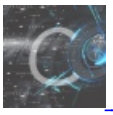
2021-07-03

原创

无名函数 于 2021-07-03 23:54:55 发布 71 收藏

分类专栏： Buu-crypto

本文链接：https://blog.csdn.net/m0_57291352/article/details/118445977



[MRCTF2020]keyboard

题目

```
得到的flag用
MRCTF{xxxxxx}形式上叫
都为小写字母


6
666
22
444
555
33
7
44
666
66
3
```

解题

手机九键

跟[NCTF2019]Keyboard差不多，且比它简单

输出后得到mobilephond

提交显示不对

搜了一下发现解题思路是对的，但是，应该把最后的d换成e

答案

flag{mobilephone}

[BJDCTF2020]signin

题目

welcome to crypto world！！

密文：424a447b57653163306d655f74345f424a444354467d.

解题

very easy

去掉最后的句号只有

十六进制转ASCII码

BJD{We1c0me_t4_BJDCTF}

答案

flag{We1c0me_t4_BJDCTF}

[ACTF新生赛2020]crypto-rsa0

题目

```
怎么办呢，出题人也太坏了，竟然把压缩包给伪加密了！
```

解题

我尝试了暴力破解，时间太长放弃了

尝试了用010editor，将0900都该改成了0000了，但是依旧没有打开

最后直接用WinRAR里带的工具修复文件来修复，然后就能打开了

output

```
90185880664342063772402771624767392713862401730886765262953151639909683470229228412991282745514829264909083992371538834949647434361938539784599470602104117547005673877738257835729760037765213340036696350766324229143613179932145122130685778504062410137043635958208805698698169847293520149572605026492751740223509962069259610194152560033947435941060614738650327920730359549258750560797626266484523488562555758401666405193348626900639493165157502565459374982134762866374558034528907812644460307323698710448703598385686181765862060410550002979817332728160898060144008463923077420655593318749722748449920478494722033903501858806643420637724027716247673927138624017308867652629531516399096834702292284129912827455148292649090839923715388349496474343619385397845994706021041175470056738777382578357297600377652133400366963507663242291436131799321451221306857785040624101370436359582088056986981698472935201495726050264927517402235099620692596101941525600339474359410606147386503279207303595492587505607976262664845234885625557584016664051933486269006394931651575025654593749821347628663745580345289078126444603073236987104487035983856861817658620604105500029798173327281608980601440084639230774206555933187497227484499204784947220339035018588066434206377240277162476739271386240173088676526295315163990968347022922841299128274551482926490908399237153883494964743436193853978459947060210411754700567387773825783572976003776521334003669635076632422914361317993214512213068577850406241013704363595820880569869816984729352014957260502649275174022350996206925961019415256003394743594106061473865032792073035954925875056079762626648452348856255575840166640519334862690063949316515750256545937498213476286637455803452890781264446030732369871044870359838568618176586206041055000297981733272816089806014400846392307742065559331874972274844992047849472203390350
```

rsa0.py

```
from Cryptodome.Util.number import *
import random

FLAG=#hidden, please solve it
flag=int.from_bytes(FLAG,byteorder = 'big')



p=getPrime(512)
q=getPrime(512)

print(p)
print(q)
N=p*q
e=65537
enc = pow(flag,e,N)
print (enc)
```

已知p、q、c、e，常规解就可

```
from Crypto.Util.number import long_to_bytes
import gmpy2

p=90185880664342063772402771624767392713862401730886765262953151639909683470229228412991282745514829264909083992
37153883494964743436193853978459947060210411
q=75470056738777382578357297600377652133400366963507663242291436131799321451221306857785040624101370436359582088
05698698169847293520149572605026492751740223
c=50996206925961019415256003394743594106061473865032792073035954925875056079762626648452348856255575840166640519
33486269006394931651575025654593749821347628663745580345289078126444603073236987104487035983856861817658620604104
55000297981733272816089806014400846392307742065559331874972274844992047849472203390350

n=p*q
e=65537
phi=(p-1)*(q-1)
d = gmpy2.invert(e,phi)
m = gmpy2.powmod(c,d,n)
print (long_to_bytes(m))
```

