BUUCTF-Crypto刷题记录

原创

Georgeiweb 于 2020-10-18 15:41:36 发布 874 收藏 1

文章标签： 加密解密 密码学

本文链接：https://blog.csdn.net/Georgeiweb/article/details/109058184

BUUCTF-Crypto刷题记录

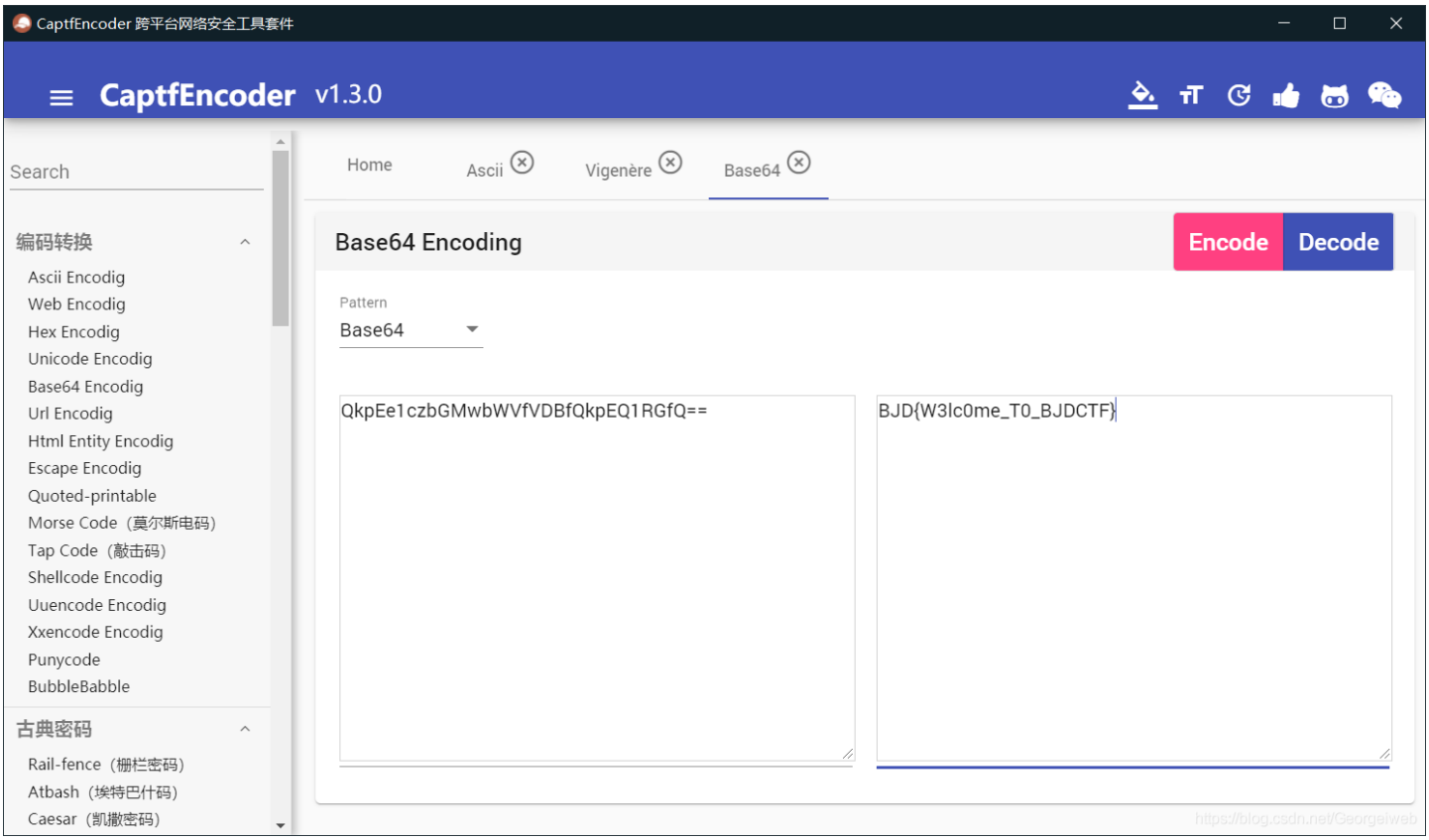
签到-y1ng

题目：welcome to BJDCTF

1079822948

QkpEe1czbGMwbWVfVDBfQkpEQ1RGfQ==

解题思路：密文后边有等号，很有可能是base 64所以用工具尝试



所以答案为flag{W3lc0me_T0_BJDCTF}

password

题目：姓名：张三

生日：19900315

key格式为key{xxxxxxxxx}

解题思路：没有什么可以看出的标志，所以尝试着，姓名缩写加生日

所以答案刚好为：flag{zs19900315}

Quoted-printable

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

解题思路，由题目就可以看出这是Quoted-printable（可打印字符引用编码),所以直接使用工具

答案为：flag{那你也很棒哦}

