




BUUCTF Crypto(密码学)刷题

原创

base吰  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](#)

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/weixin_52805837/article/details/115211662

版权



[CTF 专栏收录该内容](#)

9 篇文章 0 订阅

订阅专栏

MD5

拿到一串字符串e00cf25ad42683b3df678c61f42c6bda

根据题目可到在线MD5在线解密

密文:

类型:  [\[帮助\]](#)

查询结果:
admin1

https://blog.csdn.net/weixin_52805837

拿到flag

Url编码

根据提示可知是url编码

url编码在线解密

URL编码

| | |
|---|---|
| 1 | %66%6c%61%67%7b%61%6e%64%20%31%3d%31%7d |
|---|---|

URL编码 URL解码 交换内容 清空 下载加密/解密代码 复制加密/解密代码

Microsoft 365
立即试用 →
您的一体化协作中心
视频、通话、聊天、文件共享, 等等

encodeURIComponent,不会对特殊符号编码

| | |
|---|---------------|
| 1 | flag{and 1=1} |
|---|---------------|

一眼就解密

Challenge 4461 Solves ×

一眼就解密

1

下面的字符串解密后便能获得flag:

ZmxhZ3tUSEVfRkxBR19PRI9USEITX1NUUkiOR30= 注意:

得到的flag 请包上 flag{} 提交

https://blog.csdn.net/weixin_52805837

的确,一眼就解密了,非常明显的base64解码

base64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？

凯撒密码加密/解密

| | |
|---|--|
| 明文: | flag{5cd1004d-86a5-46d8-b720-beb5ba0417e1} |
| 偏移量 | 13 |
| <input type="button" value="加密"/> <input type="button" value="解密"/> | |
| 密文: | svnt{5pq1004q-86n5-46q8-o720-oro5on0417r1} |

https://blog.csdn.net/weixin_52805837

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

📄 题目.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

姓名：张三

生日：19900315

key格式为key{xxxxxxxxxx}

https://blog.csdn.net/weixin_52805837

此题很有意思，啥解密也想不起来，哈哈哈哈哈
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_r9VYfSc0e0_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

源数据:

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

加密 解密

编码结果:

那你也很棒哦

https://blog.csdn.net/weixin_52805837

Rabbit

Rabbit算法加密解密工具

题目编码形式: U2FsdGVkX1/+ydnDPowGbjjXhZxm2MP2Agl

U2FsdGVkX1/+ydnDPowGbjjJXhZxm2MP2AgI

自定义密码，例如：123456，如不需要密码时可以为空

Rabbit加密

Rabbit解密

清空输入框

复制结果文本

Cute_Rabbit

https://blog.csdn.net/weixin_52805837

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个元素的话就叫2栏栅栏密码。

栅栏密码加密解密

felhaagv{ewtehtehfilnakgw}

栅栏密码加密解密

| | |
|--|--|
| | 广告 |
| | <h1>PayPal</h1> <p>一个账户，收款全球。0费用开户，享卖家保障，赢逾2亿用户。</p> |
| | PayPal 打开 > |

```
felhaagv {ewtehtehfilnakgw}
```

每组字数

```
flag{wethinkwehavetheflag}
```

栅栏密码是一种简单的移动字符位置的加密方法，规则简单，容易破解。栅栏密码的加密方式：把文本按照一定的字数分成多个组，取每组第一个字连起来得到密文1，再取每组第二个字连起来得到密文2.....最后把密文1、密文2.....连成整段密文。例如：log.csdn.net/weixin_52805837

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=86934482296048119190666062003494800588905656017203025617216654058378322103517
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

Alice与Bob

1

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

https://blog.csdn.net/weixin_52805837

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

输入数字

98554799767

分解

分解质因数结果为: **101999*966233**

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

— 哈希计算 —

Hash

101999966233

MD2 MD4 MD5 SHA1 SHA224 SHA256 SHA384 SHA512 RIPEMD RIPEMD160

计算

d450209323a847c8d01c6be47c81811a

https://blog.csdn.net/weixin_52999337

拿到flag!!!

顺便康康哈希算法吧。。。

[哈希算法](#)