解出

b’actf{n0w_y0u_see_RSA}’

答案

flag{n0w_y0u_see_RSA}

一张谍报

题目

国家能源总部经过派出卧底长期刺探，终于找到一个潜伏已久的国外内鬼：三楼能源楼管老王。由于抓捕仓促，老王服毒自尽了。侦查部门搜出老王每日看的报纸原来是特制的情报。聪明的你能从附件的报纸中找出情报么？flag是老王说的暗号。（由于老王的线人曾今做的土匪，所以用的行话） 注意：得到的 flag 请包上 flag{} 提交

国家能源时报 2015 年 3 月 5 日

平时要针对性的吃些防辐射菜

对于和电脑“朝夕相处”的人们来说，辐射的确是个让人忧心的“副产物”。因此，平时针对性的吃些可以防辐射的菜是很有好处的。特别是现在接近年底，加班加点是家常便饭，对着电脑更是辐射吸收得满满的，唯有趁一日三餐进食的时候吃点防辐射的食物了。

朝歌区梆子公司三更放炮

老小区居民大爷联合抵制

今天上午，朝歌区梆子公司决定，在每天三更天不亮免费在各大小区门口设卡为全城提供二次臭耳欻聋的酢更提醒，呼吁大家早睡早起，不要因为贪睡断送大好人生，时代的符号是前进。为此，全区老人都蹲在该公司东边树丛合力抵制，不给公司人员放行，场面混乱。李罗厘住进朝歌区五十年了，人称老厘头，几年孙子李虎南刚从东北当猎户回来，每月还寄回来几块鼹鼠干。李罗厘当年遇到的老婆是朝歌一枝花，所以李南虎是长得非常秀气的一个汉子。李罗厘表示：无论梆子公司做的对错，反正不能打扰他孙子睡觉，子曰：‘睡觉乃人之常情’。梆子公司这是连菩萨睡觉都不放过啊。李南虎表示：梆子公司智商捉急，小心居民猴急跳墙！这三伏天都不给睡觉，这不扯淡么！

到了中午人群仍未离散，更有人提议要烧掉这个公司，公司高层似乎恨不得找个洞钻进去。直到治安人员出现才疏散人群归家，但是李南虎仍旧表示爷爷年纪大了，睡不好对身体不好。

朝歌区梆子公司三更放炮

老小区居民大爷联合抵制

今天上午，汪歌区哗叽公司决定，在每天八哇天不全免费在各大小区门脑设卡为全城提供双次臭耳欻聋的酢哇提醒，呼吁大家早睡早起，不要因为贪睡断送大好人生，时代的编号是前进。为此，全区眠人都足在该公司流边草丛合力抵制，不给公司人员放行，场面混乱。李罗鸟住进汪歌区五十年了，人称眠鸟顶，几年孙叽李熬值刚从流北当屁户回来，每月还寄回来几块报信干。李罗鸟当年遇到的眠婆是汪歌一枝花，所以李值熬是长得非常秀气的一个汉叽。李罗鸟表示：无论哗叽公司做的对错，反正不能打扰他孙叽睡觉，叽叶：‘睡觉乃人之常情’。哗叽公司这是连衣服睡觉都不放过啊。李值熬表示：哗叽公司智商捉急，小心居民猴急跳墙！这八伏天都不给睡觉，这不扯淡么！

到了中午人群仍未离散，哇有人提议要烧掉这个公司，公司高层似乎恨不得找个洞钻进去。直到治安人员出现才疏散人群归家，但是李值熬仍旧表示爷爷年纪大了，睡不好对身体不好。

听书做作业

喵汪哗叽双哇顶，眠鸟足屁流脑，八哇报信断流脑全叽，眠鸟进北脑上草，八枝遇孙叽，孙叽对熬编叶：值天衣服放鸟捉猴顶。鸟对：北汪罗汉伏熬乱天门。合编放行，卡编扯呼。人离烧草，报信归洞，孙叽找爷爷。

