

BUUCTF_ACTF新生赛_crypto

原创

秋风瑟瑟... 于 2020-05-04 23:28:17 发布 455 收藏

版权声明：本文为博主原创文章，遵循 [CC 4.0 BY-SA](#) 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/qq_45628145/article/details/105925192

版权

classic0

附件里面有三个文件，压缩包有密码，根据hints.txt的提示哼，压缩包的密码？这是小Z童鞋的生日吧==，进行8位数字的爆破，得到密码**19990306**



得到一个C文件，代码是

```
#include<stdio.h>
char flag[25] = ***
int main()
{
    int i;
    for(i=0;i<25;i++)
    {
        flag[i] -= 3;
        flag[i] ^= 0x7;
        printf("%c",flag[i]);
    }
    return 0;
}
```

一个flag加密的算法

cipher文件里面的内容就是加密之后的flag，按照上面的思路，写一个解密的代码跑一下就出来了

```
#include<stdio.h>
char flag[25] = "Ygvd mq[lYate[eIghqvakl]";
int main()
{
    int i;
    for(i=0;i<25;i++)
    {
        flag[i] ^= 0x7;
        flag[i] += 3;
        printf("%c",flag[i]);
    }
    return 0;
}
```

得到actf{my_naive_encryption}

classic1

附件里面有两个文件，**vignere.zip**需要密码，通过hints.txt的内容得到密码**circle**

hints.txt的内容

哇，这里有压缩包的密码哦，于是我低下了头，看向了我的双手，试图从中找到某些规律
xdfv ujk098 edft54 xdfv pok,.; wsdr43

这里更具这个提示，看下键盘，发现这些都是圈起来某一个字符的，按照顺序来就得到密码了。解压得到文件



SRLU{LZPL_S_UASHKXUPD_NXYTFTJT}

压缩包的名字提示是**vignere**(维吉尼亚密码)，根据ACTF→SRLU，得到密钥SP。

一个C加密解密维吉尼亚密码的脚本

```
#include <stdio.h>
void encryption()
{
    int a,b,i=0,j=0;
    char x[100],k[10],y[100];
    printf("请输入密文:");
    gets(x);
    printf("\n");
    printf("请输入密钥:");
    gets(k);
    printf("\n");
    a=strlen(x);
    b=strlen(k);
    strlwr(k);
    if(a>b)
    {
        for(i=0;i<a;i++)
        {
            y[i]=(x[i]+k[j]-97-97)%26+97;
            printf("%c",y[i]);
            j++;
        }
    }
}
```

```

        if(j>=b)
            j=0;
    }
}
else
{
    for(i=0;i<a;i++)
    {
        y[i]=(x[i]+k[j]-97-97)%26+97;
        printf("%c",y[i]);
        j++;
    }
}
printf("\n");
}
void decryption()
{
    int a,b,i=0,j=0;
    char x[100],k[10],y[100];
    printf("请输入密文:");
    gets(x);
    printf("\n");
    printf("请输入密钥:");
    gets(k);
    printf("\n");
    a=strlen(x);
    b=strlen(k);
    strlwr(k);
    if(a>b)
    {
        for(i=0;i<a;i++)
        {
            if(x[i]<97)
            {
                y[i]=(x[i]-(k[j]-32)+26)%26+65;
                printf("%c",y[i]);
            }
            else
            {
                y[i]=(x[i]-k[j]+26)%26+97;
                printf("%c",y[i]);
            }
            j++;
            if(j>=b)
                j=0;
        }
    }
    else
    {
        for(i=0;i<a;i++)
        {
            y[i]=(x[i]-k[j]+26)%26+97;
            printf("%c",y[i]);
            j++;
        }
    }
    printf("\n");
}
void main()

```

```
{
    int i;
list:printf("选择是编码还是解码:1. 编码 2. 解码 3. 退出\n");
scanf("%d",&i);
getchar();
switch(i)
{
    case 1:encryption();
    goto list;
    case 2:decryption();
    goto list;
    case 3:exit(1);
}
}
```

跑一下得到flag。

```
ACTFiWHATPAPCLASSICALPVIGENEREK
把对应的符号改回去就是
ACTF{WHAT_A_CLASSICAL_VIGENERE}
```