

Отчёт Лабораторной работы №7

По дисциплине Информационная безопасность

Прокошев Никита Евгеньевич

Содержание

Цель работы	5
Выполнение лабораторной работы	6
Выводы	9
Список литературы	10

Список таблиц

Список иллюстраций

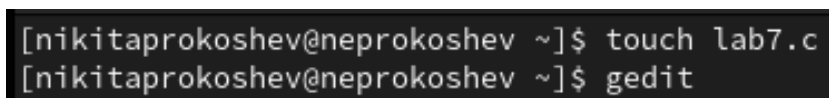
1	Создаём файл lab7.c.	6
2	Код на языке С.	7
3	Запускаем программу.	8

Цель работы

Цель: Освоить на практике применение режима однократного гаммирования.

Выполнение лабораторной работы

1. Создаём файл lab7.c (@pic:001).

A terminal window with a dark background. The prompt is [nikitaprokoshev@neprosheev ~]\$. The first command is touch lab7.c and the second is gedit. Both commands are followed by a new line.

```
[nikitaprokoshev@neprosheev ~]$ touch lab7.c
[nikitaprokoshev@neprosheev ~]$ gedit
```

Рис. 1: Создаём файл lab7.c.

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

```

#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.

3. Компилируем и запускаем программу (@pic:003).

```
[nikitaprokoshev@neprokoshev ~]$ gcc lab7.c -o lab7
[nikitaprokoshev@neprokoshev ~]$ ./lab7
Plaintext: С Новым Годом, друзья!
Key: 110001110100011101100010000010110111100
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.

Список литературы