目录

[CRYPTO 3](#_Toc23738)

[一. 可直接破解密码 3](#_Toc2532)

[1. Cyberchef 3](#_Toc4756)

[2. Brainfuck(Ook) 3](#_Toc11369)

[3. 福尔摩斯小人编码 4](#_Toc21995)

[4. 音符编码 4](#_Toc31825)

[5. 凯撒编码 4](#_Toc18572)

[6. 键盘编码 4](#_Toc27913)

[7. 敲击编码 4](#_Toc19894)

[8. 五笔输入法编码 5](#_Toc17458)

[9. 中文电码 5](#_Toc20066)

[10. DTMF拨号音识别码 5](#_Toc343)

[11. 3DES编码 5](#_Toc25755)

[12. LOGO编码 5](#_Toc13398)

[13. 零宽度字符隐写编码 6](#_Toc20158)

[14. 汉信码 6](#_Toc16429)

[15. G语言 7](#_Toc20893)

[16. toy-cipter 7](#_Toc13571)

[17. EmojiAES编码 7](#_Toc10459)

[18. 2的次幂阶乘 8](#_Toc936)

[19. OpenSSL 8](#_Toc24310)

[20. RC4 8](#_Toc7646)

[21. ECB加密 8](#_Toc29406)

[22. hashcat爆破 9](#_Toc29227)

[23. 圣堂武士密码 10](#_Toc7945)

[24. Cube密码(魔方密码) 10](#_Toc26378)

[25. JSFuck 11](#_Toc30310)

[26. AES 11](#_Toc22695)

[27. Affine Cipter(仿射密码) 11](#_Toc28056)

[28. 在线RSA解密 12](#_Toc30100)

[29. 其他各种编码 12](#_Toc23396)

[二. Python脚本 13](#_Toc31258)

[1. 词频统计解码 13](#_Toc4407)

[2. Base64解码 13](#_Toc1807)

[3. base64套娃 13](#_Toc29997)

[4. base16&base32&base64&base85套娃 13](#_Toc30806)

[5. 各种base编码解码测试 13](#_Toc4353)

[6. 大数递归 13](#_Toc123)

[7. Shamir’s Secret密码 14](#_Toc26061)

[8. LSFR爆破(B-M算法) 14](#_Toc14852)

[9. Diffie–Hellman密钥交换协议(DF) 14](#_Toc4745)

[10. boneh and durfee(DSA)(加强版wiener) 14](#_Toc9324)

[11. ECDSA(椭圆曲线参数)&&恶意签名&RSA加密模板 14](#_Toc2974)

[12. TEA解密 15](#_Toc29160)

[13. pyc脚本 15](#_Toc21524)

[三. Python写法 15](#_Toc29800)

[四. RSA 18](#_Toc27930)

[1.yafu 18](#_Toc11111)

[2.参数r 18](#_Toc5893)

