BUUCTF密码学（crypto）第1~12题

原创

何以缘起 于 2021-01-03 23:52:06 发布 1333 收藏 3

分类专栏： CTF

本文链接：https://blog.csdn.net/qq_53315404/article/details/112161797

crypto

MD5

题目：e00cf25ad42683b3df678c61f42c6bda

根据题目提示这是**MD5密文**，所以直接解密就得到了flag

flag{admin1}

Url编码

题目：%66%6c%61%67%7b%61%6e%64%20%31%3d%31%7d

题目提示这是**Url编码**，在线Url解码即得flag
flag{and 1=1}

一眼就解密

题目：下面的字符串解密后便能获得flag：ZmxhZ3tUSEVfRkxBR19PRl9USEITX1NUUklOR30=

很明显是**base64编码**，在线解码即得flag
flag{THE_FLAG_OF_THIS_STRING}

看我回旋踢

题目：synt{5pq1004q-86n5-46q8-o720-oro5on0417r1}

题目提示回旋，也就是凯撒密码，当过了z之后回到a,s到f是13位，所以全部移13位即得flag
flag{5cd1004d-86a5-46d8-b720-beb5ba0417e1}

摩丝

题目：... .-... — ...- . -.-- — ...-

直接摩斯密码解密
flag{lLOVEYOU}

[BJDCTF 2nd]签到-y1ng

题目：QkpEe1czbGMwbWVfVDBfQkpEQ1RGfQ==

明显**base64编码**，解码即得
BJD{W3lc0me_T0_BJDCTF}

password

题目：姓名：张三
生日：19900315
key格式为key{xxxxxxxxxx}

数一下x有10个，所以是10个字符得flag，刚开始试了试1990-03-15，发现不对，再试了试zs19900315,对了，张三（zs).
flag{zs19900315}

变异凯撒

题目：加密密文：afZ_r9VYfScOeO_UL^RWUc

提示是凯撒密码，a的ASCII码值是97，f是102（=97+5）。f是102，l是108（=102+6）。
Z是90，a是97（=90+7）。_是97，g是103（=103+8）。所以是递加的规律，可以自己写程序转化，即得flag。

flag{Caesar_variation}

Quoted-printable

题目：
=E9=82=A3=E4=BD=A0=E4=B9=9F=E5=BE=88=E6=A3=92=E5=93=A6

根据题目提示，这是Quoted-printable编码，在线解码即得flag
flag{那你也很棒哦}

Rabbit

题目：U2FsdGVkX1/+ydnDPowGbjjJXhZxm2MP2AgI

题目提示是Rabbit编码，直接解码即得flag
flag{Cute_Rabbit}

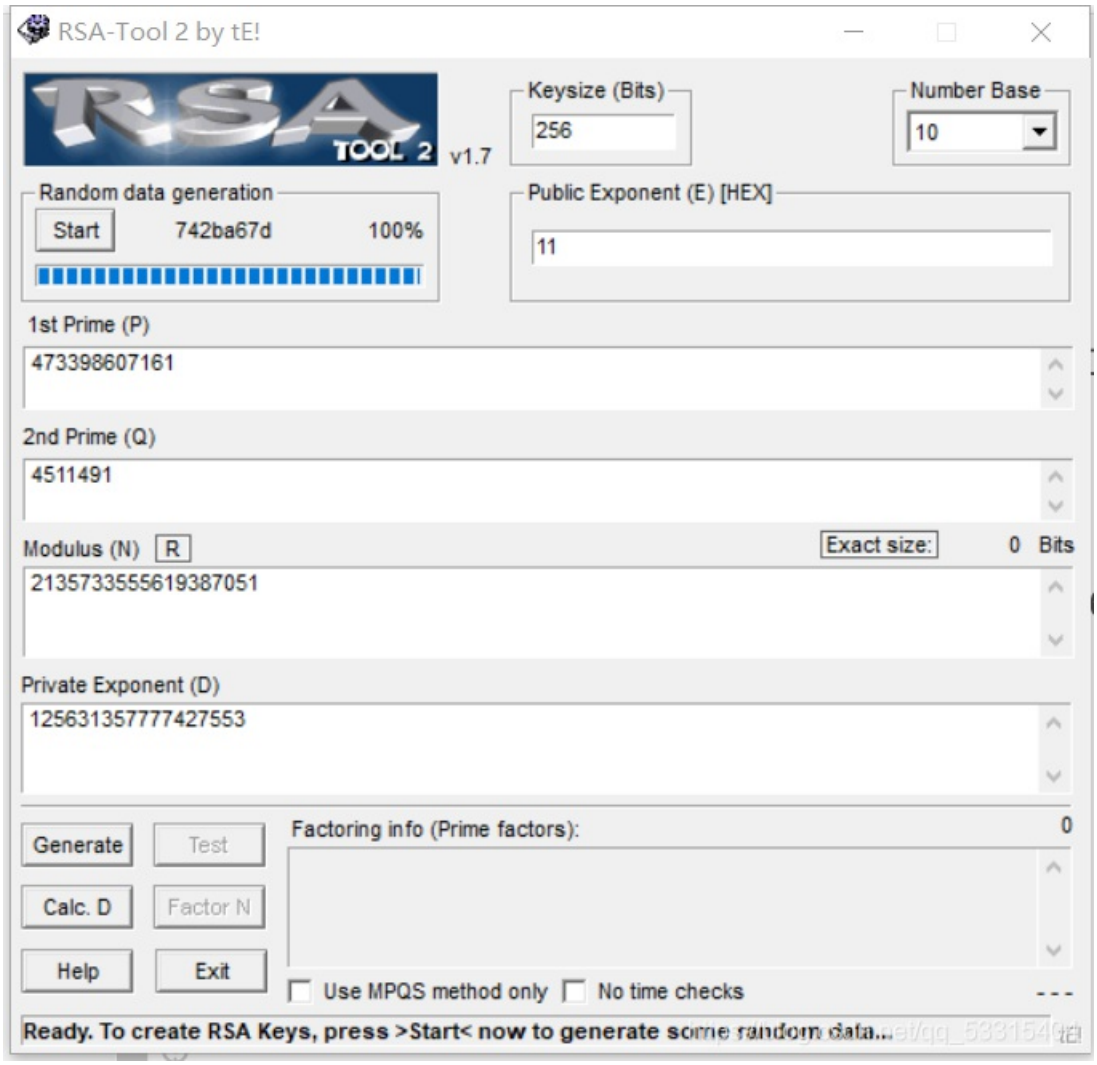
篱笆墙的影子

题目：felhaagv{ewtehtehfilnakgw}

题目提示篱笆，就是栅栏密码，当每组字数是13时，即得flag
flag{wethinkwehavetheflag}

RSA

题目：在一次RSA密钥对生成中，假设p=473398607161，q=4511491，e=17
求解出d作为flag提交
工具：RSATool2v17



e=17，十六进制下就是11。
flag{125631357777427553}