# BUUCTF Crypto(密码学)刷题

原创

base呗 于 2021-03-28 22:19:02 发布 922 收藏 10

分类专栏： CTF 文章标签： 密码学 加密解密



本文链接：https://blog.csdn.net/weixin_52805837/article/details/115211662





## MD5

拿到一串字符串e00cf25ad42683b3df678c61f42c6bda

根据题目可到在线MD5在线解密


拿到flag

## Url编码

根据提示可知是url编码
url编码在线解密


## 一眼就解密


的确，一眼就解密了，非常明显的bese64解码
bese64在线解码拿到flag！

## 看我回旋踢

根据题意，回旋踢，莫非是凯撒移位？


果然是凯撒凯撒在线解码

## 摩丝

根据题目加上给的附件一看便知是摩斯密码
摩斯电码在线解码

## password




此题很有意思，啥解密也想不起来，哈哈哈哈
key的长度刚好是张三的首字母和生日数字的总和
flag{zs19900315}

## 变异凯撒

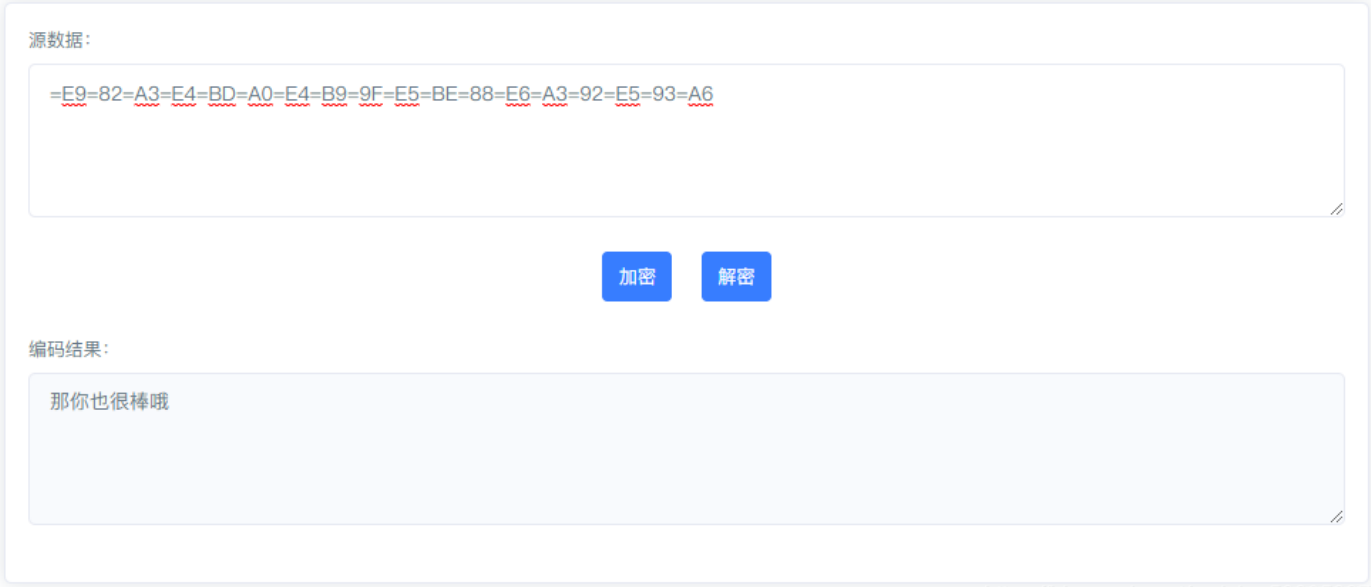
此题借助大佬脚本，得到flag

```
#include<stdio.h>
int main()
{
int i;
char a[30]=“afZ_r9VYfScOeO_UL^RWUc”;
for(i=0;a[i];i++)
{
a[i]=a[i]+i+5;
printf("%c",a[i]);
}
return 0;
}
得到flag{Caesar_variation}
```

