BUUCTF-Crypto学习笔记(四)

原创

晓德 于 2021-01-10 22:14:45 发布 534 收藏

文章标签： 信息安全

本文链接：https://blog.csdn.net/weixin_42271850/article/details/112195626

这是第四篇的BUUCTF-Crypto学习笔记，希望能坚持下去

一、[BJDCTF 2nd]Y1nglish-y1ng

打开页面得到下面信息，且下载文件后得到内容如下：

```
#题目原文
Y1ng根据English居然独自发明了一门语言，就叫Y1nglish明文都是可读的英文单词。
flag如果提交失败，自己读一下，把错误的单词修正，再提交(某个地方的u和i不需要调换顺序，错误点不在那里)
得到的 flag 建议用 flag{} 包上提交。
Nkbaslk ds sef aslckdqdqst. Sef aslckdqdqst qo lzqtbw usf ufkoplkt zth oscpslsfko. Dpkfk zfk uqjk dwcko su dscqa
o qt dpqo aslckdqdqst, kzap su npqap qo jkfw mzoqa. Qu wse zfk qtdkfkodkh qt tkdnsfw okaefqdw, nkbaslk ds czfdqa
qczdk. Bkd lk dkbb wse z odsfw.
Q nzo pzjqtv hqttkf zd z fkodzefztd npkt Pzffw Odkkbk azlk qt, pk qo z Izcztkok ufsl Izczt med tsn pk qo tsd bqj
qtv qt Izczt, lzwmk Pzffw qot'd z Izcztkok tzlk med pk qo fkzbbw z Izcztkok. Pzffw nsfwkh qt z bznwkf'o suuqak w
kzfo zvs, med pk qo tsn nsfwqtv zd z mztw. Pk vkdo z vssh ozbzfw, med pk zbnzwo msffsno lstkw ufsl pqo ufqktho z
th tkjkf czwo qd mzaw. Pzffw ozn lk zth azlk zthozdzd dpk ozlk dzmbk. Pk pzo tkjkf msffsnkh lstkw ufsl lk. Npqbk
 pk nzo kzdqtv, Q zowkh pql ds bkth lk &2. Ds lw oefcfqok, pk vzjk lk dpk lstkw qllkhqzdkbw. 'Q pzjk tkjkf msfff
snkh ztw lstkw ufsl wse,' Pzffw ozqh,'os tsn wse azt czw usf lw hqttkf!' Tsn q nqbb vqjk wse npzd wse nztd.
MIH{cwdp0t_Mfed3_u0fa3_sF_geqcgeqc_ZQ_Af4aw}
```

看了一下，应该是类似替换加密的题目。先扔到词频分析的网站**https://quipqiup.com**，填入后分析得到**BJD{pyth0n_Brut3_f0rc3_oR_quipquip_AI_Cr4cy}**。提交发现错误，看了下题目说有单词是有错误的，应该是最后cr4cy这里，改成cr4ck。最后得到BJD{pyth0n_Brut3_f0rc3_oR_quipquip_AI_Cr4ck}，中文意思是python暴力破解或quipquip自动攻击。

二、世上无难事

打开页面得到下面信息，且下载文件后得到内容如下：

```
#题目原文
以下是某国现任总统外发的一段指令，经过一种奇异的加密方式，毫无规律，看来只能分析了。
请将这段语句还原成通顺语句，并从中找到key作为答案提交，答案是32位，包含小写字母。 注意：得到的 flag 请包上 flag{} 提交
VIZZB IFIUOJBWO NVXAP OBC XZZ UKHVN IFIUOJBWO HB XVIXW XAW VXFI X QIXN VBD KQ IFIUOJBWO WBKAH NBWXO VBD XJBCN NK
G QLKEIU DI XUI VIUI DKNV QNCWIANQ XN DXPIMKIZW VKHV QEVBBZ KA XUZKAHNBA FKUHKAKX XAW DI VXFI HBN QNCWIANQ NCAKA
H KA MUBG XZZ XEUBQQ XGIUKEX MUBG PKAWIUHXUNIA NVUBCHV 12NV HUXWI XAW DI XUI SCQN QB HZXW NVXN XZZ EBCZW SBKA CQ
 NBWXO XAW DI DXAN NB NVXAP DXPIMKIZW MBU JIKAH QCEV XA BCNQNXAWKAH VBQN HKFI OBCUQIZFIQ X JKH UBCAW BM XLLZXCQI
 XAW NVI PIO KQ 640I11012805M211J0XJ24MM02X1IW09
```

