

Информационная безопасность. Лабораторная работа № 8 на тему “Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом”

Горбунова Ярослава Михайловна

RUDN University, Moscow, Russian Federation

Содержание

- Цели и задачи
- Выполнение
- Результаты
- Список литературы

Цели и задачи

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

Выполнение

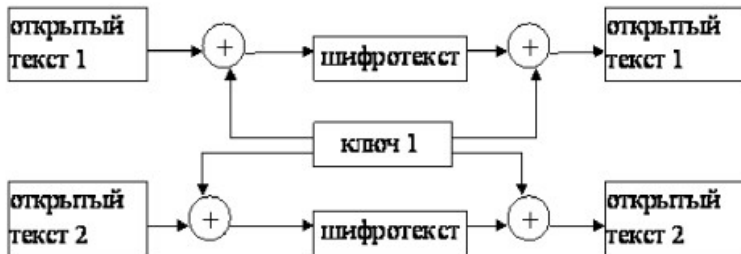


Figure 1: Общая схема шифрования двух различных текстов одним ключом

$$C1 = P1 \sqcap K$$

$$C2 = P2 \sqcap K \quad (8.1)$$

$$C1 \sqcap C2 = P1 \sqcap K \sqcap P2 \sqcap K = P1 \sqcap P2$$

$$C1 \sqcap C2 \sqcap P1 = P1 \sqcap P2 \sqcap P1 = P2 \quad (8.3)$$


```
1  /*
2  Gorbunova Y.M., NFI-01-19, 2022
3  ...
4  Single ganning
5  Principle:
6  1) text ^ gamma = ciphertext;
7  2) ciphertext ^ gamma = text;
8  3) gamma = ciphertext ^ text;
9  where "^" is additions modulo 2 (XOR)
10 ...
11 ciphertext_1 = text_1 ^ gamma
12 ciphertext_2 = text_2 ^ gamma
13 ...
14 4) ciphertext_1 ^ ciphertext_2 ^ text_1 = text_2
15    ciphertext_1 ^ ciphertext_2 ^ text_2 = text_1
16 */
17
18
19 #include <iostream>
20 #include <string>
21 #include <cstring>
22 #include <bitset>
23
24 using namespace std;
25
26 const int m = 1024; // array dimension
27 const int n = 8; // bitset dimension
28
29 // Print for unmodified text
30 void print_bitset_text(char arr[]) {
31     for (unsigned int i = 0; i < strlen(arr); i++)
32         cout << bitset<n>((unsigned char)arr[i]) << " ";
33 }
34
```

Figure 2: Программа (1)

```
35 // Print for modified text
36 void print_bitset_gamma(char arr[], char text[]) {
37     for (unsigned int i = 0; i < strlen(text); i++)
38         cout << bitset<n>((unsigned char)arr[i]) << " ";
39 }
40
41 int main()
42 {
43     // Introduce variables
44     //char text_1[m] = "НаВашисходящийот1204";
45     char text_1[m] = "NaVasishodysiyot1204";
46     //char text_2[m] = "ВСеверныйфилиалБанка";
47     char text_2[m] = "VSevernyifilialBanka";
48     int gam[m] = {
49         0x05, 0x0C, 0x17, 0x7F, 0x0E, 0x4E, 0x37, 0xD2, 0x94, 0x10,
50         0x09, 0x2E, 0x22, 0x57, 0xFF, 0xC8, 0x0B, 0xB2, 0x70, 0x54
51     }; // given key (int)
52     char gamma[m]; // key (char)
53     char gam_text_1[1024], gam_text_2[1024]; // ciphertexts
54
55     // Convert from integer to char
56     for (unsigned int i = 0; i < size(gam); i++) {
57         gamma[i] = (char)gam[i];
58     }
59
60     cout << "-----" << endl << "Part 1" << endl;
61
62     cout << "    Bitset of the key (gamma) :\n";
63     print_bitset_text(gamma);
64     cout << endl;
65
66     // Text 1
67     cout << "    Text 1 for single gamming: \n" << text_1 << endl;
68 }
```

