题目：http://www.shiyanbar.com/ctf/1918

Writeup: <http://www.shiyanbar.com/ctf/writeup/1213>

题目：

{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

思路：RSA的算法涉及三个参数，n、e1、e2。**其中，n是两个大质数p、q的积。e1和e2是一对相关的值，e1可以任意取，但要求e1与(p-1）\*(q-1）互质；再选择e2，要求（e2\*e1）mod((p-1）\*(q-1））=1。　　（n，e1）,(n，e2）就是密钥对。其中 (n，e1）为公钥，(n，e2）为私钥。若明文为c,密文为m,则有m=c^e1 mod n ,c=m^e2 mod m.**

解法：

1. 将920139713（即n）拆分成两个较大的素数18443 (p)，49891(q);

分解的Python代码

n = 3  
**while** (n<306713237): *# 306713237 = 920139713/3* **if** (920139713%n == 0):  
 print (n,920139713/n)  
 n = n + 1

1. 求欧拉函数φ(n) = (p-1)(q-1)  值是(49891-1)\*(18443-1) = **920071380。**

e1=19，与φ(n)互素，则存在唯一的x,y,使 **920071380x+19y=1。其中y为e2，可解出e2=** 96849619**。**

**eg:n=143,则p=11,q=13,** φ(n) =120.e1取小于120且与120互素的数，如13，辗转相除：

120=13\*9+3

13=3\*4+1

逆推有：1=13-3\*4 3=120-13\*9 有1=13-（120-13\*9）\*4=-4\*120+37\*13

所以额e2=37.

Python求解代码：

def ext\_euclid ( a , b ):

    if (b == 0):

        return 1, 0, a

    else:

        x , y , q = ext\_euclid( b , a % b )

        x , y = y, ( x - (a // b) \* y )

        return x, y, q

print ext\_euclid(19, 920071380);

3、将每一列密文通过大整数计算器计算得到数字通过ASCLL码转换成字母即可。