

ОТЧЕТ по лабораторной работе №7

дисциплина: Информационная безопасность

Студент: Васильева Юлия

Группа: НФИбд-03-18

МОСКВА 2021г.

Цель работы

Освоить на практике применение режима одноразового гаммирования.

Выполнение лабораторной работы

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.

```
#include <iostream>
#include <cstdlib>
#include <ctime>
#include <vector>

std::vector<uint8_t> generateKey(size_t len);
std::vector<uint8_t> findKey(std::vector<uint8_t> message, std::vector<uint8_t> encrMessage);
std::vector<uint8_t> encrypt(std::vector<uint8_t> message, std::vector<uint8_t> key);

int main() {
    std::vector<uint8_t> message = {"С Новым Годом, друзья!"};

    auto key = generateKey(message.size());
    auto encrMessage = encrypt(message, key);
    auto key2 = findKey(message, encrMessage);

    std::cout << "Message: ";

    for (auto i: message) {
        std::cout << i;
    }

    std::cout << std::endl << "Key: ";

    for (auto i: key) {
        printf("%#x\\t", (uint32_t)i);
    }

    std::cout << std::endl;

    return 0;
}

std::vector<uint8_t> generateKey(size_t len) {
    std::vector<uint8_t> out;

    std::srand(std::time(nullptr));

    for (int i = 0; i < len; i++) {
        out.push_back(std::rand()%(1<<8*sizeof(uint8_t)));
    }

    return out;
}

std::vector<uint8_t> findKey(std::vector<uint8_t> message, std::vector<uint8_t> encrMessage) {
    std::vector<uint8_t> out;

    for (int i = 0; i < message.size(); i++) {
        out.push_back(message[i] ^ encrMessage[i]);
    }

    return out;
}

std::vector<uint8_t> encrypt(std::vector<uint8_t> message, std::vector<uint8_t> key) {
    std::vector<uint8_t> out;

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

    return out;
}
```

```
Message: С Новым Годом, друзья!  
EncrMessage: d7q6a8yG000)01000eV  
Key: 0x6b 0xc5 0x17 0x2f 0xec 0x97 0xdf 0x34 0x41 0x6 0xad 0xa9 0x1 0x67 0x65  
x45 0x68 0xa7 0xa 0xa5 0xad 0xaf 0x2f 0xd0 0xd2 0x24 0x11 0xb1 0xc7 0xe5 0xca  
x32 0xab 0xe1 0x62 0x97 0x78 0x41 0xcb 0xba  
Key2: 0x6b 0xc5 0x17 0x2f 0xec 0x97 0xdf 0x34 0x41 0x6 0xad 0xa9 0x1 0x67 0x65  
x45 0x68 0xa7 0xa 0xa5 0xad 0xaf 0x2f 0xd0 0xd2 0x24 0x11 0xb1 0xc7 0xe5 0xca  
x32 0xab 0xe1 0x62 0x97 0x78 0x41 0xcb 0xba
```

Вывод

Мы освоили на практике применение режима однократного гаммирования.