## Quoted-printable

Quoted-printable 解码编码

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

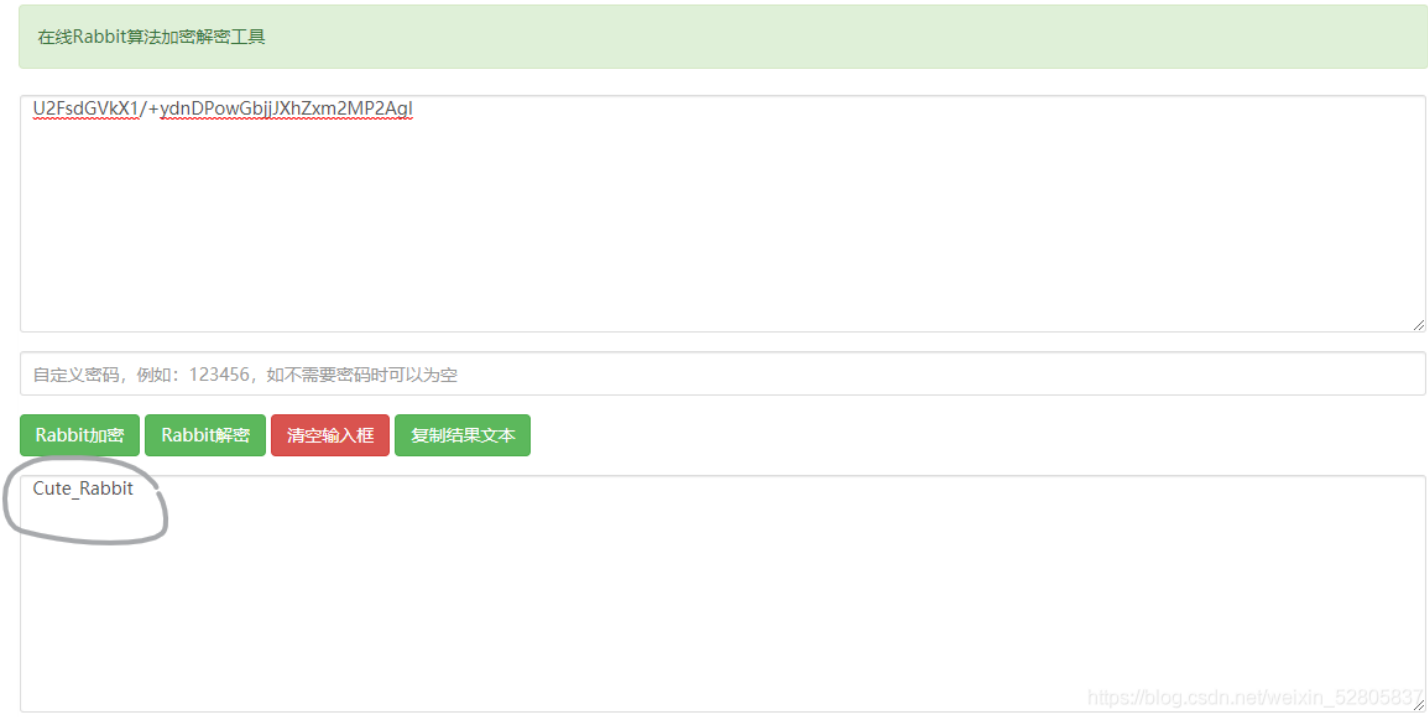





## Rabbit

Rabbit算法加密解密工具

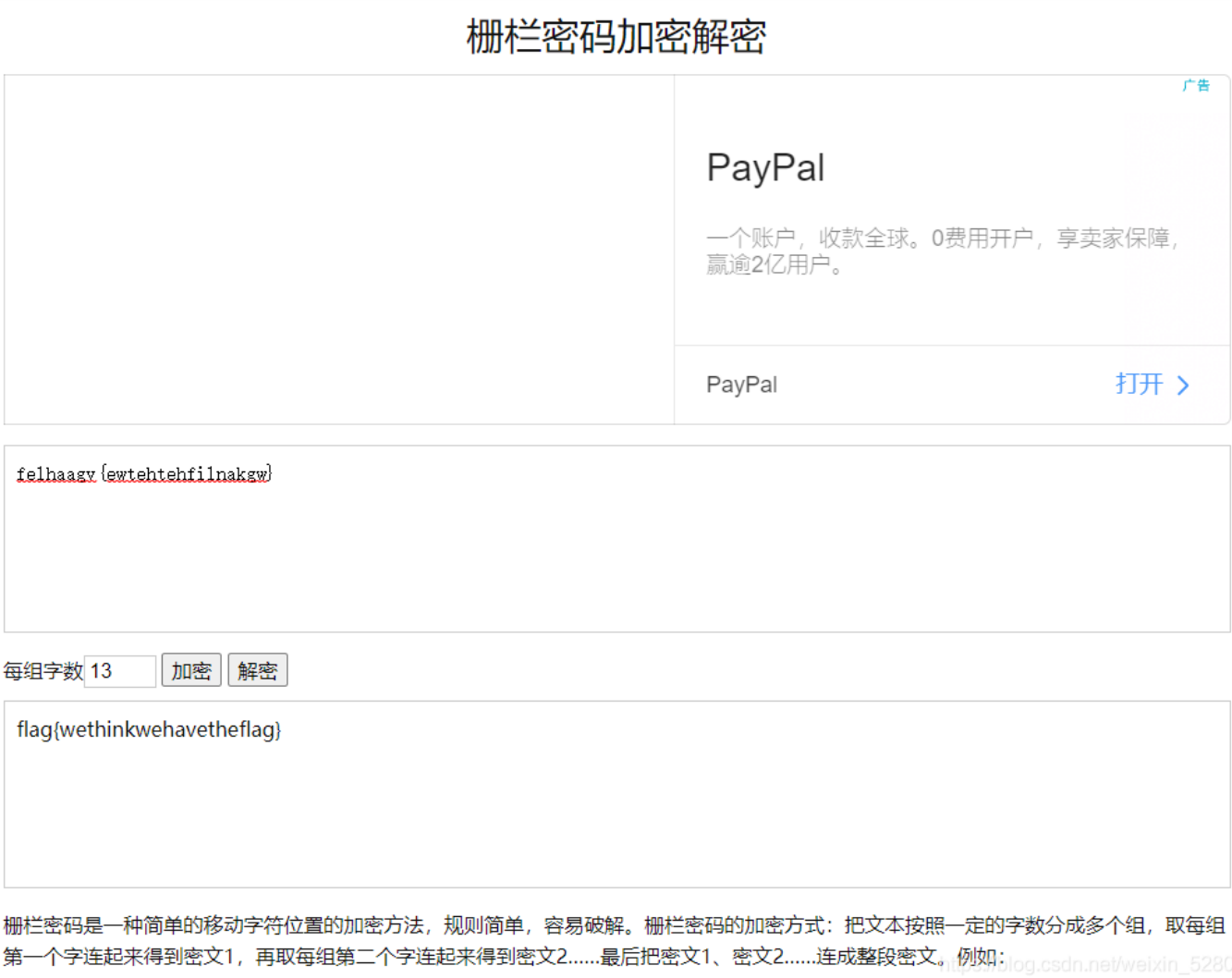
题目编码形式：U2FsdGVkX1/+ydnDPowGbjjJXhZxm2MP2AgI




得到flag

## 篱笆墙的影子

看到题目，不难联想到栅栏密码:
所谓栅栏密码，就是把明文分成N个组，然后取出每组的第一个，每组的第二个。。接着按顺序排列得出密文。若每个组里有2两个元素的话就叫2栏栅栏密码。
栅栏密码加密解密
felhaagv{ewtehtehfilnakgw}




## RSA

OK!!!又是密码题中典型的题目形式
利用脚本得到flag或者使用RSATool2v17软件解码

```
import gmpy2
import rsa

e=65537
n=869344822960481191906660620034948005889056560172030256172166540583783221035 17
p=285960468890451637935629440372639283459
q=304008741604601924494328155975272418463

phin = (p-1) * (q-1)
d=gmpy2.invert(e, phin)

key=rsa.PrivateKey(n,e,int(d),p,q)

with open("flag.enc","rb") as f:
    f=f.read()
    print(rsa.decrypt(f,key))
```