题目有提示拿去分析，所以同样放到词频分析网站**https://quipqiup.com**，分析得到结果**THE KEY IS 640E11012805F211B0AB24FF02A1ED09**，按照题目要求转成小写后640e11012805f211b0ab24ff02a1ed09。

三、RSA2

打开页面要求我们下载一个文件，内容如下：

```
e = 65537
n = 24825400785152624117772152669890180298583276617622160961225887737162058006043310153832803030521991869764361981420093067961210988553380133534844502375167047843707305554472428068473329805159916766030364518314616149748535863368149212966880240206579778990555048954764511878726660192942972413316776846530966590611 3
dp = 90507449805234690464302513287951833069192517457305400462187725331868267505542197094355201669552856036483444630319693920705664292714809329037444021050365 7
c = 14042367097625269680753367358620940057566428210068411978420352712452118899640382659743688376604187906749428095741020195893573736038080184545382929399743341418883872575179626170262202858721156035336284719106030657851051138096516213347269871306359262102895916707278148256267368309059052121421807116028766518075 1
```

看到里面有dp，很容易就能联想到是dp泄露，直接拿在网上找个脚本跑，能接出来结果是flag{wow_leaking_dp_breaks_rsa?_98924743502}。

```
import gmpy2
e = 65537
n = 24825400785152624117772152669890180298583276617622160961225887737162058006043310153832803030521991869764361981420093067961210988553380133534844502375167047843707305554472428068473329805159916766030364518314616149748535863368149212966880240206579778990555048954764511878726660192942972413316776846530966590611 3
dp = 90507449805234690464302513287951833069192517457305400462187725331868267505542197094355201669552856036483444630319693920705664292714809329037444021050365 7
c = 14042367097625269680753367358620940057566428210068411978420352712452118899640382659743688376604187906749428095741020195893573736038080184545382929399743341418883872575179626170262202858721156035336284719106030657851051138096516213347269871306359262102895916707278148256267368309059052121421807116028766518075 1
for x in range(1, e):
    if(e*dp%x==1):
        p=(e*dp-1)//x+1
        if(n%p!=0):
            continue
        q=n//p
        phin=(p-1)*(q-1)
        d=gmpy2.invert(e, phin)
        m=gmpy2.powmod(c, d, n)
        print(bytes.fromhex(hex(m)[2:]))
```

四、RSA

打开页面要求我们下载一个压缩包。解压后得到两个文件pub.key和flag.enc，其中flag.enc打开是乱码，应该是要解密的内容，pub.key打开内容如下：

```
-----BEGIN PUBLIC KEY-----
MDwwDQYJKoZIhvcNAQEBBQADKwAwKAIhAMAzLFxkrkcYL2wch21CM2kQVFpY9+7+
/AvKr1rzQczdAgMBAAE=
-----END PUBLIC KEY-----
```

能看到很明显是RSA的公钥，拿去在线网站**http://tool.chacuo.net/cryptrsakeyparse**进行分解，得到

```
key长度：256
模数：C0332C5C64AE47182F6C1C876D42336910545A58F7EEFEFC0BCAAF5AF341CCDD
指数：65537 (0x10001)

将n转成10进制：869344822960481191906660620034948005889056560172030256172166540583783221035 7
将n分解成pq
p = 285960468890451637935629440372639283459
q = 304008741604601924494328155975272418463
```

