BUUCTF Crypto 6

原创

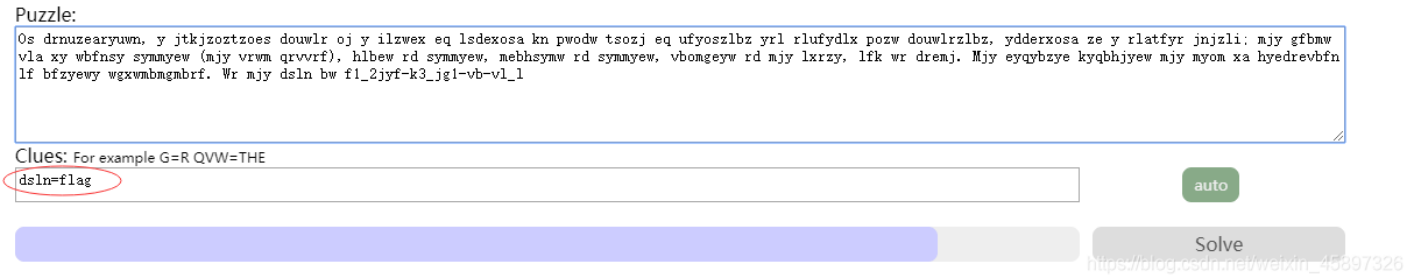
葵。 于 2020-02-15 19:32:28 发布 488 收藏

old-fashion

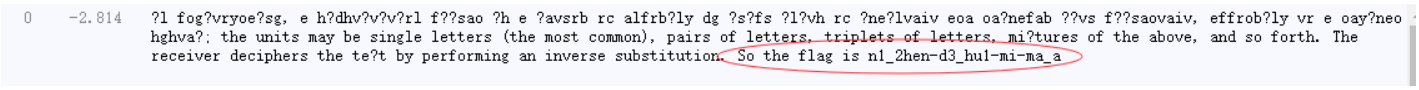
看题目是古典密码，凯撒栅栏暴力破解没发现成句子的，同时怀疑

```
f. Wr mjy dsln bw f1_2jyf-k3_jg1-vb-vl_l
```

这个是flag，感觉是替换密码，找到替换密码的网站，



打上条件dsln=flag，solve
得到



RSA2

依旧是rsa，这次已知e,n,dp,c
也是依旧不会写
直接找的脚本

```python
import gmpy2 as gp

e = 65537
n = gp.mpz(248254007851526241177721526698901802985832766176221609612258877371620580060433101538328030305219918697643619814200930679612109885533801335348445023751670478437073055544724280684733298051599167660303645183146161497485358633681492129668802402065797789905550489547645118787266601929429724133167768465309665906113)
dp = gp.mpz(905074498052346904643025132879518330691925174573054004621877253318682675055421970943552016695528560364834446303196939207056642927148093290374440210503657)

c = gp.mpz(140423670976252696807533673586209400575664282100684119784203527124521188996403826597436883766041879067494280957410201958935737360380801845453829293997433414188838725751796261702622028587211560353362847191060306578510511380965162133472698713063592621028959167072781482562673683090590521214218071160287665180751)

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=gp.invert(e, phin)
        m=gp.powmod(c, d, n)
        if(len(hex(m)[2:])%2==1):
            continue
        print('--------------')
        print(m)
        print(hex(m)[2:])
        print(bytes.fromhex(hex(m)[2:]))
```

```
--------------
3670434958110785066911905751469631231338751225710158680692616521935747246580688484040488309932916523151997
666c61677b776f775f6c65616b696e675f64705f627265616b735f7273613f5f393839323437343333530327d
b'flag{wow_leaking_dp_breaks_rsa?_98924743502}'
```

robomunication

听到MP3的时候我人都傻了，看了一下波形，没法分辨是“.”还是“-”，只能边听边写，最后摩斯电码翻译过来是

答案就是BOOPBEEP喽。

世上无难事

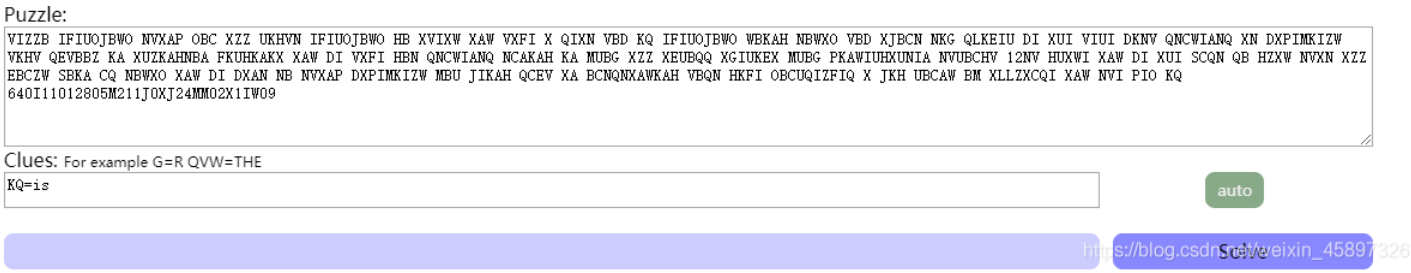
打开附件，看到

KQ 640I11012805M211J0XJ24MM02X1IW09

再加上

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

这几个关键提示，猜测是替换密码，



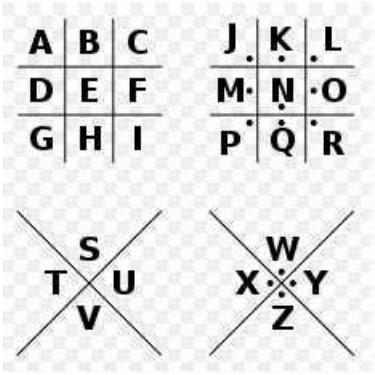
我放的条件是KQ=is，当然也可以PIO=key

0 -1.288 HELLO EVERYBODY THANK YOU ALL RIGHT EVERYBODY GO AHEAD AND HAVE A SEAT HOW IS EVERYBODY DOING TODAY HOW ABOUT TIM SPICER WE ARE HERE WITH STUDENTS AT WAKEFIELD HIGH SCHOOL IN ARLINGTON VIRGINIA AND WE HAVE GOT STUDENTS TUNING IN FROM ALL ACROSS AMERICA FROM KINDERGARTEN THROUGH 12T GRADE AND WE ARE JUST SO GLAD THAT ALL COULD JOIN US TODAY AND WE WANT TO THANK WAKEFIELD FOR BEING SUCH AN OUTSTANDING HOST GIVE YOURSELVES A BIG ROUND OF APPLAUSE AND THE KEY IS 640E11012805F211B0AB24FF02A1ED09

得到flag。

萌萌哒的八戒

看到图片结合题目，明显想到猪圈密码



对照翻译
WHENTHEPIGWANTTOEAT
whenthepigwanttoeat
大小写都试试
发现小写为flag。

异性相吸

题目提示异或，将key和密文转ascii后异或，

```
key=open('Key.txt').read()
se=open('密文.txt').read()
flag=''
for i in range(0,len(key)):
    res=ord(list(se)[i]) ^ ord(list(key)[i])
    flag=flag+chr(res)
print (flag)
```

运行即得结果