

Защита лабораторной работы №8

Информационная безопасность

Мальков Р.С

2024

Российский университет дружбы народов, Москва, Россия

Освоить на практике применение режима однократного гаммирования разных текстов одним ключом.

Ход выполнения лабораторной работы

```
#include <random>
#include <iostream>
#include <string>

using namespace std;

string xor_txt_f(string text, string key)
{
    if (text.size() != key.size()) {
        return "Error";
    }
    string encrypted;
    for (int i = 0; i < text.size(); i++)
    {
        char encr_symbol = text[i] xor key[i];
        encrypted.push_back(encr_symbol);
    }
    return encrypted;
}

string generate_key(int len) {
    const string sym = "ABCDEF0123456789";
    random_device random_device;
    mt19937 generator(random_device());
    uniform_int_distribution<> distribution(0, sym.size() - 1);
    string key = "";
    for (int i = 0; i < len; i++)
    {
        key += sym[(distribution(generator))];
    }
    return key;
}
```

Рис. 1: (рис. 1. Программный код приложения, реализующего режим однократного гаммирования)

Ход выполнения лабораторной работы

```
int main()
{
    string word = "This is the test message 1";
    string word2 = "2 is this the test message";
    string key = generate_key(word.size());

    std::cout << "generated key: " << key << "\n";

    string c1 = xor_txt_f(word, key);
    string c2 = xor_txt_f(word2, key);

    std::cout << "encrypted message No1: " << c1 << "\n";
    std::cout << "encrypted message No2: " << c2 << "\n";

    string xored_c1c2 = xor_txt_f(c1, c2);

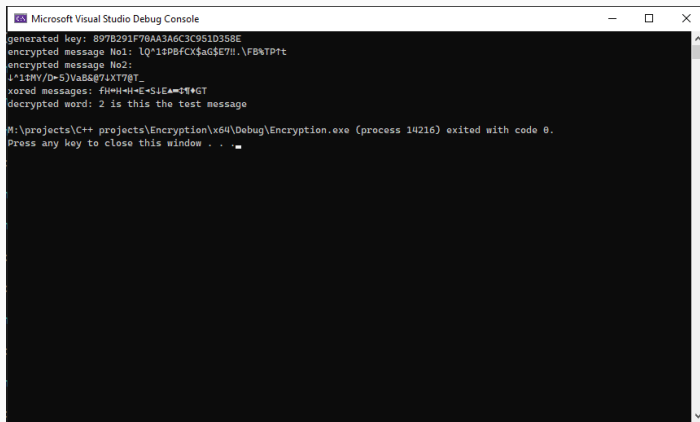
    std::cout << "xored messages: " << xored_c1c2 << "\n";

    string encr_key = xor_txt_f(xored_c1c2, word);

    std::cout << "decrypted word: " << encr_key << "\n";
}
```

Рис. 2: (рис. 2. Программный код приложения, реализующего режим одноратного гаммирования)

Ход выполнения лабораторной работы

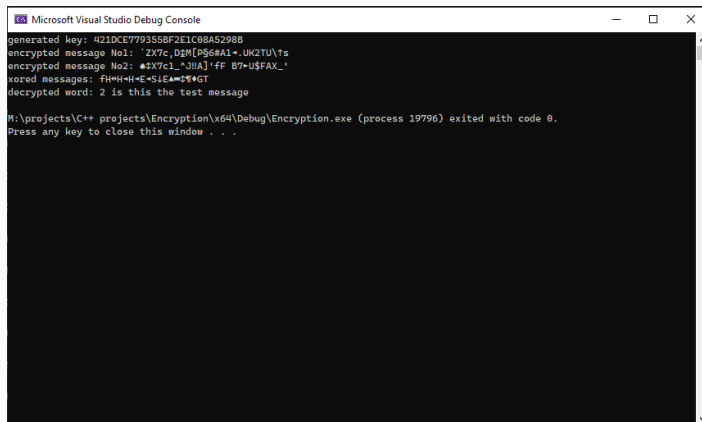


```
Microsoft Visual Studio Debug Console
generated key: 897B291F70AA3A6C3C951D358E
encrypted message No1: lQ*1$PBfCX$aG$E7!!.\FB%TP!t
encrypted message No2:
4^1$MY/D*5)VaB6@74XT7@T_
xored messages: fH*H*H*E*S4E*~$T*GT
decrypted word: 2 is this the test message

M:\projects\C++ projects\Encryption\x64\Debug\Encryption.exe (process 14216) exited with code 0.
Press any key to close this window . . .
```

Рис. 3: (рис. 3. Результат)

Ход выполнения лабораторной работы



```
Microsoft Visual Studio Debug Console
generated key: 421DCE7793558F2E1C08A5298B
encrypted message No1: 'ZX7c,D2M[P$6#A1<.UK2TU\ts
encrypted message No2: 'X7c1_^JHA]'fF B7-U$FAX_'
xored messages: fH*H-H-E-S1E*E*GT
decrypted word: 2 is this the test message

M:\projects\C++ projects\Encryption\x64\Debug\Encryption.exe (process 19796) exited with code 0.
Press any key to close this window . . .
```

Рис. 4: (рис. 4. Результат)

В ходе выполнения данной лабораторной работы было освоено на практике применение режима однократного гаммирования к двум сообщениям.

[0] Методические материалы курса