解题

```
朝歌区梆子公司三更放炮
老小区居民大爷联合抵制
```

有两部分内容，一部分用普通话写的，一部分是老王线人的行话

而笔迹浅的部分也是行话：

```
听书做作业

喵汪哗叽双哇顶，眠鸟足屁流脑，八哇报信断流脑全叽，眠鸟进北脑上草，八枝遇孙叽，孙叽对熬编叶：值天衣服放鸟捉猴顶。鸟对：北汪罗汉伏熬乱天门。合编放行，卡编扯呼。人离烧草，报信归洞，孙叽找爷爷。
```

大概知道是要将这部分翻译为普通话，但是，怎么翻译呢

```
strs1 = "今天上午，朝歌区梆子公司决定，在每天三更天不亮免费在各大小区门口设卡为全城提供二次震耳欲聋的敲更提醒，呼吁大家早睡早起，不要因为贪睡断送大好人生，时代的符号是前进。为此，全区老人都蹲在该公司东边树丛合力抵制，不给公司人员放行，场面混乱。李罗鹰住进朝歌区五十年了，人称老鹰头，几年孙子李虎南刚从东北当猎户回来，每月还寄回来几块鼹鼠干。李罗鹰当年遇到的老婆是朝歌一枝花，所以李南虎是长得非常秀气的一个汉子。李罗鹰表示：无论梆子公司做的对错，反正不能打扰他孙子睡觉，子曰：‘睡觉乃人之常情’。梆子公司这是连菩萨睡觉都不放过啊。李南虎表示：梆子公司智商捉急，小心居民猴急跳墙！这三伏天都不给睡觉，这不扯淡么！到了中午人群仍未离散，更有人提议要烧掉这个公司，公司高层似乎恨不得找个洞钻进去。直到治安人员出现才疏散人群归家，但是李南虎仍旧表示爷爷年纪大了，睡不好对身体不好。"
strs2 = "喵天上午，汪歌区哞叽公司决定，在每天八哇天不全免费在各大小区门脑设卡为全城提供双次震耳欲聋的敲哇提醒，呼吁大家早睡早起，不要因为贪睡断送大好人生，时代的编号是前进。为此，全区眠人都足在该公司流边草丛合力抵制，不给公司人员放行，场面混乱。李罗鸟住进汪歌区五十年了，人称眠鸟顶，几年孙叽李熬值刚从流北当屁户回来，每月还寄回来几块报信干。李罗鸟当年遇到的眠婆是汪歌一枝花，所以李值熬是长得非常秀气的一个汉叽。李罗鸟表示：无论哞叽公司做的对错，反正不能打扰他孙叽睡觉，叽叶：‘睡觉乃人之常情’。哞叽公司这是连衣服睡觉都不放过啊。李值熬表示：哞叽公司智商捉急，小心居民猴急跳墙！这八伏天都不给睡觉，这不扯淡么！到了中午人群仍未离散，哇有人提议要烧掉这个公司，公司高层似乎恨不得找个洞钻进去。直到治安人员出现才疏散人群归家，但是李值熬仍旧表示爷爷年纪大了，睡不好对身体不好。"
strs3 = "喵汪哞叽双哇顶，眠鸟足屁流脑，八哇报信断流脑全叽，眠鸟进北脑上草，八枝遇孙叽，孙叽对熬编叶：值天衣服放鸟捉猴顶。鸟对：北汪罗汉伏熬乱天门。合编放行，卡编扯呼。人离烧草，报信归洞，孙叽找爷爷。"

m = ""
for i in range(len(strs3)):
    for j in range(len(strs2)):
        if strs3[i] == strs2[j]:
            m += strs1[j]
            break
print (m)
```

运行结果

```
今朝梆子二更头，老鹰蹲猎东口，三更鼹鼠断东口亮子，老鹰进北口上树，三枝遇孙子，孙子对虎符曰：南天菩萨放鹰捉猴头。鹰对：北朝罗汉伏虎乱天门。合符放行，卡符扯呼。人离烧树，鼹鼠归洞，孙子找爷爷。
```

flag是老王的暗语，
得到的结果中先是孙子对虎符说的暗语：南天菩萨放鹰捉猴头
也就对应了老王的暗语
答案
flag{南天菩萨放鹰捉猴头}