

Лабораторная работа №7

Алли Мохамед Заян - студент группы НКНбд-01-18

08.12.2021

Элементы криптографии.

Однократное гаммирование

Умение пользоваться режимом однократного гаммирования.

Освоить на практике применение режима однократного гаммирования

Написать приложение, которое кодирует и декодирует сообщения с помощью хог-шифра.

Результаты выполнения лабораторной работы. Часть 1

Написал код, шифрующий и дешифрующий сообщение: скриншоты

```

1 //main.cpp
2 #include <iostream>
3 #include <string>
4 #include <string.h>
5 #include <conio.h>
6
7 using namespace std;
8
9 string encrypt(string s, string key){
10     string encrypted;
11
12     encrypted = "";
13
14     for (int i=0; i < s.length(); i++){
15         encrypted += s[i]^key[i];
16     }
17
18     return encrypted;
19 }
20
21 string decrypt(string key, string s){
22     string open_text;
23
24     open_text = "";
25
26     for (int i=0; i < s.length(); i++){
27         open_text += s[i]^key[i];
28     }
29
30     return open_text;
31 }
32
33 int main()
34 {
35     string key = "open.txt";
36     string s = "open.txt";
37
38     string encrypted = encrypt(s, key);
39     string open_text = decrypt(key, encrypted);
40
41     cout << "Encrypted text: " << encrypted << endl;
42     cout << "Decrypted text: " << open_text << endl;
43
44     return 0;
45 }

```

Рис. 1: Код 1

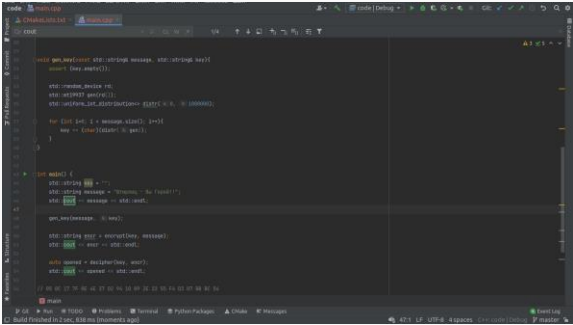


Рис. 2: Код 2

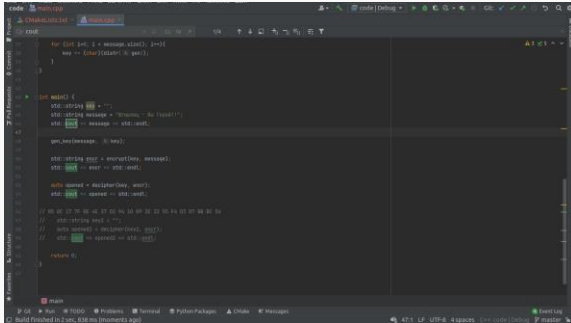
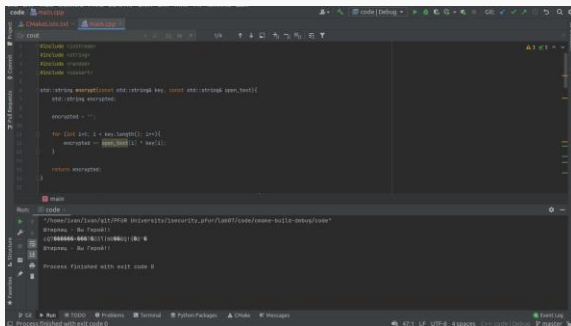


Рис. 3: Код 3

Результат кодировки и декодировки:



```
code
main.cpp
#include <iostream>
#include <string>
#include <vector>
#include <string>

std::string encrypt(const std::string& text, const std::string& key){
    std::string encrypted;

    encrypted = "";

    for (int i=0; i < text.length(); i++){
        encrypted += text[i] ^ key[i];
    }

    return encrypted;
}

int main()
{
    std::string text = "Hello, World!";
    std::string key = "key";
    std::string encrypted = encrypt(text, key);
    std::cout << encrypted << endl;
    return 0;
}
```

Run: code

```
"/home/ivan/ivan/git/2PQR_university/security_pqr/Task7/code/main-built-devs/code"
$ g++ -std=c++11 -c main.cpp -o main.o
$ g++ -std=c++11 -o main main.o
$ ./main
Hello, World!
Process finished with exit code 0
```

Рис. 4: Код 4

Освоил на практике применение режима однократного гаммирования