Лабораторная работа № 7

Покрас Илья Михайлович

2023, Москва

Цель работы

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

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

Рис. 1: Добавление библиотек

```cpp
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;
}
```

Рис. 2: Функция шифровка/дешифровки текста

Ход работы

```
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. 3: Функция определения ключа

Ход работы

```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;
}
```

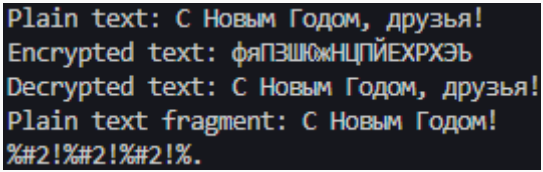

Рис. 5: Результаты работы программы

Вывод

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