NJCTF-easy_crypto writeup

原创

qq_33528164 于 2017-03-14 23:09:32 发布 1222 收藏

文章标签： 加密 算法 压缩

上个星期天和队友一起玩了一把CTF，虽然真正做出来的只有一道题。其他就是一起出主意。

下面的是easy_crypto的writeup。

easy_crypto的附件是一个压缩包。包中有四个文件，Cipher.txt encrypt.c flag.txt plain.txt。其中Cipher.txt是plain.txt加密后的文件。

加密算法是encrypt.c。而flag.txt是明文加密后的文件，只要我们解密出来这个文件即可得出flag。

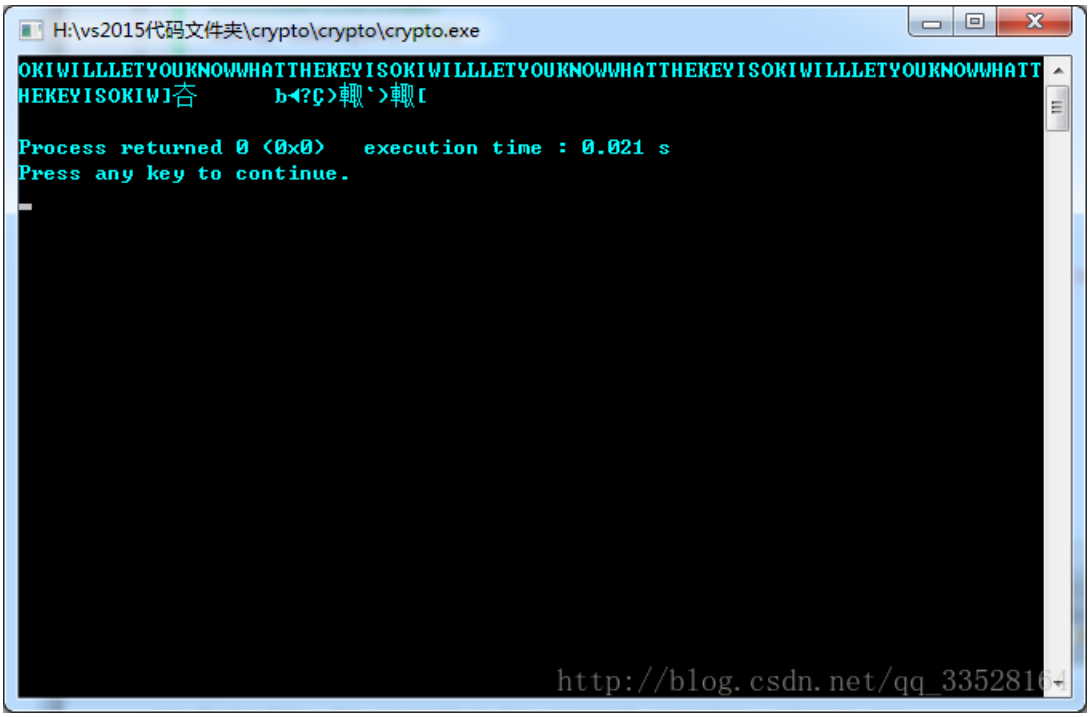
下面给出加密算法：

```c
#include <stdlib.h>
#include <stdio.h>
#include <string.h>
int main(int argc, char **argv)
{
    if (argc != 3)
    {
        printf("USAGE: %s input_file output_file\n", argv[0]);
        return 0;
    }
    FILE* input_file  = fopen(argv[1], "rb");
    FILE* output_file = fopen(argv[2], "wb");
    if (!input_file || !output_file)
    {
        printf("Error\n");
        return 0;
    }
    char key[] = "XXXXXXXXXXXX";
    char p, t, c = 0;
    int i = 0;
    while ((p = fgetc(input_file)) != EOF)
    {

        c = ((key[i % strlen(key)] ^ t) + (p-t) + i*i ) & 0xff;
        t = p;
        i++;
        fputc(c, output_file);
    }
    return 0;
}
```

