Донецький Національний Технічний Університет

Лабораторна робота № 8

«Дослідження програмних реалізацій з застосуванням динамічного методу»

Виконав:

ст. групи ІПЗІм -17

Лисенко А. С.

Перевірила:

доцент каф. ПМІ

Маслова Н. О.

Покровськ 2017

Вариант 9

Для дизассемблирования буду использовать программу которая генерирует шифрованное сообщение по ключу (ключ генерируется случайно), а также дешифрует его, алгоритм работы шифрования представлен ниже

for (int i = 0; i < strlen(mess); i++) {

int gidit = key[i % 10] - '0';

mess[i] += gidit;

if (mess[i] == 0x20)

mess[i] = 0x2F;

}

Алгоритм работы дешифрования:

for (int i = 0; i < strlen(mess); i++) {

if (mess[i] == 0x2F)

mess[i] = 0x20;

int gidit = key[i % 10] - '0';

mess[i] -= gidit;

}

Для начала найдём функцию, которая выполняет шифрование и дешифрование, это делаем с помощью нахождения функций по строкам в программе IDA Pro 6.8. Для отображении функции по строкам нажимаем сочетание клавиш shift + f12



Рис. 1 – Функция шифрования и дешифрования

Далее переходим в эту функцию с помощью левой кнопки мыши, поднимаемся выше, ищем заголовок этой функции находим, нажимаем клавишу f5 переходим в режим псевдокода, скриншоты сравнения представлены ниже

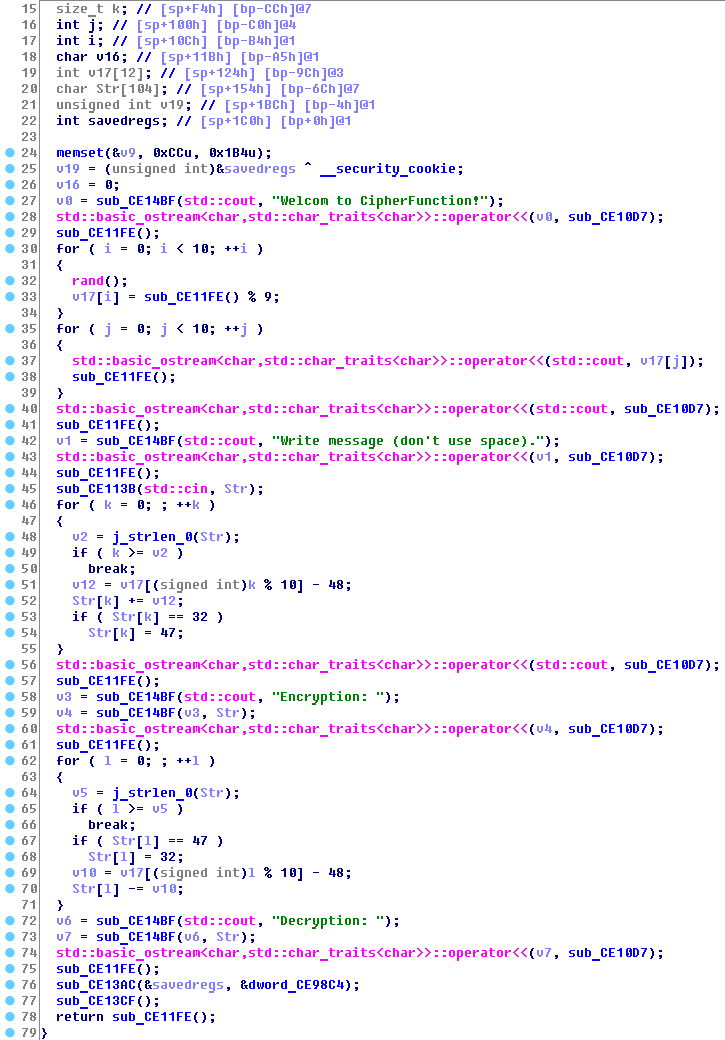


Рис. 2 – Псевдокод функции int сipherFunction()

Здесь мы можем заметить int sub\_CE95C0() – это название функции, далее можем увидеть цикл for(), где происходит генерация ключа, а затем по очереди идут алгоритмы шифрования и дешифрования сообщения.

Для того чтобы найти главную функцию мы переходим с помощью сочетания клавиш ctrl + x в заголовок int cipherFunction(), затем выбираем вид главной панели Graph overview, с помощью правой кнопки мыши, затем проходим по функции которая подсвечивается зеленым цветом, через ctrl + x и попадаем в главную функцию int main(), псевдокод представлен ниже

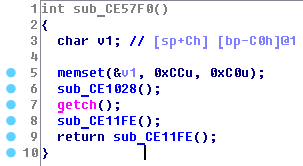


Рис. 3 – Псевдокод функции int main()

Далее переходим в функцию sub\_CE1028() и видим что эта функция возвращает значение функции int сipherFunction()

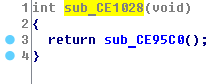


Рис. 4 – Псевдокод возвращение функции int сipherFunction()

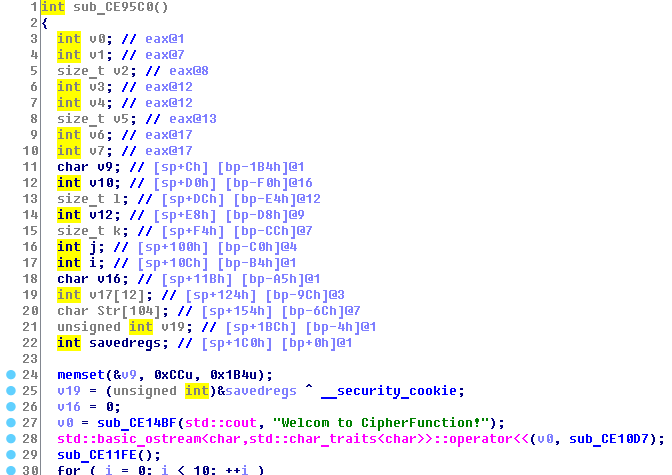


Рис. 5 – Псевдокод функции int сipherFunction()



Рис. 6 – Скриншот работы программы через IDA Pro Debugger

Листинг программы

Код на С++

#include <iostream>

#include <conio.h>

using namespace std;

int cipherFunctuion() {

char mess[100];

int key[10];

char flag = 0;

cout << "Welcom to CipherFunction!" << endl;

for(int i = 0; i < 10; i++)

key[i] = 0 + rand() % 9;

for (int i = 0; i < 10; i++)

cout << key[i];

cout << endl;

cout << "Write message (don't use space)." << endl;

cin >> mess;

for (int i = 0; i < strlen(mess); i++) {

int gidit = key[i % 10] - '0';

mess[i] += gidit;

if (mess[i] == 0x20)

mess[i] = 0x2F;

}

cout << endl;

cout << "Encryption: " << mess << endl;

for (int i = 0; i < strlen(mess); i++) {

if (mess[i] == 0x2F)

mess[i] = 0x20;

int gidit = key[i % 10] - '0';

mess[i] -= gidit;

}

cout << "Decryption: " << mess << endl;

return 0;

}

int main() {

cipherFunctuion();

\_getch();

return 0;

}