这时候其实c、p、q、e都有了，可以直接拿脚本解密，得到flag{decrypt_256}。

```python
import rsa
import gmpy2
e = 65537
n = 86934482296048119190666062003494800588905656017203025617216654058378322103517
p = 285960468890451637935629440372639283459
q = 304008741604601924494328155975272418463
fn = (p-1)*(q-1)
d = int(gmpy2.invert(e,fn))
key = rsa.PrivateKey(n,e,d,q,p)         #在pkcs标准中,pkcs#1规定,私钥包含(n,e,d,p,q)
with open("flag.enc","rb") as f:
    f = f.read()
    print(rsa.decrypt(f,key))
```

五、异性相吸

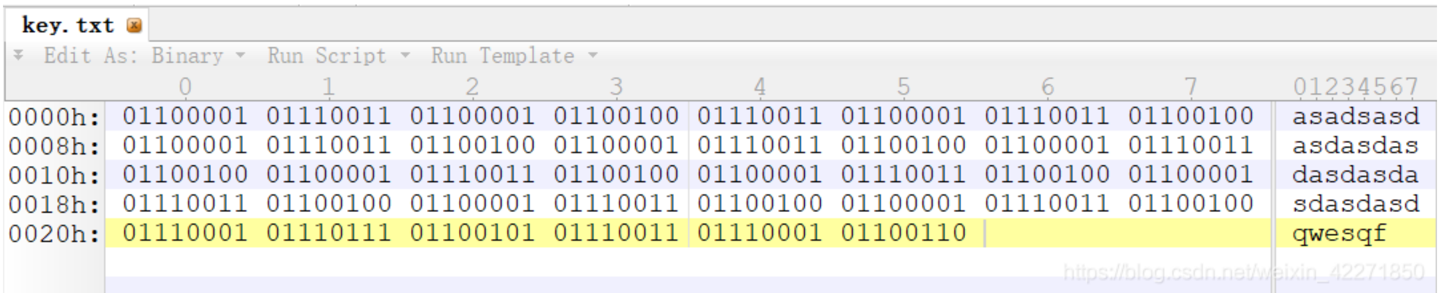
打开题目提示如下内容：

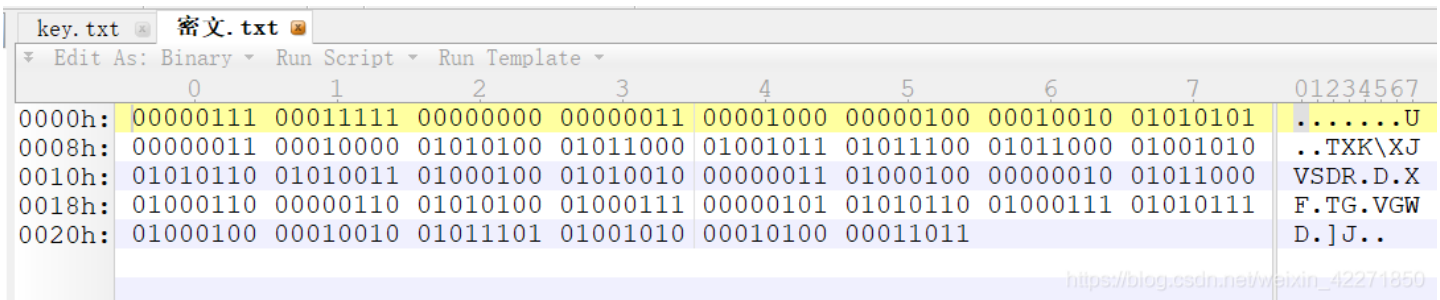
```
最近出现了一个奇葩观点，说性别都不一样，怎么能谈恋爱？为了证明这个观点错误，请大家证明异性是相吸的。
注意：得到的 flag 请包上 flag{} 提交
```

