РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

ПРЕЗЕНТАЦИЯ ПО ЛАБОРАТОРНОЙ РАБОТЕ №7

дисциплина: Информационная безопасность

Преподователь: Кулябов Дмитрий Сергеевич

Студент: Поляков Арсений Андреевич

Группа: НФИбд-01-19

МОСКВА
2022 г.

Прагматика выполнения лабораторной работы

- Требуется разработать приложение позволяющие 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.

Цель работы

Освоить на практике применение режима однократного гаммирования.

Выполнение лабораторной работы

1. Создал функцию позволяющую зашифровывать, расшифровывать данные с помощью сообщения и ключа. А также позволяющую получить ключ.

```
vector<uint8_t> operate(vector<uint8_t> message, vector<uint8_t> key)
{
    if (message.size() != key.size()) {
        return {};
    }

    vector<uint8_t> temp;

    for (int i = 0; i < message.size(); i++) {
        temp.push_back(message[i] ^ key[i]);
    }
    return temp;
}
```

2. Создал функцию для вывода результатов

```
void print_bytes(vector<uint8_t> message)
{
    for (const auto &e : message) {
        cout << hex << unsigned(e) << " ";
    }
    cout << endl;
}
```

3. Определил биты ключей и сообщения

```
vector<uint8_t> key{0x05, 0x0C, 0x17, 0x7F, 0x0E, 0x4E, 0x37, 0xD2, 0x94, 0x10, 0x09, 0x2E, 0x22, 0x57, 0xFF, 0xC8, 0x0B, 0xB2, 0x70, 0x54};
vector<uint8_t> key2{0x05, 0x0C, 0x17, 0x7F, 0x0E, 0x4E, 0x37, 0xD2, 0x94, 0x10, 0x09, 0x2E, 0x22, 0x55, 0xF4, 0xD3, 0x07, 0xBB, 0xBC, 0x54};
vector<uint8_t> message{0xD8, 0xF2, 0xE8, 0xF0, 0xEB, 0xE8, 0xF6, 0x20, 0x2D, 0x20, 0xC2, 0xFB, 0x20, 0xC3, 0xE5, 0xF0, 0xEE, 0xE9, 0x21, 0x2
```

4. Определил главную функцию

```
vector<uint8_t> crypt = operate(message, key);

cout << "Original Message: " << endl;
print_bytes(message);

cout << "Crypted message: " << endl;
print_bytes(crypt);

cout << "Original key: " << endl;
print_bytes(key);

cout << "Get key: " << endl;
print_bytes(operate(message, crypt));

cout << "Decrypted with key2: " << endl;
print_bytes(operate(crypt, key2));
```

5. Запуск программы.

```
Original Message:
d8 f2 e8 f0 eb e8 f6 20 2d 20 c2 fb 20 c3 e5 f0 ee e9 21 21
Crypted message:
dd fe ff 8f e5 a6 c1 f2 b9 30 cb d5 2 94 1a 38 e5 5b 51 75
Original key:
5 c 17 7f e 4e 37 d2 94 10 9 2e 22 57 ff c8 b b2 70 54
Get key:
5 c 17 7f e 4e 37 d2 94 10 9 2e 22 57 ff c8 b b2 70 54
Decrypted with key2:
d8 f2 e8 f0 eb e8 f6 20 2d 20 c2 fb 20 c1 ee eb e2 e0 ed 21
```

Ключ Центра:

05 0C 17 7F 0E 4E 37 D2 94 10 09 2E 22 57 FF C8 0B B2 70 54

Сообщение Центра:

Штирлиц – Вы Герой!!

D8 F2 E8 F0 EB E8 F6 20 2D 20 C2 FB 20 C3 E5 F0 EE E9 21 21

Зашифрованный текст, находящийся у Мюллера:

DD FE FF 8F E5 A6 C1 F2 B9 30 CB D5 02 94 1A 38 E5 5B 51 75

Дешифровальщики попробовали ключ:

05 0C 17 7F 0E 4E 37 D2 94 10 09 2E 22 55 F4 D3 07 BB BC 54

и получили текст:

D8 F2 E8 F0 EB E8 F6 20 2D 20 C2 FB 20 C1 EE EB E2 E0 ED 21

Штирлиц – Вы Болван!

Выводы

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