攻防世界crypto篇





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。

cjV5RyBscDlJlEJqTSB0RmhC

VDZ1aCB5N2lKlFFzWiBiaE0q

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 BiM 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 af4fcfb0d1dc7bd97055e8275cd4b78ec63c5d592f567c66393a061324aa2e6a8d8fc2a910cbee1ed9 q=0xfa0f9463ea0a93b929c099320d31c277e0b0dbc65b189ed76124 ncb11abbebfd6aaae8032db1316dc22d3f7c3d631e24df13ef23d3b381a1c3e04abcc745d402ee3a031ac2718fae63b240837b4f657f29ca4702da9af22a3a019d6890 4a969ddb01bcf941df70af042f4fae5cbeb9c2151b324f387e525094c41 c=0x7fe1a4f743675d1987d25d38111fae0f78bbea6852cba5beda47db76d119a3efe24cb04b9449f 53becd43b0b46e269826a983f832abb53b7a7e24a43ad15378344ed5c20f51e268186d24c76050c1e73647523bd5f91d9b6ad3e86bbf9126588b1dee21e6997372e36c3e https://blog.csdn.net/newly00 74284734748891829665086e0dc523ed23c386bb520 他严重低估了我们的解密能力

看到有q,p,e,c就可以知道是RSA加密

因为 ϕ (N) = (P-1)(Q-1)

E*D%φ(N)=1(D是私钥, E是公钥)

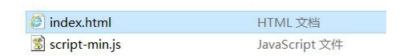
M = C^D mod N(M是明文)

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



打开网页, 出现

按

}

Flag in your Hand

Type in some token to get the flag.

Ti	ps: Flag is in your hand.
То	ken:
G	https://blog.csdn.net/newly00
按F12	
var i	ic = false;
var f	Fg = "";
i f	<pre>cion getFlag() { var token = document.getElementById("secToken").value; ic = checkToken(token); if g = bm(token); ishowFlag()</pre>
}	
v v t	<pre>cion showFlag() { var t = document.getElementById("flagTitle"); var f = document.getElementById("flag"); c.innerText = !!ic ? "You got the flag below!!" : "Wrong!"; c.className = !!ic ? "rightflag" : "wrongflag"; f.innerText = fg;</pre>
	12

看了java的源码,知道要让ic返回值为true.

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: security-xbu
```

Get flag!

You got the flag below!!

RenIbyd8Fgg5hawvQm7TDQ