Презентация Лабораторной работы №7

По дисциплине Информационная безопасность

Прокошев Н.Е.

21 октября 2023

Информация

Докладчик

- Прокошев Никита Евгеньевич
- студент НФИбд-02-20
- Факультет Физико-Математических и Естественных наук
- Российский университет дружбы народов
- 1032202460@rudn.ru
- https://github.com/neprokoshev

Вводная часть

Цели и задачи

Цель: Освоить на практике применение режима однократного гаммирования.

Выполнение лабораторной работы

1. Создаём файл lab7.c (@pic:001).

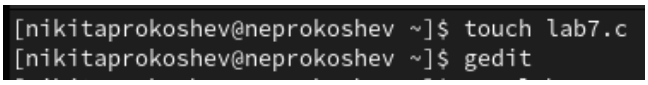

Рис. 1: Создаём файл lab7.c.

2. Пишем код для создания ключа, шифровки и дешифровки на языке с (@pic:002).
3. Компилируем и запускаем программу (@pic:003).

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

void encrypt (char* plaintext, char* key) {
        int plaintextLength = strlen(plaintext);
        int keyLength = strlen(key);

        for (int i = 0; i < plaintextLength; i++) {
                char encryptedChar = plaintext[i] ^ key[i % keyLength];
                plaintext[i] = encryptedChar;
        }
}

void decrypt (char* ciphertext, char* key) {
        int ciphertextLength = strlen(ciphertext);
        int keyLength = strlen(key);

        for (int i = 0; i < ciphertextLength; i++) {
                char decryptedChar = ciphertext[i] ^ key[i % keyLength];
                ciphertext[i] = decryptedChar;
        }
}

char* generateKey(const char* word) {
        srand(time(NULL));
        char* key = (char*)malloc((strlen(word)+1) * sizeof(char));
        int i;

        for (i = 0; word[i] != '\0';i++) {
                int hexDigit = rand() & 16;
                sprintf(&key[i], "%X", hexDigit);
        }
        key[i] = '\0';

        return key;
}

int main() {
        char plaintext[] = "С Новым Годом, друзья!";
        char *key = generateKey(plaintext);
        printf("Plaintext: %s\n", plaintext);
        printf("Key: %s\n", key);

        encrypt(plaintext, key);
        printf("Encrypted Text: %s\n", plaintext);

        decrypt(plaintext, key);
        printf("Decrypted Text: %s\n", plaintext);

        free(key);

        return 0;
}
```

Рис. 2: Код на языке C.

```
[nikitaprokoshev@neprokoshev ~]$ gcc lab7.c -o lab7
[nikitaprokoshev@neprokoshev ~]$ ./lab7
Plaintext: С Новым Годом, друзья!
Key: 11000111010001110110001000001011011110 0
Encrypted Text: ◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆
Decrypted Text: С Новым Годом, друзья!
```

Рис. 3: Запускаем программу.

Выводы

В ходе данной лабораторной работы удалось освоить на практике применение режима однократного гаммирования.

:::