Лабораторная работа №7

Основы информационной безопастности

Астраханцева А. А.

9 мая 2024

Российский университет дружбы народов, Москва, Россия

Докладчик

- Астраханцева Анастасия Александровна
- студентка НКАбд-01-22
- Студ. билет: 1132226437
- Российский университет дружбы народов
- https://anastasiia7205.github.io/

Цель работы

Освоить на практике применение режима однократного гаммирования.

Выполнение лабораторной работы

Код приложения

```
import randomimport string

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

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!"
```

Ответы на 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 слиишком 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/зашиформванного 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

Выводы

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

Спасибо за внимание