Лабораторная работа № 7

Дисциплина: Информационная безопасность

Покрас Илья Михайлович

Содержание

Список иллюстраций

1 Цель работы

Целью данной лабораторной работы является освоение на практике применения режима однократного гаммирования.

2 Выполнение лабораторной работы

1. Я добавил нужные библиотеки для дальнейших действий(2.1).

```
#include <iostream>
#include <string>
#include <windows.h>
```

Рис. 2.1: Добавление библиотек

2. Я создал функцию, которая не только шифрует, но и дешифрует текст.

```
std::string encryptdecrypt(std::string text, std::string key)
{
    std::string result;
    int keyLength = key.length();

    for (std::size_t i = 0; i < text.length(); ++i)
    {
        result += text[i] ^ key[i % keyLength];
    }

    return result;
}
```
(**??**).

3. Я создал функцию, которая которая определяет ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста(2.2).

```cpp
std::string findpossiblekeys(std::string text, std::string fragment)
{
    std::string possible_keys;

    for (int i = 0; i <= (int)text.length() - fragment.length(); i++)
    {
        std::string key = "";
        for (int j = 0; j < fragment.length(); j++)
        {
            char c = text[i + j] ^ fragment[j];
            key.push_back(c);
        }

        std::string intact_plaintext = encryptdecrypt(text, key);

        if (intact_plaintext.find(fragment) != std::string::npos){possible_keys += key;}
    }

    return possible_keys;
}
```

Рис. 2.2: Функция определения ключа

4. В int main я создал задание переменных и вызов всех функций(2.3).

```cpp
int main()
{
    SetConsoleCP(1251);
    SetConsoleOutputCP(1251);

    std::string plaintext = "";
    std::string key = "%#2!";
    std::string fragtext;

    std::cout << "Plain text: ";
    std::getline(std::cin, plaintext);

    std::string ciphertext = encryptdecrypt(plaintext, key);
    std::cout << "Encrypted text: " << ciphertext << std::endl;

    std::string decryptedText = encryptdecrypt(ciphertext, key);
    std::cout << "Decrypted text: " << decryptedText << std::endl;

    std::cout << "Plain text fragment: ";
    std::getline(std::cin, fragtext);

    std::string possibleKey = findpossiblekeys(ciphertext, fragtext);

    std::cout << possibleKey;

    return 0;

}
```

Рис. 2.3: Int main

5. Я получил следующий результат(2.4).

```
Plain text: С Новым Годом, друзья!
Encrypted text: фяПЗШЮжНЦПЙЕХРХЭЬ
Decrypted text: С Новым Годом, друзья!
Plain text fragment: С Новым Годом!
%#2!%#2!%#2!%.
```

Рис. 2.4: Результаты работы программы

3 Вывод

В ходе проделанной лабораторной работы я освоил на практике применение режима однократного гаммирования.

Список литературы

[1] https://esystem.rudn.ru/pluginfile.php/2090284/mod_resource/content/2/007-lab_crypto-gamma.pdf