

# BUUCTF Crypto 6

原创

葵。 于 2020-02-15 19:32:28 发布 488 收藏

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\\_45897326/article/details/104329140](https://blog.csdn.net/weixin_45897326/article/details/104329140)

版权

## 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 mly 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，

Puzzle:

```
0s drnuzearyuwn, y jtkjzoztzoes douwlr oj y ilzwex eq lsdexosa kn pwodw tsozj eq ufyoszlbz yrl rlufydlx pozw dowlrlzlbz, ydderxosa ze y rlatfyr jnjzli: mly gfbmw  
vla xy wbfnsy symnyew (mly vrwm qrvvrf), hlbew rd symnyew, mehsymw rd symnyew, vbomgeyw rd mly lxrzy, lfk wr dremj. Mly eyqbyze kyqbhyew mly myom xa hyedrevbfm  
lf bfzyewy wgxwmbmgmbrf. Wr mly dsln bw f1_2jyf-k3_jg1-vb-vl_l
```

Clues: For example G=R QVW=THE

dsln=flag

auto

Solve

[https://blog.csdn.net/weixin\\_45897326](https://blog.csdn.net/weixin_45897326)

打上条件dsln=flag，solve

得到

```
0 -2.814 ?l fog?vryoe?sg, e h?dhv?v?v?rl f??sao ?h e ?avsrbc rc alfrb?ly dg ?s?fs ?l?vh rc ?me?lvaiv eoa oa?nefab ??vs f??saovaiv, effrob?ly vr e oay?neo  
hghva?: the units may be single letters (the most common), pairs of letters, triplets of letters, mi?tures of the above, and so forth. The  
receiver decipheres the te?t by performing an inverse substitution. So the flag is n1_2hen-d3_hul-mi-ma_a
```

## RSA2

依旧是rsa，这次已知e,n,dp,c

也是依旧不会写

直接找脚本

```

import gmpy2 as gp

e = 65537
n = gp.mpz(24825400785152624117772152669890180298583276617622160961225887737162058006043310153832803030521991869
7643619814200930679612109885533801335348445023751670478437073055544724280684733298051599167660303645183146161497
485358633681492129668802402065797789905550489547645118787266601929429724133167768465309665906113)
dp = gp.mpz(9050744980523469046430251328795183306919251745730540046218772533186826750554219709435520166955285603
64834446303196939207056642927148093290374440210503657)

c = gp.mpz(14042367097625269680753367358620940057566428210068411978420352712452118899640382659743688376604187906
7494280957410201958935737360380801845453829293997433414188838725751796261702622028587211560353362847191060306578
510511380965162133472698713063592621028959167072781482562673683090590521214218071160287665180751)

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:]))

```

```

-----
36704349581107850669119057514696312313387512257101586806926165219357472465806884840404883099329165231519
97
666c61677b776f775f6c65616b696e675f64705f627265616b735f7273613f5f39383932343734333530327d
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，

Puzzle:

```
VIZZB IFIU0JBWO NVXAP OBC XZZ UKHVN IFIU0JBWO HB XVIXW XAW VXFI X QIXN VBD KQ IFIU0JBWO WBKAH NBWKO VBD XJBCN NKG QLKEIU DI XUI VIUI DKNV QNCWIANQ XN DXPIMKIZW  
VKHY QEVBBZ KA XUZHAKHBA FKUHAKX XAW DI VXFI HBN QNCWIANQ NCAKAH KA MUBG XZZ XEUBQQ XGIUKEK MUBG PKAWIUHKUNIA NVUBCHV 12NV HUXWI XAW DI XUI SCQN QB HZXW NVXN XZZ  
EBCZW SBKA CQ NBWKO XAW DI DXAN NB NVXAP DXPIMKIZW MBU JIKAH QCEV XA BCNQXKXWKAH VBQN HKFI OBCUQIZFIQ X JKH UBCAW BM XLLZXCQI XAW NVI PIO KQ  
640I11012805M211J0XJ24MM02X1IW09
```

Clues: For example G=R QVW=THE

KQ=is

auto

[https://blog.csdn.net/qq\\_45897326](https://blog.csdn.net/qq_45897326)

我放的条件是KQ=is，当然也可以PIO=key

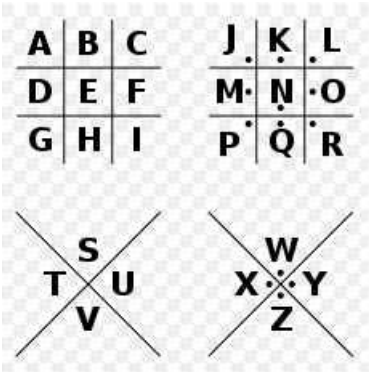
```
0 -1.288 HELLO EVERYBODY THANK YOU ALL RIGHT EVERYBODY GO AHEAD AND HAVE A SEAT HOW IS EVERYBODY DOING TODAY HOW ABOUT TIM SPICER WE ARE HERE WITH  
STUDENTS AT WAKEFIELD HIGH SCHOOL IN ARLINGTON VIRGINIA AND WE HAVE GOT STUDENTS TUNING IN FROM ALL ACROSS AMERICA FROM KINDERGARTEN THROUGH 121  
GRADE 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