

# Защита лабораторной работы №7

Информационная безопасность

---

Мальков Р.С

2024

Российский университет дружбы народов, Москва, Россия

- Освоить на практике применение режима однократного гаммирования

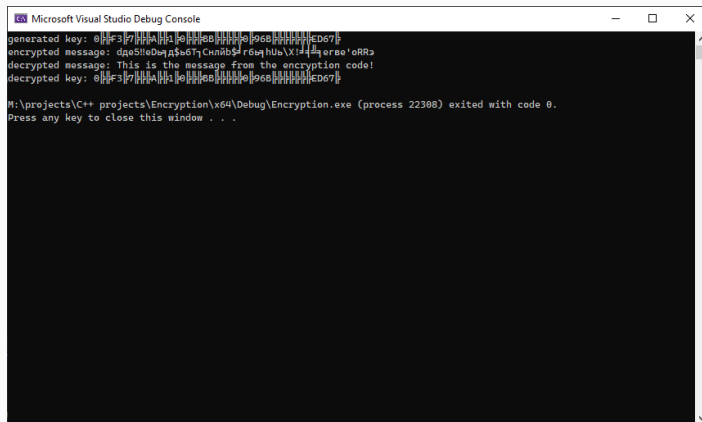
# Ход выполнения лабораторной работы

Для решения задачи написан программный код:

```
7  ~string xor_txt_f(string text, string key)
8  {
9      if (text.size() != key.size()) {
10         return "Error";
11     }
12     string encrypted;
13     for (int i = 0; i < text.size(); i++)
14     {
15         char encr_symbol = text[i] xor key[i];
16         encrypted.push_back(encr_symbol);
17     }
18     return encrypted;
19 }
20
21
22
23 ~string generate_key(int len) {
24     char sym[] = "ABCDEFGHIJKLMNOPQRSTUVWXYZ";
25     string key = "";
26     for (int i = 0; i < len; i++)
27     {
28         key.push_back(sym[(rand() * 100) % len]);
29     }
30     return key;
31 }
32
33 ~int main()
34 {
35     string word = "Happy new year my friends!";
36     string key = generate_key(word.size());
37
38     std::cout << "generated key: " << key << "\n";
39
40     string encrypted = xor_txt_f(word, key);
41
42     std::cout << "encrypted message: " << encrypted << "\n";
43
44     string decrypted = xor_txt_f(encrypted, key);
45
46     std::cout << "decrypted message: " << decrypted << "\n";
47
48     string encr_key = xor_txt_f(decrypted, encrypted);
49
50     std::cout << "decrypted key: " << key << "\n";
51 }
```

**Рис. 1:** (рис. 1. Программный код приложения, реализующего режим однократного гаммирования)

# Результат



```
Microsoft Visual Studio Debug Console
generated key: 0|F3|7|A|1|E|8B|96B|ED67|
encrypted message: dde5!eDьд$e6Tчнлйb$г6яhUь\X!дqерe'oRRэ
decrypted message: This is the message from the encryption code!
decrypted key: 0|F3|7|A|1|E|8B|96B|ED67|

M:\projects\C++ projects\Encryption\x64\Debug\Encryption.exe (process 22308) exited with code 0.
Press any key to close this window . . .
```

Рис. 2: (рис. 2. Результат)

В ходе выполнения данной лабораторной работы было освоено на практике применение режима однократного гаммирования

[0] Методические материалы курса