但是观察得出key不知道是多少？这时候，题目给的Cipher.txt ， plain.txt就起到作用了，通过这两个文件来得出key。

下面给出代码。

```cpp
#include <stdlib.h>
#include <stdio.h>
#include <string.h>
#include<iostream>
using namespace std;

int main()
 {
    FILE* input_file  = fopen("plain.txt", "rb");
    FILE* output_file = fopen("cipher.txt", "rb");
    char key[100];
    char p, t, c = 0;
    int i = 0;
    while ((p = fgetc(input_file)) != EOF&&(c = fgetc(output_file))!=EOF)
    {
        key[i]=(c -((p-t) + i*i ))^t;
        t = p;
        i++;
    }
    cout<<key<<endl;
    return 0;
}
```



字符串如下：

OKIWILLLETYOUKNOWWHATTHEKEYIS

OKIWILLLETYOUKNOWWHATTHEKEYIS

OKIWILLLETYOUKNOWWHATTHEKEYIS

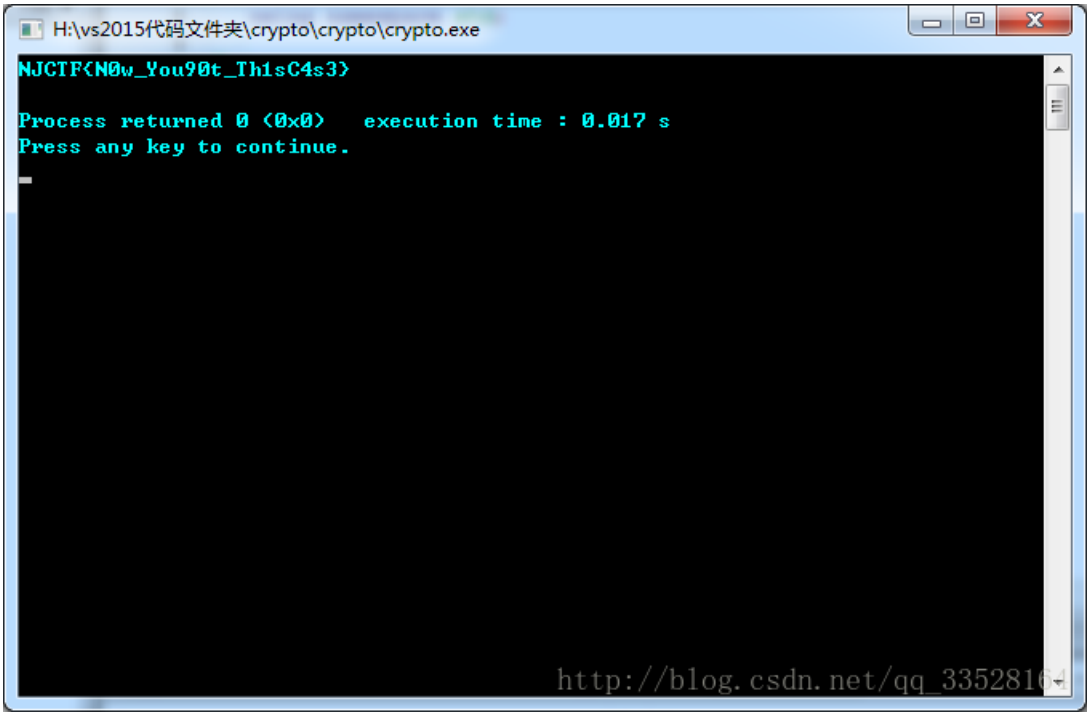
OKIW

从这上面我们可以得出：

key数组就是OKIWILLLETYOUKNOWWHATTHEKEYIS。

得到key之后，我们就要解密密文，还要写出算法：

```cpp
#pragma once
#pragma execution_character_set("utf-8")
#include <stdlib.h>
#include<ctype.h>
#include <stdio.h>
#include <cstring>
#include<iostream>
using namespace std;

int main()
{
    FILE* input_file = fopen("flag.txt", "rb");
    char key[] = "OKIWILLLETYOUKNOWWHATTHEKEYIS";
    char flag[100] = "";
    char p,t,c;
    p = t = c = 0;
    int i = 0;
    while ((c = fgetc(input_file)) != EOF)
    {
        p = c - i*i + t - (key[i % strlen(key)] ^ t);
        flag[i] = p;
        t = p;
        i++;
    }
    cout << flag << endl;
    return 0;
}
```



于是Flag：NJCTF{N0w_You90t_Th1sC4s3}。
解题完毕。