложение по модулю 2” для каждого символа ключа и текста для передачи/зашифорванного текста. Именно поэтому нужно ключ такой же длины.

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

Операция XOR (исключающее ИЛИ) используется в режиме однократного гаммирования. Особенностью XOR является то, что результат равен true (1) только в том случае, если только один из операндов равен true (1).

6. Как по открытому тексту и ключу получить шифротекст?

Для получения шифротекста необходимо применить операцию XOR для каждого элемента текста и ключа (попарно).

7. Как по открытому тексту и шифротексту получить ключ?

Для получения ключа необходимо применить операцию XOR для каждого элемента текста и шифротекста (попарно).

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

– полная случайность ключа;
– равенство длин ключа и открытого текста;
– однократное использование ключа

5 Выводы

В ходе выполнения ЛР№7 я освоила на практике применение режима однократного гаммирования.

Список литературы

1. Курс “Основы инфомационной безопасности”