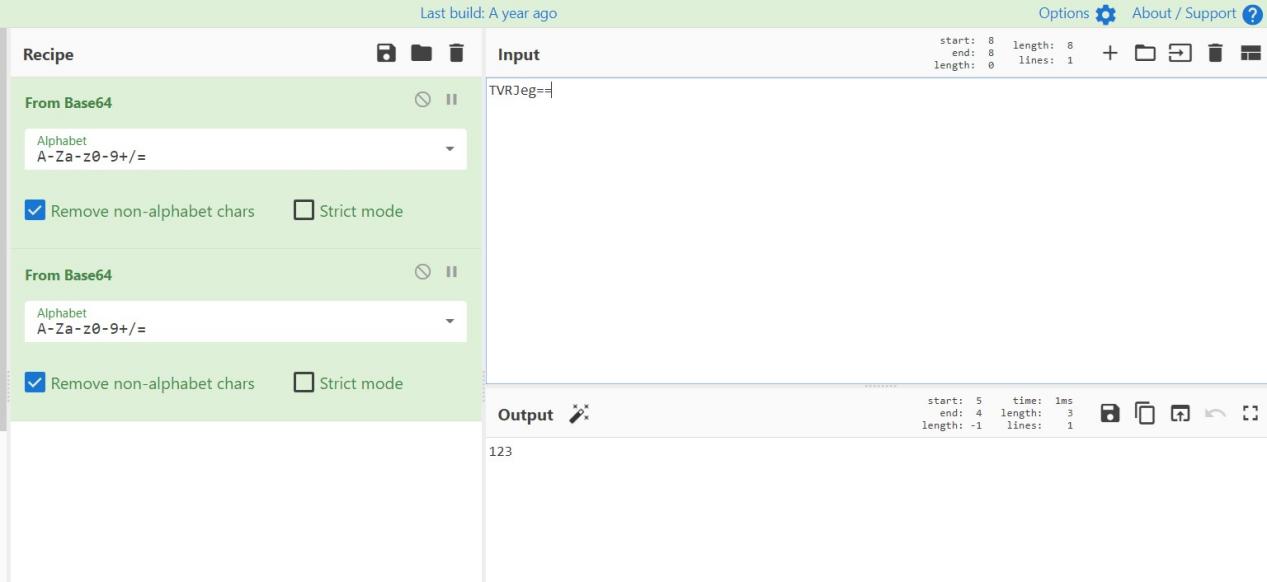
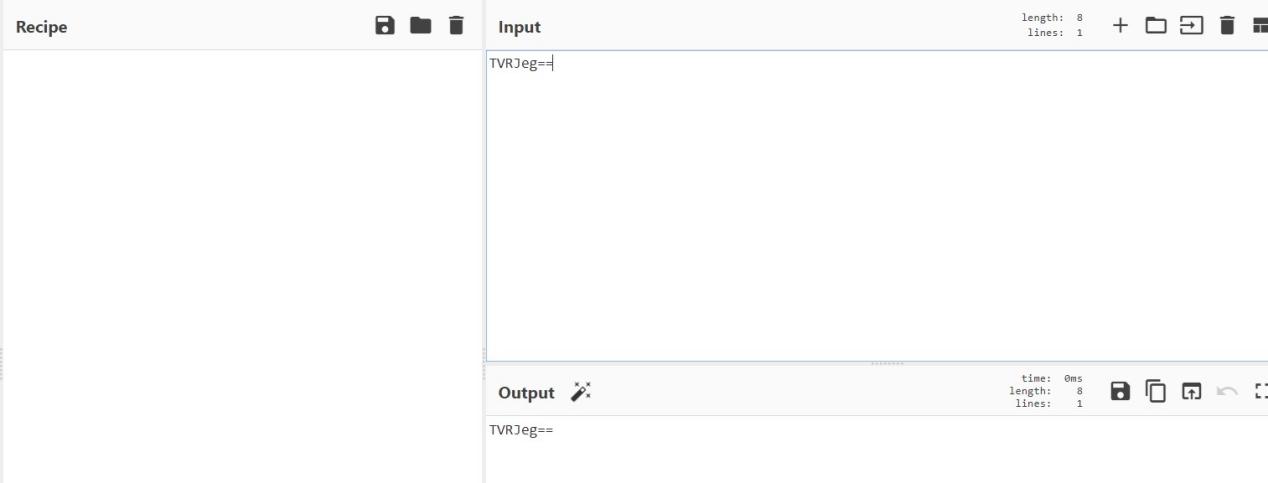
[五. Sagemath 18](#_Toc16784)

# CRYPTO

## 可直接破解密码

### Cyberchef

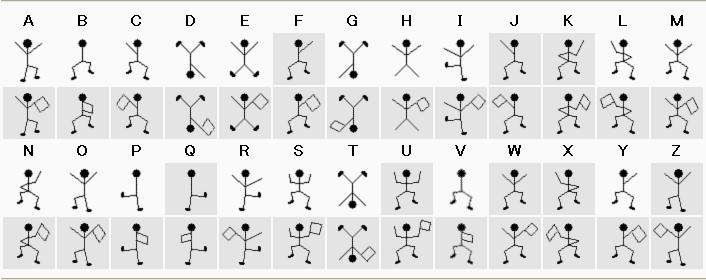
直接将密文放到cyberchef中，注意有的需要手动加上=号(例如BASE32)，点击画笔即可得到解密后的明文



