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

本文链接：https://blog.csdn.net/weixin_43790779/article/details/108562822

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

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jjencode，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：U2FsdGVkX19mGsGlfl3nciNVpWZZRqZO2PYjJ1ZQuRqoiknyHSWeQv8ol0uRZP94MqeD2xz+

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0ok!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_xlwv_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 = 10404683571266406477919473497427118563553892788988061192993193971100130156168227017793162297464278992091890256336129334543405576429361244688838391280714339400901980347181644892396963798067122111111796522740242963493548186870116652235057036472787328333237198686019424573942350856678366338061914243182086105117 9
q = 14017104807410798860577373167101890181392813058242288979773207152973309170384371085928226776378346173824295809861094912035449798794591102117084245755218288013364271130722707213381225334112983041615845049925821696787985758156538089078839506813003393118039592648243115029588092648008631773345739257393141022050 1
c = 47727589112047710280490206707783367995687789300728410840578098676080227326112953050960524306418815507811417764989040055898738309733018985236447449515453454045784661767250302904216493449369524802549029394172151482057357307548084673516399434748162809802304470974446824892230544995241979097198573005971574060750692043150227038944662261795076270708354282260865097677467593538223028093850477632928915436972770970684065129247964093932899827380710190473939729592289191158218628680570031454010725811159896806860736632597715874452506870602409912651439198579620477183440177418789258678004315563117856254690017713708524742921 94

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

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