

# **Отчет по лабораторной работе 8**

Дисциплина: Информационная безопасность

---

Дяченко Злата Константиновна, НФИбд-03-18

# Прагматика выполнения лабораторной работы

Данная лабораторная работа выполнялась мной для приобретения теоретических знаний и практических навыков применения однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

## Цель выполнения лабораторной работы

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

# Задачи выполнения лабораторной работы

Осуществить шифрование и дешифрование текстов P1 и P2 в режиме однократного гаммирования. (рис. 1).

```
P1
205 224 194 224 248 232 241 245 238 228 255 249 232 233 238 242 49 50 48 52
P2
194 209 229 226 229 240 237 251 233 244 232 235 232 224 235 193 224 237 234 224
Шифротекст C1:
200 236 213 159 246 166 198 39 122 244 246 215 202 190 17 58 58 128 64 96
Шифротекст C2:
199 221 242 157 235 190 218 41 125 228 225 197 202 183 20 9 235 95 154 180
Дешифрованный текст P1:
205 224 194 224 248 232 241 245 238 228 255 249 232 233 238 242 49 50 48 52
Дешифрованный текст P2:
194 209 229 226 229 240 237 251 233 244 232 235 232 224 235 193 224 237 234 224
```

**Figure 1:** Открытый текст и шифротекст

# Задачи выполнения лабораторной работы

```
1  #include <iostream>
2  #include <string>
3  #include <math.h>
4  #include <iomanip>
5  #include <ctime>
6  #include <stdlib.h>
7  using namespace std;
8
9
10
11 void convert(string letter, int array[])
12 {
13     for (int i = 0; i < letter.length(); i++)
14     {
15         unsigned char x = letter.at(i);
16         array[i] = int(x);
17     }
18 }
19
20
21 void printM(int array[], int len){
22     for (int j = 0; j < len; j++) {
23         cout << setw(4) << array[j];
24     }
25     cout<<endl;
26 }
27
28 void gammir(int text[], int key[], int len, int shifrotext[]){
29     for (int i=0; i<len; i++){
30         shifrotext[i]=text[i]^key[i];
31     }
32 }
33
34 void poisk(int c1[], int c2[], int len1, int p1[], int p2[]){
35     for (int i=0; i<len1; i++){
36         p2[i]=c1[i]^c2[i]^p1[i];
37     }
38 }
```

Figure 2: Функции программы

# Задачи выполнения лабораторной работы

```
40 int main(){
41     setlocale(LC_ALL, "Russian");
42     string p1,p2;
43     int len1;
44     p1="НаВашисходящийот1204";
45     p2="ВСеверныйфилиалБанка";
46     len1=p1.size();
47     int s1[len1], s2[len1];
48     convert(p1, s1);
49     convert(p2,s2);
50     cout<<"P1"<<endl;
51     printM(s1, len1);
52     cout<<"P2"<<endl;
53     printM(s2, len1);
54
55     int K[len1];
56     K[0]=0x05;
57     K[1]=0x0C;
58     K[2]=0x17;
59     K[3]=0x7F;
60     K[4]=0x0E;
61     K[5]=0x4E;
62     K[6]=0x37;
63     K[7]=0xD2;
64     K[8]=0x94;
65     K[9]=0x10;
66     K[10]=0x09;
67     K[11]=0x2E;
68     K[12]=0x22;
69     K[13]=0x57;
70     K[14]=0xFF;
71     K[15]=0xC8;
72     K[16]=0x0B;
73     K[17]=0x82;
74     K[18]=0x70;
75     K[19]=0x54;
76
77     int c1[len1], c2[len1];
78     gammir(s1, K, len1, c1);
79     cout<<"Шифротекст C1:"<<endl;
80     printM(c1, len1);
81     gammir(s2, K, len1, c2);
82     cout<<"Шифротекст C2:"<<endl;
83     printM(c2, len1);
```

# Задачи выполнения лабораторной работы

```
84  
85     int d1[len1],d2[len1];  
86     gammir(c1, K, len1, d1);  
87     cout<<"Дешифрованный текст P1:"<<endl;  
88     printM(d1, len1);  
89     gammir(c2, K, len1, d2);  
90     cout<<"Дешифрованный текст P12:"<<endl;  
91     printM(d2, len1);  
92
```

**Figure 4:** Функция main. Дешифрование

## Задачи выполнения лабораторной работы

Определить и выразить аналитически способ, при котором злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить (рис. 5).

```
92  
93     int p22[len1];  
94     poisk(c1,c2,len1,s1,p22);  
95     cout<<"Прочитанный P2:"<<endl;  
96     printM(p22, len1);  
97  
98 }
```

**Figure 5:** Получение текста



# Задачи выполнения лабораторной работы

```
P2
194 209 229 226 229 240 237 251 233 244 232 235 232 224 235 193 224 237 234 224
Шифротекст C1:
200 236 213 159 246 166 198 39 122 244 246 215 202 190 17 58 58 128 64 96
Шифротекст C2:
199 221 242 157 235 190 218 41 125 228 225 197 202 183 20 9 235 95 154 180
Дешифрованный текст P1:
205 224 194 224 248 232 241 245 238 228 255 249 232 233 238 242 49 50 48 52
Дешифрованный текст P12:
194 209 229 226 229 240 237 251 233 244 232 235 232 224 235 193 224 237 234 224
Прочитанный P2:
194 209 229 226 229 240 237 251 233 244 232 235 232 224 235 193 224 237 234 224
```

Figure 6: Результат

## Результаты выполнения лабораторной работы

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