### Brainfuck(Ook)

网站<https://www.splitbrain.org/services/ook>破解，注意brainfuck编码前缀为++++++++，如果缺少需要补上才能解码

### 福尔摩斯小人编码



### 音符编码

网站https://www.qqxiuzi.cn/bianma/wenbenjiami.php?s=yinyue破解

### 凯撒编码

位移为1-25，例如位移为1的密文gmbh对应明文为flag

### 键盘编码

例如RESXC对应键盘上的图案为C

### 敲击编码

每个字母按照/分割，空格两边.的数量为坐标值

例如..... ../... ./... ./... ../代表wllm



### 五笔输入法编码

类似bnhn s wwy vffg vffg rrhy fhnv 对应 也 要 从 娃 娃 抓 起

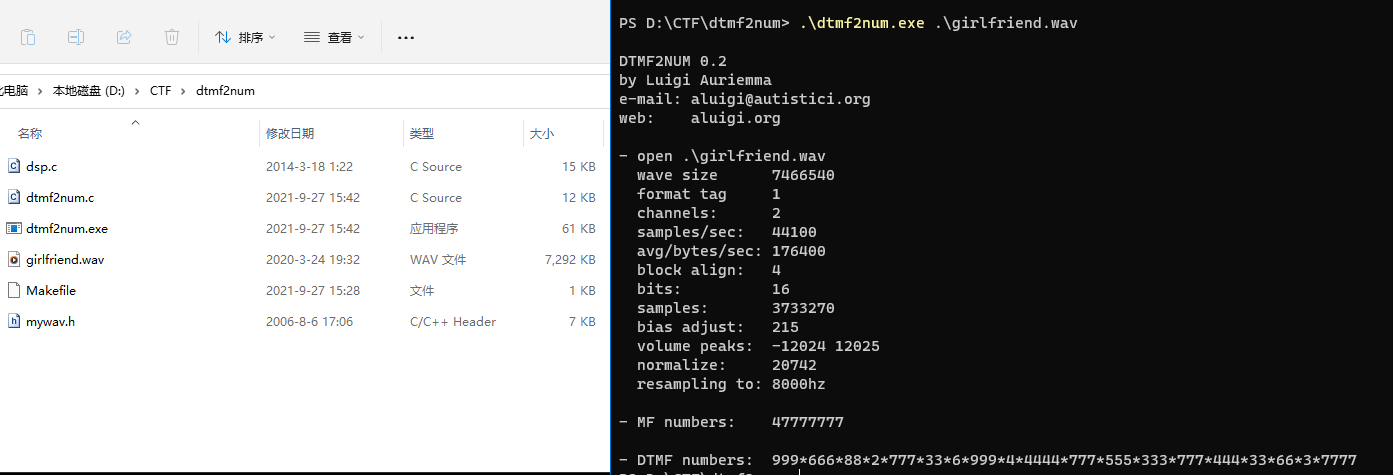
### 中文电码

<http://code.mcdvisa.com/> 网站查询