## 丢失的MD5

此题又被恶心到，哈哈哈哈

默默偷看wp

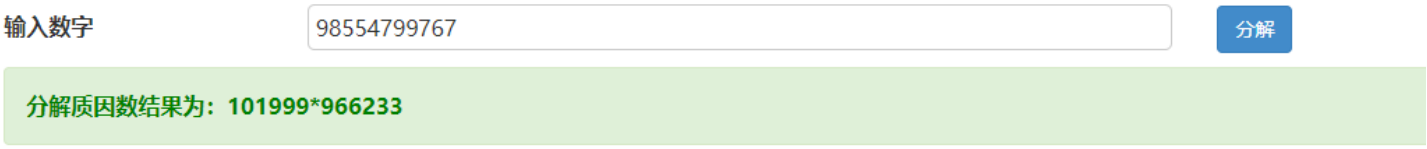
利用脚本得到flag！！！

推荐大佬详细解题思路丢失的MD5

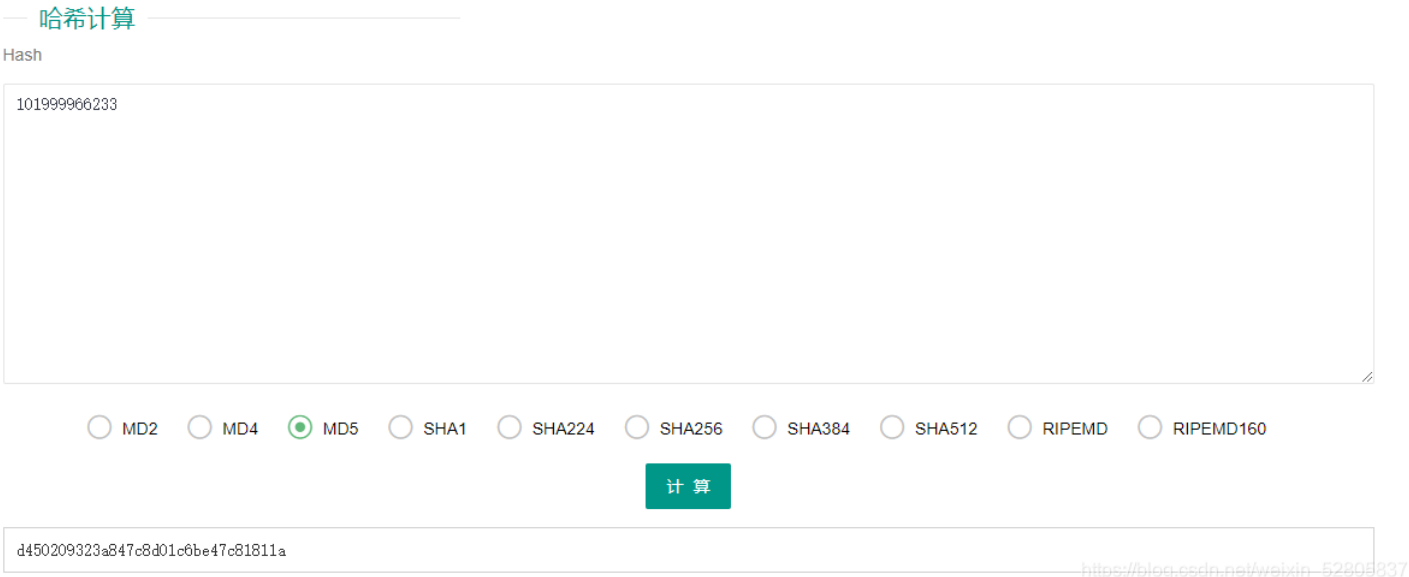
```
import hashlib
for i in range(32,127):
    for j in range(32,127):
        for k in range(32,127):
            m=hashlib.md5()
            m.update('TASC'.encode('utf-8')+chr(i).encode('utf-8')+'O3RJMV'.encode('utf-8')+chr(j).encode('utf-8
')+'WDJKX'.encode('utf-8')+chr(k).encode('utf-8')+'ZM'.encode('utf-8'))
            des=m.hexdigest()
            if 'e9032' in des and 'da' in des and '911513' in des:
                print (des)
```

## Alice与Bob

根据题目条件，先去分解大整数在线分解质因数计算器工具




然后将小的放前面，大的放后面，合成一个新的数字，进行md5的32位小写哈希




拿到flag！！！
顺便康康哈希算法吧。。。

哈希算法