Figure 3: Программа (2)

```
69      cout << "    Bitset of the Text 1 :\n";
70      print_bitset_text(text_1);
71      cout << endl;
72
73      cout << "    Ciphertext computation...\n";
74
75      // Convert text to ciphertext
76      for (unsigned int i = 0; i < strlen(text_1); i++) {
77          gam_text_1[i] = text_1[i] ^ gamma[i];
78      }
79      cout << "    Bitset of the Ciphertext (gam_text_1) :\n";
80      print_bitset_gamma(gam_text_1, text_1);
81      cout << endl;
82
83      // Text 2
84      cout << "    Text 2 for single garming: \n" << text_2 << endl;
85
86      cout << "    Bitset of the Text 2 :\n";
87      print_bitset_text(text_2);
88      cout << endl;
89
90      cout << "    Ciphertext computation...\n";
91
92      // Convert text to ciphertext
93      for (unsigned int i = 0; i < strlen(text_2); i++) {
94          gam_text_2[i] = text_2[i] ^ gamma[i];
95      }
96      cout << "    Bitset of the Ciphertext (gam_text_2) :\n";
97      print_bitset_gamma(gam_text_2, text_2);
98
99      cout << endl;
100     cout << "-----" << endl;
101     cout << endl << "-----" << endl << "Part 2" << endl;
102
```

Figure 4: Программа (3)

```
103 cout << "    1) Accept Text 2 is unknown. Define Text 2 via cybertext 1, cybertest 2 and Test 1: \n";
104 cout << "    Text 2 computation...\n";
105 // Define text_2
106 cout << "    Check of correct computation work...\n    Obtained Text 2 after single gamming" << endl;
107 for (unsigned int i = 0; i < strlen(text_1); i++) {
108     cout << static_cast<char>(bitset<n>((unsigned char)(gam_text_1[i] ^ gam_text_2[i] ^ text_1[i])).to_ulong() + 256);
109 }
110 cout << endl;
111
112 cout << "    2) Accept Text 1 is unknown. Define Text 1 via cybertext 1, cybertest 2 and Test 2: \n";
113 cout << "    Text 1 computation...\n";
114 // Define text_2
115 cout << "    Check of correct computation work...\n    Obtained Text 1 after single gamming" << endl;
116 for (unsigned int i = 0; i < strlen(text_2); i++) {
117     cout << static_cast<char>(bitset<n>((unsigned char)(gam_text_1[i] ^ gam_text_2[i] ^ text_2[i])).to_ulong() + 256);
118 }
119 cout << endl << "-----" << endl;
120
121
```

Figure 5: Программа (4)

```
-----
Part 1
  Bitset of the key (gamma) :
00000101 00001100 00010111 01111111 00001110 01001110 00110111 11010010 10010100 00010000 00001001 00101110 00100010 01010111 11111111 11001000 00001011 10110010 01110000 01010100
  Text 1 for single ganning:
NoVasishodysiyot1204
  Bitset of the Text 1 :
01001110 01100001 01010110 01100001 01100011 01101001 01110011 01101000 01101111 01001000 01110001 01110011 01101001 01111001 01101111 01101000 00110010 00110000 00110100
  Ciphertext computation...
  Bitset of the Ciphertext (gam_text_1) :
01001011 01101101 01000001 00011110 01111101 00100111 01000100 10111010 11111011 01110100 01110000 01011101 01001011 00101110 10010000 10111100 00111010 10000000 01000000 01100000
  Text 2 for single ganning:
VSevernyifilialBanka
  Bitset of the Text 2 :
01010110 01010011 01100101 01101010 01100101 01110010 01101110 01111001 01101001 01100110 01101001 01101100 01101001 01100001 01101100 01000010 01100001 01101110 01101011 01100001
  Ciphertext computation...
  Bitset of the Ciphertext (gam_text_2) :
01010011 01011111 01110010 00010001 01101011 00111100 01011001 10101011 11111101 01110110 01100000 01000010 01001011 00110110 10010011 10001010 01101010 11011100 00011011 00110101
-----
Part 2
  1) Accept Text 2 is unknown. Define Text 2 via cybertext 1, cybertest 2 and Text 1:
  Text 2 computation...
  Check of correct computation work...
  Obtained Text 2 after single ganning
VSevernyifilialBanka
  2) Accept Text 1 is unknown. Define Text 1 via cybertext 1, cybertest 2 and Text 2:
  Text 1 computation...
  Check of correct computation work...
  Obtained Text 1 after single ganning
NoVasishodysiyot1204
-----
```

Figure 6: Вывод работы программы

Результаты

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

Список литературы

1. Методические материалы курса