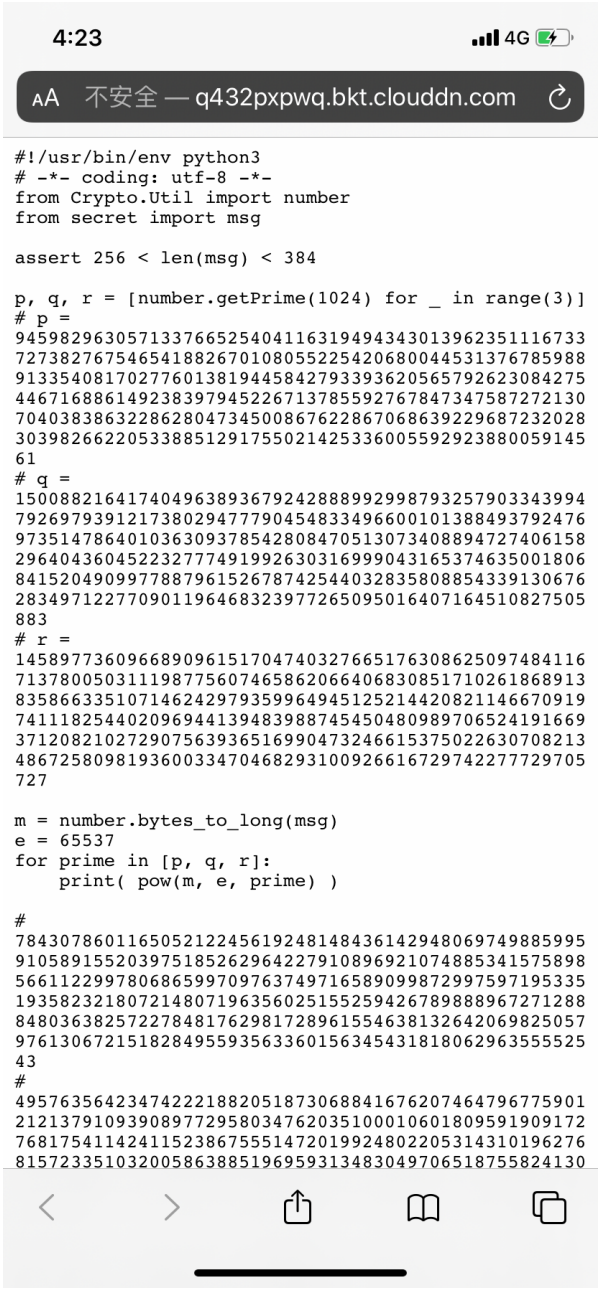
week2

crypto

第二题Remainder

学长们看到截图怕是也一惊，因为疫情，被留在了老家，没有电脑。但是我并不想因为这个而放弃进vidar的机会啊啊啊啊QwQ，想着既然没工具，那就写写密码学，这种在草稿纸上也能写思路的题目，翻找了一下感觉c2比较适合我




```
#!/usr/bin/env python3
# -*- coding: utf-8 -*-
from Crypto.Util import number
from secret import msg

assert 256 < len(msg) < 384

p, q, r = [number.getPrime(1024) for _ in range(3)]
# p =
945982963057133766525404116319494343013962351116733
727382767546541882670108055225420680044531376785988
913354081702776013819445842793393620565792623084275
446716886149238397945226713785592767847347587272130
704038386322862804734500867622867068639229687232028
303982662205338851291755021425336005592923880059145
61
# q =
150088216417404963893679242888992998793257903343994
792697939121738029477790454833496600101388493792476
973514786401036309378542808470513073408894727406158
296404360452232777491992630316999043165374635001806
841520490997788796152678742544032835808854339130676
283497122770901196468323977265095016407164510827505
883
# r =
145897736096689096151704740327665176308625097484116
713780050311198775607465862066406830851710261868913
835866335107146242979359964945125214420821146670919
741118254402096944139483988745450480989706524191669
371208210272907563936516990473246615375022630708213
486725809819360033470468293100926616729742277729705
727

m = number.bytes_to_long(msg)
e = 65537
for prime in [p, q, r]:
    print( pow(m, e, prime) )

#
784307860116505212245619248148436142948069749885995
910589155203975185262964227910896921074885341575898
566112299780686599709763749716589099872997597195335
193582321807214807196356025155259426789888967271288
848036382572278481762981728961554638132642069825057
976130672151828495593563360156345431818062963555525
43
#
495763564234742221882051873068841676207464796775901
212137910939089772958034762035100010601809591909172
768175411424115238675551472019924802205314310196276
815723351032005863885196959313483049706518755824130
```

看一下题目，让我想到了week1的那道rsa（参考了一些教程https://www.freebuf.com/articles/others-articles/161475.html等），好像差不多，但

是显然不一样，这里是有三条方程，百度一下怎么算这种方程，得知中国剩余定理（https://blog.csdn.net/destiny1507/article/details/81751168），利用这个定理可以解出方程。写一个脚本（https://paste.ubuntu.com/p/zwKz6M4dQP），找了一个朋友用teamviewer借用一下电脑（捂脸）
发现打印出来的东西很奇怪，看一下十六进制emmmmm发现除了字母和符号之外还有一些是转义之后是'\n'，想到加个decode看看（还有切片...居然忘记了）
https://paste.ubuntu.com/p/q6tHBMkwMz
这下OK了，其实过程真的非常之艰辛...结果

```
True
763
1hAyuFoOUCamGW9BP7pGKCG81iSEnwAOM8x
********** DO NOT GUESS ME ********
hg In number theory,
am the Chinese
e{ remainder theorem
Cr states that if one
T_  knows the
w0 remainders of the
Nt Euclidean division
+6  of an integer n
Ot by several
h3 integers, then
R_ YOU CAN FIND THE
mE FLAG, ;D
!!
!}
********** USE YOUR BRAIN *********
```