类似0086 1562 2535 5174 对应 人 工 智 能

### DTMF拨号音识别码

将音频放在dtmf2num文件夹，文件夹打开cmd运行.\dtmf2num.exe .\文件名得到DTMF码

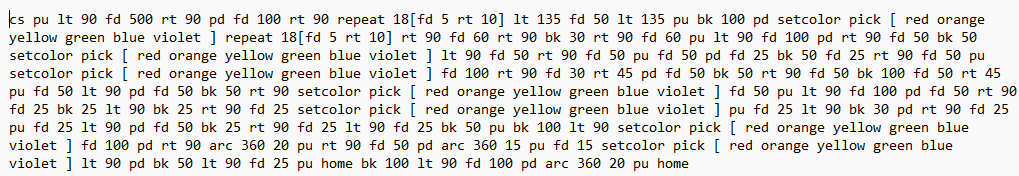


### 3DES编码

<https://www.sojson.com/encrypt_triple_des.html> 编码解码

### LOGO编码

类似：

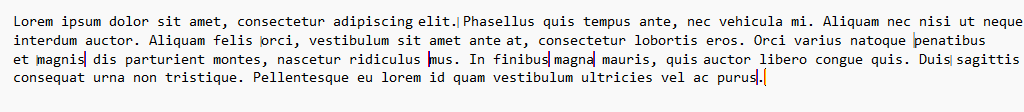


使用网站：<https://www.calormen.com/jslogo/> 将上面的文本粘贴并点击执行即可回显结果



### 零宽度字符隐写编码

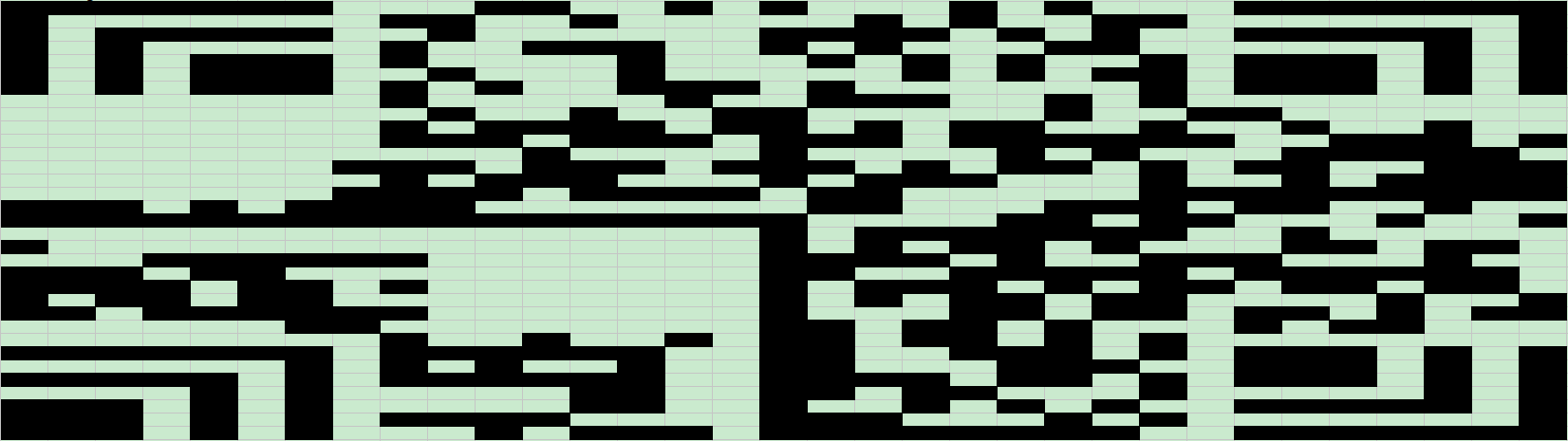
类似：



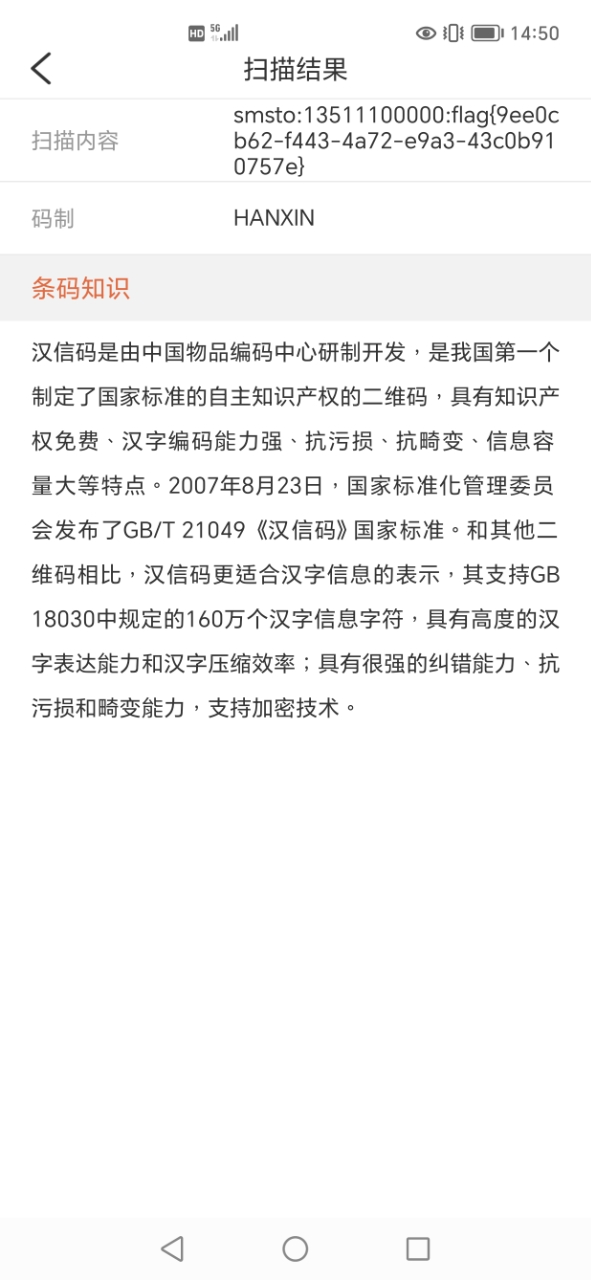
使用网站：<https://www.calormen.com/jslogo/> 将上面的文本粘贴并点击Decode解码