Rabbit

题目：U2FsdGVkX1/+ydnDPowGbjjJXhZxm2MP2AgI

解题思路：这道题由题目得知是rabbit，所以直接使用工具

网站：Rabbit加密

答案为：flag{Cute_Rabbit}

老文盲了

题目：罼雧締罙擴灝淛匶襫黼瀬鎶軄鶛驕鰳哵罙鞹鯑

解题思路：由题，全为中文繁体字，先从读音下手，所以使用网站在线汉字转拼音

从读音看出答案为flag{淛匶襫黼瀬鎶軄鶛驕鰳哵}

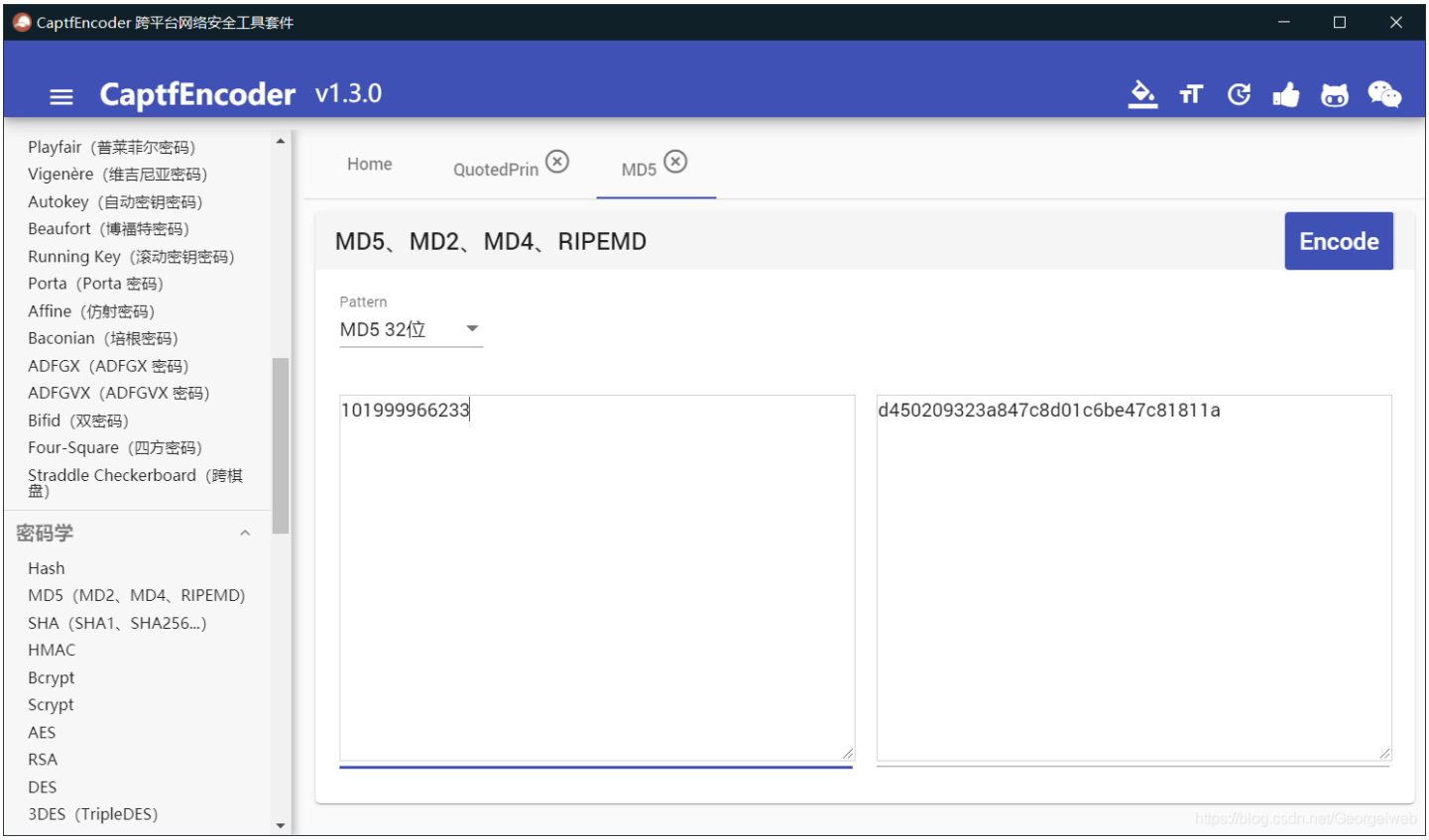
Alice与Bob

题目：密码学历史中，有两位知名的杰出人物，Alice和Bob。他们的爱情经过置换和轮加密也难以混淆，即使是没有身份认证也可以知根知底。就像在数学王国中的素数一样，孤傲又热情。下面是一个大整数:98554799767,请分解为两个素数，分解后，小的放前面，大的放后面，合成一个新的数字，进行md5的32位小写哈希，提交答案。 注意：得到的 flag 请包上 flag{} 提交

解题思路：直接由题目解题得，使用工具在线分解质数

98554799767=101999*966233

所以在对101999966233进行MD5的32位小写哈希，



答案为：flag{d450209323a847c8d01c6be47c81811a}

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flga提交

解题思路：直接写出python脚本，直接解出答案

```
import gmpy2
from Crypto.Util import number
p = 473398607161
q = 4511491
e = 17
d = gmpy2.invert(e,(p-1)*(q-1))
print (d)
```

所以直接得出答案：flag{125631357777427553}

Windows系统密码

题目：Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
ctf:1002:06af9108f2e1fecf144e2e8adef09efd:a7fcb22a88038f35a8f39d503e7f0062:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SUPPORT_388945a0:1001:aad3b435b51404eeaad3b435b51404ee:bef14eee40dffbc345eeb3f58e290d56:::
解题思路：密文全由阿拉伯数字和小写字母组成，很大的可能是MD5，所以我直接把ctf里边的两串字母串带入工具，然后答案是good-luck，提交，答案正确。
工具网站：cmd在线破解

