Отчёт по лабораторной работе №8

Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом

Тимур Дмитриевич Калинин

Содержание

List of Figures

List of Tables

1 Цель работы

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

2 Выполнение лабораторной работы

1. Напишем программу decryptor.c, которая будет выводить два шифротекста по известным текстам и ключу. (Рис. 2.1)

```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 p1[length];
    char p2[length];
    char key[length];

    printf("Введите текст P1: ");
    fgets(p1, length, stdin);
    printf("Введите текст P2: ");
    fgets(p2, length, stdin);
    printf("Введите ключ: ");
    fgets(key, length, stdin);

    char *c1 = encryptor(p1, key, length);
    printf("Шифрованный текст C1: %s\n", c1);

    char *c2 = encryptor(p2, key, length);
    printf("Расшифрованный текст: %s\n", c2);

    return 0;
}
```

Figure 2.1: Код decryptor.c

2. Проверим работу программы decryptor (Рис. 2.2)

```
[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 2.2: Работа программы decryptor

3 Контрольные вопросы

1. Как, зная один из текстов (P1 или P2), определить другой, не зная при этом ключа?

Применить операцию “исключающее или” к первому шифротексту, второму шифротексту и известному тексту.

2. Что будет при повторном использовании ключа при шифровании текста?

Получится исходный текст.

3. Как реализуется режим шифрования однократного гаммирования одним ключом двух открытых текстов?

Один и тот же ключ применяется для двух текстов.

4. Перечислите недостатки шифрования одним ключом двух открытых текстов.

Если злоумышленник узнает некий шаблон текста, то по нему он может попробовать прочитать сообщение.

5. Перечислите преимущества шифрования одним ключом двух открытых текстов.

Не требуется использовать несколько различных ключей.

4 Выводы

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

5 Библиография

1. Лабораторная работа №8. - 3 с. URL: https://esystem.rudn.ru/pluginfile.php/1651895/mod_resource/content/2/008-lab_crypto-key.pdf