### 汉信码

汉信码：

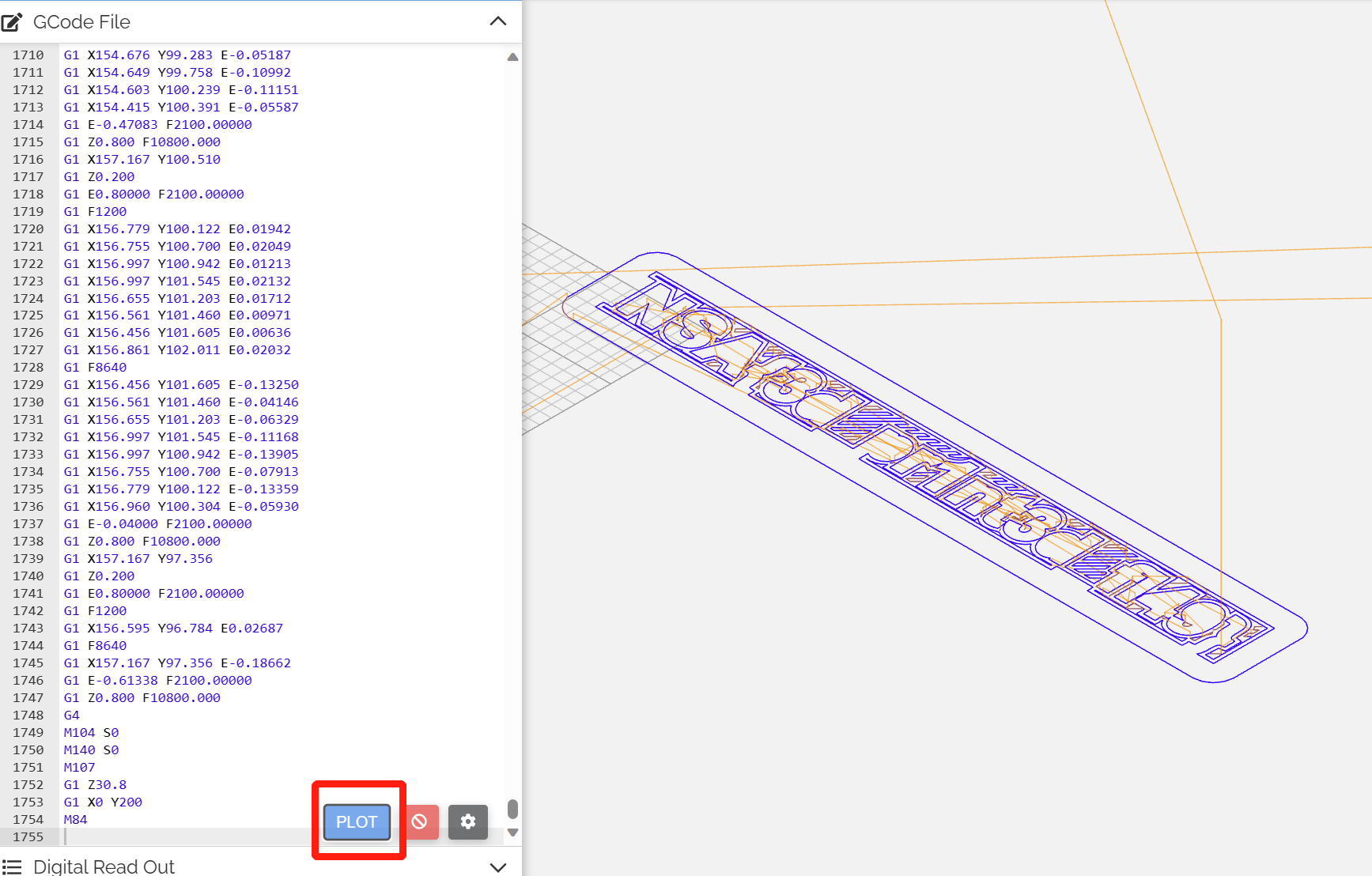


手机用中国编码软件扫描得



### G语言

使用网站：https://ncviewer.com，将代码沾到左侧，点击PLOT即可



### toy-cipter

根据下面pdf的对照关系解密即可