且题目需要我们下载一个压缩包，解压里面有两个文件key.txt和密文.txt，打开后内容如下：

```
#key.txt
asadsasdasdasdasdasdasdasdasdasdqwesqf
#密文.txt
ǒ哂█塔屋鞚卖到腘堂ↄSelf矔嘅均ↄ瓻
```

密文一堆乱码，很容易就联想到用二进制的形式去读取，然后再看到题目提示异性相吸，猜测可能是二进制的异或操作。把两个文件都用101Editor打开，发现两个文件的二进制格式长度一致，更加证明了我们的想法。





```
key = '0110000101110011011000010110010001110011011000010111001101100100011000010111001101100100011000010111001101100100011000010111001101100100011000010111001101100100011000010111001101100100011000010111001101100100011000010111001101100100011000010111001101100100011100010111011101100101011100110111000101100110'
cip = '0000011100011111000000000000001100001000000001000001001001010101000000110001000001010100010110000100101101011100010110000100101001010110010100110100010001010010000000110100010000000010010110000100011000000110010101000100011100000101010101100100011101010111010001000001001001011101010010100001010000011011'
flag = ''
for i in range(0,len(key)):
    if(key[i] == cip[i]):
        flag += '0'
    else:
        flag += '1'
flag = hex(int(flag,2))
print(flag)
```

然后直接将得出的结果通过在线网站**https://www.bejson.com/convert/ox2str**转换为字符串，最终得到结果flag{ea1bc0988992276b7f95b54a7435e89e}。

六、还原大师

打开题目提示如下内容：

```
我们得到了一串神秘字符串：TASC?O3RJMV?WDJKX?ZM,问号部分是未知大写字母，为了确定这个神秘字符串，我们通过了其他途径获得了这个字串的32位MD5码。
但是我们获得它的32位MD5码也是残缺不全，E903???4DAB????08?????51?80??8A?,请猜出神秘字符串的原本模样，并且提交这个字串的32位MD5码作为答案。
注意：得到的 flag 请包上 flag{} 提交
```

看题目大概是一串字符串，有三个明文是未知的。然后也有一串明文MD5加密的内容，也有部分是未知的。只缺了三个且是大写中文，则直接爆破26*26*26此就能得到答案了。直接写脚本爆破，得到答案E9032994DABAC08080091151380478A2。

```
import hashlib
dict = 'ABCDEFGHIJKLNMOPQRSTUVWXYZ'
a = hashlib.md5()
for i in dict:
    for j in dict:
        for k in dict:
            a = hashlib.md5()
            tmp = 'TASC' + i + 'O3RJMV' + j + 'WDJKX' + k + 'ZM'
            a.update(tmp.encode(encoding='utf-8'))
            tmp_md5 = (a.hexdigest()).upper()
            if(tmp_md5[0:4] == 'E903' and tmp_md5[7:11] == '4DAB' and tmp_md5[15:17] == '08' and tmp_md5[22:24] == '51' and tmp_md5[25:27] == '80' and tmp_md5[29:31] == '8A'):
                print(tmp)
                print(tmp_md5)
                break;
```

七、[GKCTF2020]汉字的秘密

打开页面要求我们下载一个文件，内容如下：

```
#题目原题
王壮 夫工 王中 王夫 由由井 井人 夫中 夫夫 井王 土土 夫由
土夫 井中 士夫 王工 王人 土由 由口夫
```

