Презентация по лабораторной работе №7

Калинин Тимур Дмитриевич

РУДН

Цель работы

Цель работы

Освоить на практике применение режима однократного гаммирования.

Выполнение лабораторной работы

Выполнение лабораторной работы

Освоить на практике применение режима однократного гаммирования.

Код программы шифрования

lab07 > C encryptor.c

```c
#include <stdio.h>
#include <stdlib.h>
#include <string.h>


char* encryptor(char* original_str, char* key, int length){
    char* encrypted_str = (char *)malloc(length*sizeof(char));
    int i;
    for(i=0; i<length; i++){
        encrypted_str[i] = (char)(original_str[i] ^ key[i]);
    }
    return encrypted_str;
}

int main(){
    int length = 64;
    char initial_string[length];
    char key[length];

    printf("Введите строку: ");
    fgets(initial_string, length, stdin);
    printf("Введите ключ: ");
    fgets(key, length, stdin);

    char *encrypted_str = encryptor(initial_string, key, length);
    printf("Шифрованный текст: %s\n", encrypted_str);

    char *decrypted_str = encryptor(encrypted_str, key, length);
    printf("Расшифрованный текст: %s\n", decrypted_str);
    free(encrypted_str);

    return 0;
}
```

Figure 1: Код encryptor.c

Код программы нахождения ключа

lab07 > C key_finder.c

```c
#include <stdio.h>
#include <stdlib.h>
#include <string.h>


char* encryptor(char* original_str, char* key, int length){
    char* encrypted_str = (char *)malloc(length*sizeof(char));
    int i;
    for(i=0; i<length; i++){
        encrypted_str[i] = (char)(original_str[i] ^ key[i]);
    }
    return encrypted_str;
}

int main(){
    int length = 64;
    char initial_string[length];
    char key[length];

    printf("Введите строку: ");
    fgets(initial_string, length, stdin);
    printf("Введите зашифрованную строку: ");
    fgets(key, length, stdin);

    char *encrypted_str = encryptor(initial_string, key, length);
    printf("Ваш ключ: %s\n", encrypted_str);

    free(encrypted_str);

    return 0;
}
```

Figure 2: Код key_finder.c

Проверка работы программы шифрования

```
[tdkalinin@tdkalinin lab07]$ ./encryptor
Введите строку: Happy new year, friends!
Введите ключ: 00000000000000000000000000
Шифрованный текст: xQ@@I^UGIUQBVBYU^TC:0

Расшифрованный текст: Happy new year, friends!
```

Figure 3: Работа программы encryptor

Проверка работы программы нахождения ключа

```
[tdkalinin@tdkalinin lab07]$ ./key_finder
Введите строку: Happy new year, friends!
Введите зашифрованную строку: vxz^fgasdfg230432vasd
Ваш ключ: >
.GFWRBT
ns!
```

Figure 4: Работа программы key_finder

Итог

Итог

Мы освоили на практике применение режима однократного гаммирования.