

Презентация по лабораторной работе №8

Калинин Тимур Дмитриевич

РУДН

Цель работы

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

Выполнение лабораторной работы

Код программы шифрования

```
1  #include <stdio.h>
2  #include <stdlib.h>
3  #include <string.h>
4
5
6  char* encryptor(char* original_str, char* key, int length){
7      char* encrypted_str = (char *)malloc(length*sizeof(char));
8      int i;
9      for(i=0; i<length; i++){
10         encrypted_str[i] = (char)(original_str[i] ^ key[i]);
11     }
12     return encrypted_str;
13 }
14
15 int main(){
16     int length = 64;
17     char p1[length];
18     char p2[length];
19     char key[length];
20
21     printf("Введите текст P1: ");
22     fgets(p1, length, stdin);
23     printf("Введите текст P2: ");
24     fgets(p2, length, stdin);
25     printf("Введите ключ: ");
26     fgets(key, length, stdin);
27
28     char *c1 = encryptor(p1, key, length);
29     printf("Шифрованный текст C1: %s\n", c1);
30
31     char *c2 = encryptor(p2, key, length);
32     printf("Расшифрованный текст: %s\n", c2);
33
34     return 0;
35 }
```

Проверка работы программы шифрования

```
[tdkalinin@tdkalinin lab08]$ gcc decryptor.c -o decryptor
[tdkalinin@tdkalinin lab08]$ ./decryptor
Введите текст P1: This is message 1
Введите текст P2: This is message 2
Введите ключ: 000540346023421
Шифрованный текст C1: dXYFY@[UA@UUT*1

Шифрованный текст C2: dXYFY@[UA@UUT*2

[tdkalinin@tdkalinin lab08]$
```

Figure 2: Работа программы decryptor

Итог

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