

攻防世界crypto篇

原创

newly00 于 2020-02-28 16:27:06 发布 1581 收藏 1

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/newly00/article/details/104536827>

版权

1.告诉你个秘密

题目给了这样一串字符：

```
636A56355279427363446C4A49454A7154534230526D6843
56445A31614342354E326C4B4946467A5769426961453067
```

乍一看看不出什么，那就边猜边试吧。

既有数字又有字母，且字符个数是2的倍数，可能是十六进制吧。

那就将其转换成十进制，再根据asc码转化成字符。

```
cjV5RyBscDIJIEJqTSB0RmhC
```

```
VDZ1aCB5N2IKIFFzWiBiaE0g
```

还是看不出来flag是什么样子的。

难道方法不对吗？

再试一次吧，再用base64解码，出现了这样的结果

```
r5yG lp9l BjM tFhB T6uh y7iJ QsZ bhM
```

还是不对，没想法了。

后来查了百度之后说是键盘围绕加密（我的脑洞还是不够大啊）

最后得到flag为TONGYUAN

2.cr3-what-is-this-encryption

```
题目描述：Fady同学以为你是菜鸟，不怕你看到他发的东西。他以明文形式将下面这些东西发给了他的朋友 p=0xa6055ec186de51800ddd6fcbf0192384ff42d707a55f57
af4fcb0d1dc7bd97055e8275cd4b78ec63c5d592f567c66393a061324aa2e6a8d8fc2a910cbee1ed9 q=0xfa0f9463ea0a93b929c099320d31c277e0b0dbc65b189ed76124
f5a1218f5d91fd0102a4c8de11f28be5e4d0ae91ab319f4537e97ed74bc663e972a4a9119307 e=0x6d1fdab4ce3217b3fc32c9ed480a31d067fd57d93a9ab52b472dc393ab
7852fbc11abbebfd6aaae8032db1316dc22d3f7c3d631e24df13ef23d3b381a1c3e04abcc745d402ee3a031ac2718fae63b240837b4f657f29ca4702da9af22a3a019d6890
4a969ddb01bcf941df70af042f4fae5cbeb9c2151b324f387e525094c41 c=0x7fe1a4f743675d1987d25d38111fae0f78bbea6852cba5beda47db76d119a3efe24cb04b9449f
53becd43b0b46e269826a983f832abb53b7a7e24a43ad15378344ed5c20f51e268186d24c76050c1e73647523bd5f91d9b6ad3e86bbf9126588b1dee21e6997372e36c3e
74284734748891829665086e0dc523ed23c386bb520 他严重低估了我们的解密能力 https://blog.csdn.net/newly00
```

看到有q,p,e,c就可以知道是RSA加密

因为 $\phi(N) = (P-1)(Q-1)$

$E * D \% \phi(N) = 1$ （D是私钥，E是公钥）

$M = C^D \bmod N$ （M是明文）

先将p,q,e转化为十进制，再根据公式计算出D,N，M。

再将M转化成字符

最后得到flag为ALEXCTF{RS4_I5_E55ENT1AL_T0_D0_BY_H4ND}

3.flag_in_your_hand1

打开附件，看到

 index.html	HTML 文档
 script-min.js	JavaScript 文件

打开网页，出现

Flag in your Hand

Type in some token to get the flag.

Tips: Flag is in your hand.

Token:

Get flag!

<https://blog.csdn.net/newly00>

按F12

```
var ic = false;
var fg = "";

function getFlag() {
    var token = document.getElementById("secToken").value;
    ic = checkToken(token);
    fg = bm(token);
    showFlag()
}

function showFlag() {
    var t = document.getElementById("flagTitle");
    var f = document.getElementById("flag");
    t.innerHTML = !!ic ? "You got the flag below!!" : "Wrong!";
    t.className = !!ic ? "rightflag" : "wrongflag";
    f.innerHTML = fg;
}
```

<https://blog.csdn.net/newly00>

看了java的源码，知道要让ic返回值为true.

```
var a = [118, 104, 102, 120, 117, 108, 119, 124, 48, 123, 101, 120];
```

而token里要填的是a数列里的每位数减3，转换 asc码得到的字符，输入后得到flag

Flag in your Hand

Type in some token to get the flag.

Tips: Flag is in your hand.

Token:

Get flag!

You got the flag below!!

RenIbyd8Fgg5hawvQm7TDQ