Информационная безопасность. Отчет по лабораторной работе №8

Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом

Терентьев Егор Дмитриевич 1032192875

Содержание

List of Figures

List of Tables

1 Цель работы

Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

2 Выполнение лабораторной работы

Два текста кодируются одним ключом (однократное гаммирование). Требуется не зная ключа и не стремясь его определить, прочитать оба текста. Необходимо разработать приложение, позволяющее шифровать и дешифровать тексты P1 и P2 в режиме однократного гаммирования. Приложение должно определить вид шифротекстов C1 и C2 обоих текстов P1 и P2 при известном ключе.

Для этого у меня есть функция позволяющая зашифровывать данные с помощью сообщения и ключа fig. 2.1.

```
vector<uint8_t> encrypt(vector<uint8_t> message, vector<uint8_t> key)
{
    if (message.size() != key.size())
    {
        return {};
    }
    vector<uint8_t> encrypted;
    for (int i = 0; i < message.size(); i++)
    {
        encrypted.push_back(message[i] ^ key[i]);
    }
    return encrypted;
}
```

Figure 2.1: encrypt_fuction

Далее я создал функцию для того, чтобы расщифровывать сообщения с помощью сообщения и ключа fig. 2.2.

```cpp
vector<uint8_t> decrypt(vector<uint8_t> message, vector<uint8_t> key)
{
    if (message.size() != key.size())
    {
        return {};
    }
    vector<uint8_t> decrypted;
    for (int i = 0; i < message.size(); i++)
    {
        decrypted.push_back(message[i] ^ key[i]);
    }
    return decrypted;
}
```

Figure 2.2: decrypt_func

Затем создал функцию получения ключа fig. 2.3.

```cpp
vector<uint8_t> get_key(vector<uint8_t> message, vector<uint8_t> crypt)
{
    if (message.size() != crypt.size())
    {
        return {};
    }
    vector<uint8_t> key;
    for (int i = 0; i < message.size(); i++)
    {
        key.push_back(message[i] ^ crypt[i]);
    }
    return key;
}
```

Figure 2.3: get_key

Создал функцию получения расшифрованного сообщения без ключа fig. 2.4

```cpp
vector<uint8_t> get_message_with_three_pieces(vector<uint8_t> cr1, vector<uint8_t> cr2, vector<uint8_t> msg1)
{
    if (cr1.size() != cr2.size() and cr1.size() != msg1.size())
    {
        return {};
    }
    vector<uint8_t> msg2;
    for (int i = 0; i < cr1.size(); i++)
    {
        msg2.push_back(cr1[i] ^ cr2[i] ^ msg1[i]);
    }
    return msg2;
}
```

Figure 2.4: decrypt_without_key

Остальное в программе отвечает за вывод полученных результатов fig. 2.5

```cpp
void print_bytes(vector<uint8_t> message)
{
    for (const auto& e : message)
    {
        cout << hex << unsigned(e) << "";
    }
    cout << endl;
}

void print_text(vector<uint8_t> message)
{
    string str(message.begin(), message.end());
    cout << str << endl;
}


int main()
{
    string message1 = "hello this is lab 8";
    string message2 = "this lab 8 ab hello";
    vector<uint8_t> first(message1.begin(), message1.end());
    vector<uint8_t> second(message2.begin(), message2.end());

    string keystr = "thisiskeystringlab7";
    vector<uint8_t> key(keystr.begin(), keystr.end());

    vector<uint8_t> crypt1 = encrypt(first, key);
    vector<uint8_t> crypt2 = encrypt(second, key);


    cout << "Original Message number 1: " << endl;
    print_text(first);
    cout << endl << "Original Message number 2: " << endl;
    print_text(second);
    cout << endl << "Crypted message number 1: " << endl;
    print_bytes(crypt1);
    cout << endl << "Crypted message number 2: " << endl;
    print_bytes(crypt2);


    cout << endl <<"Finding message 2:" << endl;
    vector<uint8_t> msg_found = get_message_with_three_pieces(crypt1, crypt2, first);
    print_text(msg_found);
    return 0;
}
```

Figure 2.5: output_prog

Получаю вывод программы, где мы видим, что мы смогли расшифровать сообщение без знаний ключа fig. 2.6

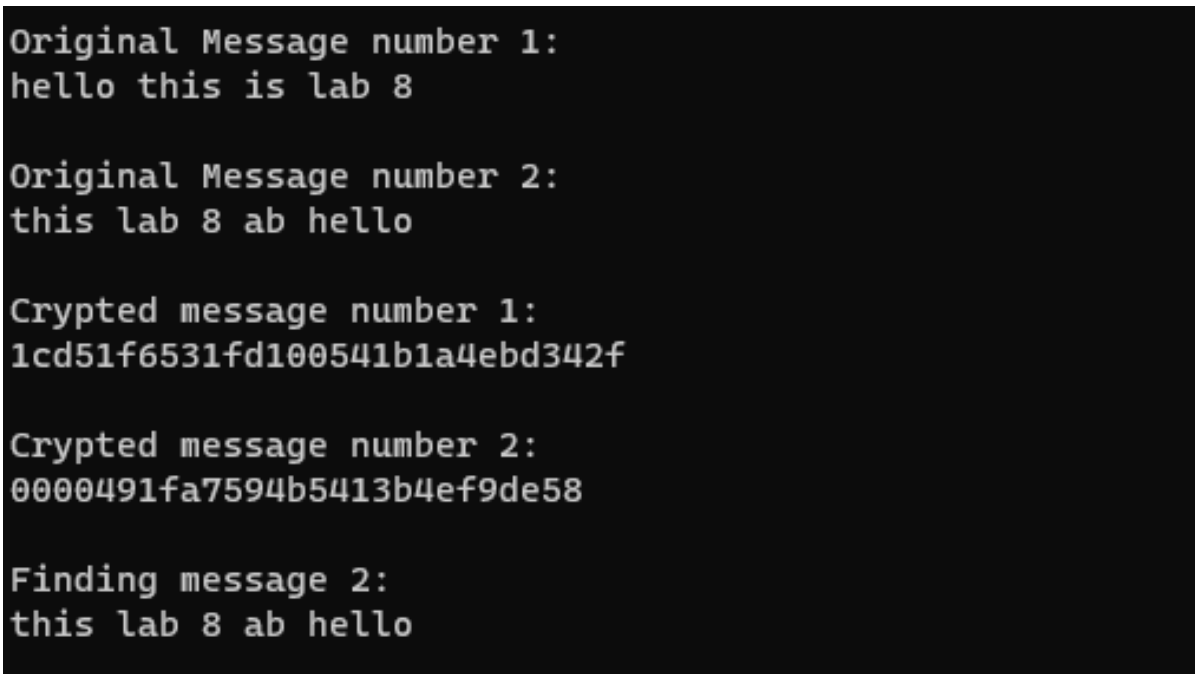

Figure 2.6: console_output

3 Выводы

В результате выполнения работы я освоил на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

4 Список литературы

1. Методические материалы курса