观察一下题目，都是些汉字，那要不就是特殊的编码方式，要不就是替换。百度了一下没找到这类的编码，那大概率就是替换。可以看到题目本身用空格划分了词组，一般是两个有些是三个。基本可以判断不是替换成字母，因为单词不可能都这么短。再观察一下存在大量重复的汉字，那么证明替换后的表达方式应该不会很长，不然不会这么多重复。这时大概就能猜到是替换成数字，刚好ASCII编码的范围也是两位数到三位数。到底这么替换，后面也是百度了writeup才知道这是当铺密码，是每个汉字凸出来的笔画数，如王是6，壮是9。先写一个对应的字典，然后脚本跑一下：

```
dict = {'王':6,'壮':9,'夫':7,'中':2,'由':1,'井':8,'人':3,'土':5,'士':5,'工':4,'口':0}
arr = ['王壮','夫工','王中','王夫','由由井','井人','夫中','夫夫','井王','土土','夫由','土夫','井中','士夫','王工','王人'
,'土由','由口夫']
flag = ''
for i in arr:
    tmp = ''
    for j in i:
        tmp += str(dict[j])
    flag += chr(int(tmp))
print(flag)
```

脚本跑出来的结果比较奇怪，**EJ>CvSHMV7G9R9@?3k**，然后取一下前面几个字符的ASCII值和FLAG对比一下就能得到结果，类似前面变异凯撒一一样在写个脚本跑一下，最后得到结果flag{you_are_good}。

```
E:69   F:70
J:74   L:76
>:62   A:65
C:67   G:71
```

```
dict = {'王':6,'壮':9,'夫':7,'中':2,'由':1,'井':8,'人':3,'土':5,'士':5,'工':4,'口':0}
arr = ['王壮','夫工','王中','王夫','由由井','井人','夫中','夫夫','井王','土土','夫由','土夫','井中','士夫','王工','王人'
,'土由','由口夫']
flag = []
for i in arr:
    tmp = ''
    for j in i:
        tmp += str(dict[j])
    flag.append(int(tmp))
str = ''
for i in range(0,len(flag)):
    str += chr(i+flag[i]+1)
print(str.lower())
```

八、RSAROLL

打开页面要求我们下载一个压缩包，其中题目.txt内容如下：

```
#题目原题
RSA roll! roll! roll!
Only number and a-z
 (don't use editor
which MS provide)
```

另外一个data.txt内容如下：

```
{920139713,19}

704796792
752211152
274704164
18414022
368270835
483295235
263072905
459788476
483295235
459788476
663551792
475206804
459788476
428313374
475206804
459788476
425392137
704796792
458265677
341524652
483295235
534149509
425392137
428313374
425392137
341524652
458265677
263072905
483295235
828509797
341524652
425392137
475206804
428313374
483295235
475206804
459788476
306220148
```

那么一开始给的应该是n和e。先去在线网站分解n，得到p=**18443**，q=**49891**。然后处理一下data.txt，将前面的删掉方便我们按行数读取文件，然后进行解密，结果为flag{13212je2ue28fy71w8u87y31r78eu1e2}。

```
import gmpy2
n = 920139713
e = 19
p = 18443
q = 49891
phi = (p-1) * (q-1)
d = gmpy2.invert(e,phi)
f = open('./test.txt','r')
flag = ''
for lines in f.readlines():
    tmp = pow(int(lines),d,n)
    flag += chr(tmp)
print(flag)
f.close()
```

九、robomunication

打开页面要求我们下载一个压缩包，里面是一个语言里面只有bi和bu两种声音，那么很容易猜到集中可能二进制、摩斯密码、培根密码。先用0.5倍数去记录对应的内容

```
假设  bi 为 .   bu 为 -
.... . .-.. .-.. --- .-- .... .- - .. ... - .... . -.- . -.-- .. - .. ... -... --- --- .--. -... . . .--.
```

然后拿去摩斯解密得到HELLOWHATISTHEKEYITISBOOPBEEP。

十、Unencode

打开页面要求我们下载一个文件，内容如下：

```
#题目原题
89FQA9WMD<V1A<V1S83DY.#<W3$Q,2TM]
```

看题目中由encode可以猜到是一种编码方式，百度下发现是UUencode，通过在线网站**https://www.qqxiuzi.cn/bianma/uuencode.php**解码得到结果flag{dsdasdsa99877LLLKK}。