Лабораторная работа 8

Попов Дмитрий Павлович, НФИбд-01-19

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

ПРЕЗЕНТАЦИЯ ПО ЛАБОРАТОРНОЙ РАБОТЕ №8

дисциплина: Информационная безопасность

Преподователь: Кулябов Дмитрий Сергеевич

Студент: Попов Дмитрий Павлович

Группа: НФИбд-01-19

МОСКВА

2022 г.

Прагматика выполнения лабораторной работы

Прагматика выполнения 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 ; Необходимо определить и выразить аналитически способ, при котором злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить.

Цель работы

Цель работы

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

Выполнение лабораторной работы

1. Создал функцию позволяющую зашифровывать, расшифровывать данные с помощью сообщения и ключа. А также позволяющую получить ключ

1. Создал функцию позволяющую зашифровывать, расшифровывать данные с помощью сообщения и ключа. А также позволяющую получить ключ

```
7   vector<uint8_t> encrypt(vector<uint8_t> message, vector<uint8_t> key)
8   {
9       if (message.size() != key.size())
10      {
11          return {};
12      }
13      vector<uint8_t> encrypted;
14      for (int i = 0; i < message.size(); i++)
15      {
16          encrypted.push_back(message[i] ^ key[i]);
17      }
18      return encrypted;
19  }
```

Figure 1: encrypt_fuction

2. Создал функцию для вывода результатов

2. Создал функцию для вывода результатов

```
49  void print_bytes(vector<uint8_t> message)
50  {
51      for (const auto& e : message)
52      {
53          cout << hex << unsigned(e) << " ";
54      }
55      cout << endl;
56  }
57
58  void print_text(vector<uint8_t> message)
59  {
60      string str(message.begin(), message.end());
61      cout << str << endl;
62  }
```

Figure 2: output_prog

3. Создал функцию определения текста, зная два шифротекста и оригинальный текст одного из них

3. Создал функцию определения текста, зная два шифротекста и оригинальный текст одного из них

```
64  vector<uint8_t> get_message_with_three_pieces(vector<uint8_t> cr1, vector<uint8_t> cr2, vector<uint8_t> msg1)
65  {
66      if (cr1.size() != cr2.size() and cr1.size() != msg1.size())
67      {
68          return {};
69      }
70      vector<uint8_t> msg2;
71      for (int i = 0; i < cr1.size(); i++)
72      {
73          msg2.push_back(cr1[i] ^ cr2[i] ^ msg1[i]);
74      }
75      return msg2;
76  }
```

Figure 3: finding_mess

4. Определил главную функцию

4. Определил главную функцию

```
78  int main()
79  {
80      string message1 = "message1 in the chat";
81      string message2 = "chat have message2 !";
82      vector<uint8_t> first(message1.begin(), message1.end());
83      vector<uint8_t> second(message2.begin(), message2.end());
84
85      string keystr = "ourkeyisthebestworld";
86      vector<uint8_t> key(keystr.begin(), keystr.end());
87
88      vector<uint8_t> crypt1 = encrypt(first, key);
89      vector<uint8_t> crypt2 = encrypt(second, key);
90
91
92      cout << "Original Message number 1: " << endl;
93      print_text(first);
94      cout << endl << "Original Message number 2: " << endl;
95      print_text(second);
96      cout << endl << "Crypted message number 1: " << endl;
97      print_bytes(crypt1);
98      cout << endl << "Crypted message number 2: " << endl;
99      print_bytes(crypt2);
100
101
102     cout << endl <<"Finding message 2:" << endl;
103     vector<uint8_t> msg_found = get_message_with_three_pieces(crypt1, crypt2, first);
104     print_text(msg_found);
105     return 0;
106 }
```

Figure 4: Main

5. Запуск программы

5. Запуск программы

```
[dpopov@dpopov lab8]$ g++ lab8.cpp
[dpopov@dpopov lab8]$ ./a.out
Original Message number 1:
message1 in the chat

Original Message number 2:
chat have message2 !

Crypted message number 1:
2 10 1 18 4 1e c 42 54 1 b 42 11 1b 11 57 c 1a d 10

Crypted message number 2:
c 1d 13 1f 45 11 8 5 11 48 8 7 16 0 15 10 a 40 4c 45

Finding message 2:
chat have message2 !
[dpopov@dpopov lab8]$
```

Figure 5: output_console

6. Способ, при котором злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить:

6. Способ, при котором злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить:

злоумышленник может получить два зашифрованных текста, например, во время передачи информации через сеть. Также если он сможет получить часть оригинального сообщения одного из двух зашифрованных текстов, он сможет прочитать оба текста и без ключа.

Вывод

Вывод

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