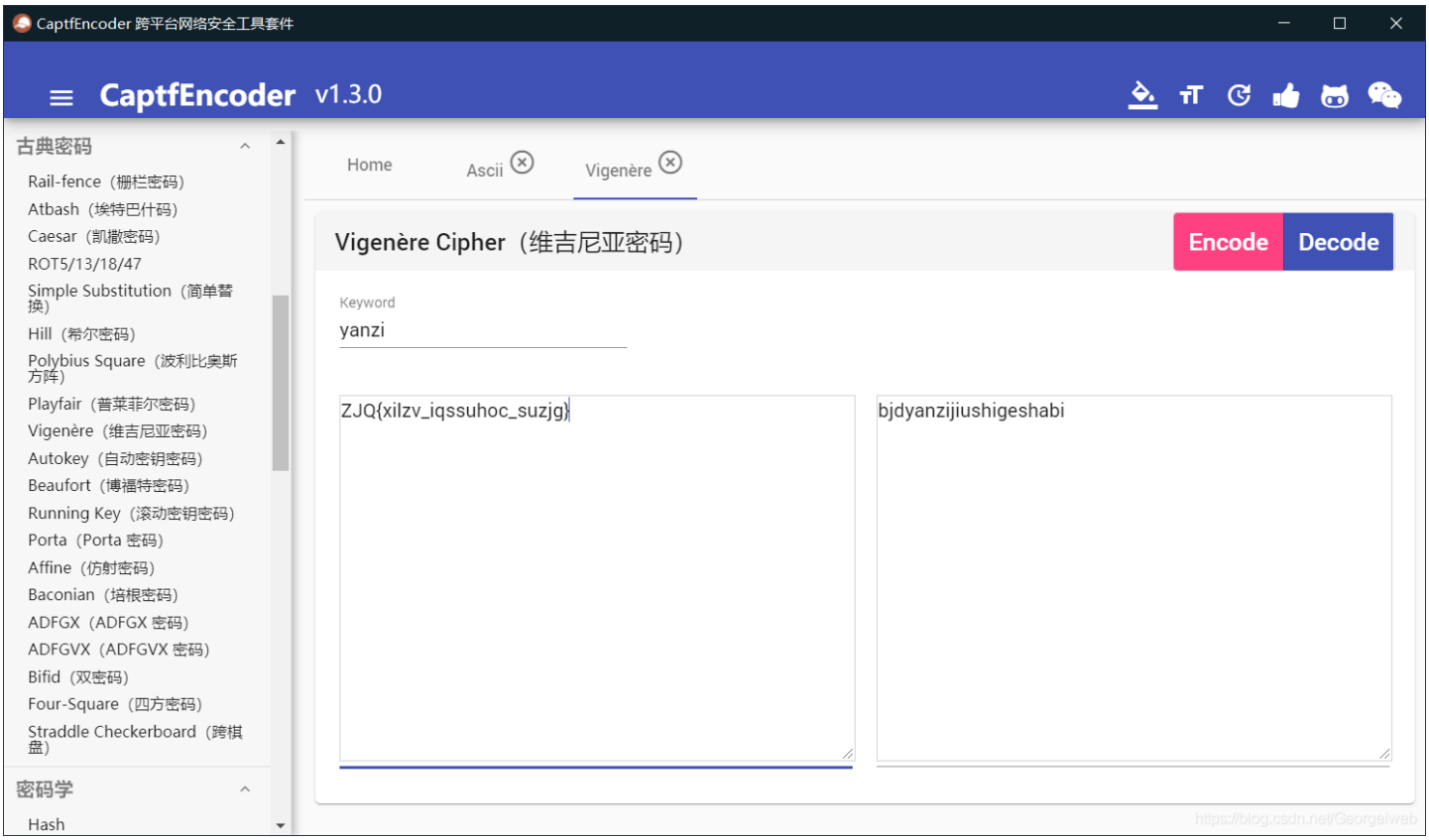
cat-flag

题目：

解题思路：由图可以看出，图中只有两种图形，所以我推断可能是二进制
二进制为：
01000010
01001010
01000100
01111011
01001101
00100001
01100001
00110000
01111110
01111101
ASCII码转换为
424a447b4d2161307e7d
在转化为明文为BJD{M!a0~}
所以答案为flag{M!a0~}

燕言燕语-y1ng

题目：79616E7A69205A4A517B78696C7A765F6971737375686F635F73757A6A677D20
解题思路：由题目看出，这可能是十六进制组成，先转换试试。
转换出来是
yanzi ZJQ{xilzv_iqssuhoc_suzjg}
但这明显不是答案
所以再次分析，yanzi可能是密钥。继续解密
因为密钥长度比密文短，所以我推测这是维吉尼亚加密，密钥循环使用。
BJD{yanzi_jiushige_shabi}



丢失的MD5

题目：

```
import hashlib
for i in range(32,127):
    for j in range(32,127):
        for k in range(32,127):
            m=hashlib.md5()
            m.update('TASC'+chr(i)+'O3RJMV'+chr(j)+'WDJKX'+chr(k)+'ZM')
            des=m.hexdigest()
            if 'e9032' in des and 'da' in des and '911513' in des:
                print (des)
```

解题思路：这道题直接给的代码，所以先试试可不可以直接跑出
python3跑不出来
python2跑出来（python3不兼容python2）
答案为flag{e9032994dabac08080091151380478a2}