Лабораторная работа № 8

Дисциплина: Информационная безопасность

Покрас Илья Михайлович

Содержание

1 Цель работы **4**

2 Выполнение лабораторной работы **5**

3 Вывод **7**

Список литературы **8**

Список иллюстраций

2.1 Добавление библиотек 5
2.2 Функция шифровки текста 5
2.3 Функция дешифровки ключа 5
2.4 Int main 6
2.5 Результаты работы программы 6

1 Цель работы

Целью данной лабораторной работы является освоение на практике применения режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

2 Выполнение лабораторной работы

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

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

Рис. 2.1: Добавление библиотек

2. Я создал функцию, которая шифрует текст(2.2).

```
std::string encrypt(std::string plaintext, std::string key)
{
    std::string ciphertext;
    for (int i = 0; i < plaintext.length(); ++i){ciphertext.push_back(plaintext[i] ^ key[i % key.length()]);}
    return ciphertext;
}
```

Рис. 2.2: Функция шифровки текста

3. Я создал функцию, которая которая дешифрует текст путем вызова функции шифровки, при этом входными данными будут шифротекст и ключ(2.3).

```
std::string decrypt(std::string ciphertext, std::string key){return encrypt(ciphertext, key);}
```

Рис. 2.3: Функция дешифровки ключа

4. В int main я создал задание переменных и вызов всех функций(2.4).

```cpp
int main()
{

    std::string key = "@##?!#";
    std::string P1 = "Plain text 1";
    std::string P2 = "Plain text 2";

    std::string C1 = encrypt(P1, key);
    std::string C2 = encrypt(P2, key);

    std::cout << "Encrypted C1: " << C1 << std::endl;
    std::cout << "Encrypted C2: " << C2 << std::endl;

    std::string decryptedP1 = decrypt(C1, key);
    std::string decryptedP2 = decrypt(C2, key);

    std::cout << "Decrypted text 1: " << decryptedP1 << std::endl;
    std::cout << "Decrypted text 2: " << decryptedP2 << std::endl;

    return 0;
}
```

Рис. 2.4: Int main

5. Я получил следующий результат(2.5).

```
Encrypted C1: OBVO4F[K
Encrypted C2: OBVO4F[K
Decrypted text 1: Plain text 1
Decrypted text 2: Plain text 2
```

Рис. 2.5: Результаты работы программы

3 Вывод

В ходе проделанной лабораторной работы я освоил на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

Список литературы

[1] https://esystem.rudn.ru/pluginfile.php/2090286/mod_resource/content/2/008-lab_crypto-key.pd