Лабораторная работа 7

Юдин Герман Станиславович, НФИбд-01-19

Содержание

List of Figures

List of Tables

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №7

дисциплина: Информационная безопасность

Преподователь: Кулябов Дмитрий Сергеевич

Студент: Юдин Герман Станиславович

Группа: НФИбд-01-19

МОСКВА

2022 г.

1 Цель работы

Освоить на практике применение режима однократного гаммирования.

2 Выполнение 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.

Для этого у меня есть функция позволяющая зашифровывать, расшифровывать данные с помощью сообщения и ключа. А также позволяющая получить ключ (Рис fig. 2.1).

```
vector<uint8_t> encrypt(vector<uint8_t> message, vector<uint8_t> key) {
    if (message.size() != key.size()) {
        return {};
    }
    vector<uint8_t> encrypted;
    for (int i = 0; i < message.size(); i ++) {
        encrypted.push_back(message[i]^key[i]);
    }
    return encrypted;
}
```

Figure 2.1: encrypt_fuction

Функция для вывода результатов (Рис fig. 2.2)

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

Figure 2.2: output_prog

Биты сообщения и ключей (Рис fig. 2.3).

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!

Figure 2.3: bytes

Главная функция (Рис fig. 2.4)

```cpp
int main()
{
        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, 0x21};

    vector<uint8_t> crypt = encrypt(message, key);
    cout << "Priginal message: " << endl;
    print_bytes(message);
    cout << "Crypted message: " << endl;
    print_bytes(crypt);
    cout << "Decrypted with correct key: " << endl;
    print_bytes(decrypt(crypt, key));
    cout << "Original key: " << endl;
    print_bytes(key);
    cout << "We get key: " << endl;
    print_bytes(get_key(message, crypt));
    cout << "Decrypted with different key: " << endl;
    print_bytes(decrypt(crypt, key2));
    return 0;
}
```

Figure 2.4: Main

Затем я запускаю программу и сравниваю полученные результаты с тем, что должен был получить в методичке. Видно, что все ключи и закодированные и раскодированные сообщения сошлись (Рис fig. 2.5)

```
[gsyudin@gsyudin Working]$ ./a.out
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
Decrypted with correct key:
d8 f2 e8 f0 eb e8 f6 20 2d 20 c2 fb 20 c3 e5 f0 ee e9 21 21
Original key:
5 c 17 7f e 4e 37 d2 94 10 9 2e 22 57 ff c8 b b2 70 54
We get key:
5 c 17 7f e 4e 37 d2 94 10 9 2e 22 57 ff c8 b b2 70 54
Decrypted with different key:
d8 f2 e8 f0 eb e8 f6 20 2d 20 c2 fb 20 c1 ee eb e2 e0 ed 21
[gsyudin@gsyudin Working]$
```

Figure 2.5: console_output

3 Выводы

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

4 Список литературы

1. Методические материалы курса