




CTFSHOW crypto0-13 Writeup

原创

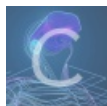
abtgu  于 2020-09-13 15:20:33 发布  1736  收藏 10

分类专栏: [CTF 密码学](#) 文章标签: [密码学](#)

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_43790779/article/details/108562822

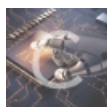
版权



[CTF 同时被 2 个专栏收录](#)

22 篇文章 1 订阅

订阅专栏



[密码学](#)

10 篇文章 2 订阅

订阅专栏

文章目录

[crypto0](#)

[crypto2](#)

[crypto3](#)

[crypto4](#)

[crypto5](#)

[crypto6](#)

[crypto7](#)

[crypto8](#)

[crypto9](#)

[crypto10](#)

[crypto11](#)

[crypto12](#)

[crypto13](#)

[密码学签到](#)

[babyrsa](#)

crypto0

题目: `gmbh{ifmmp_dug}`

解题思路: 观察, 发现是凯撒加密, 位移为1。

crypto2

题目：无

解题思路：打开文本，发现是jencode，直接在控制台执行即可得到flag，flag{3e858ccd79287cfe8509f15a71b4c45d}。

crypto3

题目：无

解题思路：打开文本，发现是aaencode，直接在控制台执行即可得到flag，flag{js_da_fa_hao}

crypto4

题目：p=447685307 q=2037 e=17，提交flag{d}即可

解题思路：直接上脚本

```
import gmpy2
p = 447685307
q = 2037
e = 17
phi = (p-1)*(q-1)
d = gmpy2.invert(e, phi)
print(d)
```

crypto5

题目：p=447685307 q=2037 e=17 c=704796792，提交flag{m}

解题思路：直接上脚本

```
import gmpy2
p=447685307
q=2037
e=17
c=704796792

phi = (p-1)*(q-1)
d = gmpy2.invert(e, phi)
m = gmpy2.powmod(c, d, p*q)

print(m)
```

crypto6

题目：

密文：U2FsdGVkX19mGsGlf3nciNVpWZZRqZO2PYjJ1ZQuRqoiknyHSWeQv8oI0uRZP94MqeD2xz+

密钥：

加密方式名称

解题思路：观察密文，猜测是Rabbit加密，尝试进行Rabbit解密，得到flag，解密网址<http://www.jsons.cn/rabbitencrypt/>。

crypto7

题目：无

解题思路：打开文本，发现是Ook!加密，解密网址<https://www.splitbrain.org/services/ook>。

crypto8

题目：无

解题思路：打开文本，发现是Brainfuck加密，解密网址<https://www.splitbrain.org/services/ook>。

crypto9

题目：无

解题思路：将压缩包放在kali下使用fcrackzip暴力破解，

```
fcrackzip -D -u -p /user/share/wordlists/rockyou.txt serpent.zip
```

得到密码是4132。

因为压缩包以serpent命名，所以猜想serpent加密，解密网址

<http://serpent.online-domain-tools.com/>，key=4132。

解密得到flag，flag{c960a0f3bf871d7da2a8413ae78f7b5f}。

crypto10

题目：解密后 提交 flag{明文}

解题思路：打开文本，发现是quoted-printable编码，解码网址：<http://web.chacuo.net/charsetquotedprintable>。

crypto11

题目：密文：a8db1d82db78ed452ba0882fb9554fc

解题思路：md5碰撞

<https://www.somd5.com/>。

crypto12

题目：uozt{Zgyzhv_xlww_uiln_xguhsld}

解题思路：猜测uozt对应flag，u-f，o-l，z-a，t-g，正好符合埃特巴什码，解码得flag，flag{Atbase_code_from_ctfshow}。

crypto13

题目：链接：<https://pan.baidu.com/s/1Q6qAdororzP0H7alkoY1rg> 提取码：7mjw 格式flag{*****}

解题思路：

题中说明base家族，猜测是多种base组合，常见的时base32和base64，写脚本执行，发现得到flag，flag{b4Se_Fami1y_Is_FUn}。

```
import base64
def base(s):
    try:
        s = base64.b32decode(s)
        s = base(s)
    except:
        try:
            s = base64.b64decode(s)
            s = base(s)
        except:
            return s
    return s
f = open('base.txt')

text = f.read()

print(base(text))
```

密码学签到

题目: }wohs.ftc{galf

解题思路: 观察, 直接逆序输出即可得到flag, flag{ctf.show}

babyrsa

题目: 无

解题思路: 直接上脚本

```
import gmpy2
import binascii
e = 65537
p = 104046835712664064779194734974271185635538927889880611929931939711001301561682270177931622974642789920918902
5633612933454340557642936124468883839128071433940090198034718164489239696379806712211111179652274024296349354818
68701166522350570364727873283332371986860194245739423508566783663380619142431820861051179
q = 140171048074107988605773731671018901813928130582422889797732071529733091703843710859282267763783461738242958
0986109491203544979879459110211708424575521828801336427113072270721338122533411298304161584504992582169678798575
81565380890788395068130033931180395926482431150295880926480086317733457392573931410220501
c = 477275891120477102804902067077833679956877893007284108405780986760802273261129530509605243064188155078114177
6498904005589873830973301898523644744951545345404578466176725030290421649344936952480254902939417215148205735730
7548084673516399434748162809802304470974446824892230544995241979097198573005971574060750692043150227038944662261
7950762707083542822608650976774675935382230280938504776329289154369727709706840651292479640939328998273807101904
7393972959228919115821862868057003145401072581115989680686073663259771587445250687060240991265143919857962047718
344017741878925867800431556311785625469001771370852474292194

phi = (p-1)*(q-1)
d = gmpy2.invert(e, phi)
m = gmpy2.powmod(c, d, p*q)

print(binascii.unhexlify(hex(m)[2:]))
```