### EmojiAES编码

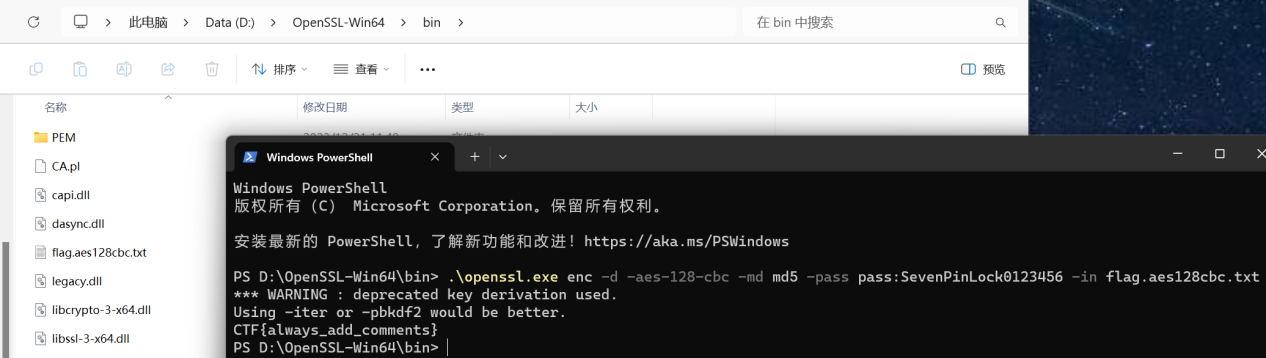
带密码的emoji解码。使用网站：https://aghorler.github.io/emoji-aes/

### 2的次幂阶乘

访问：<https://oeis.org/A244060/list>

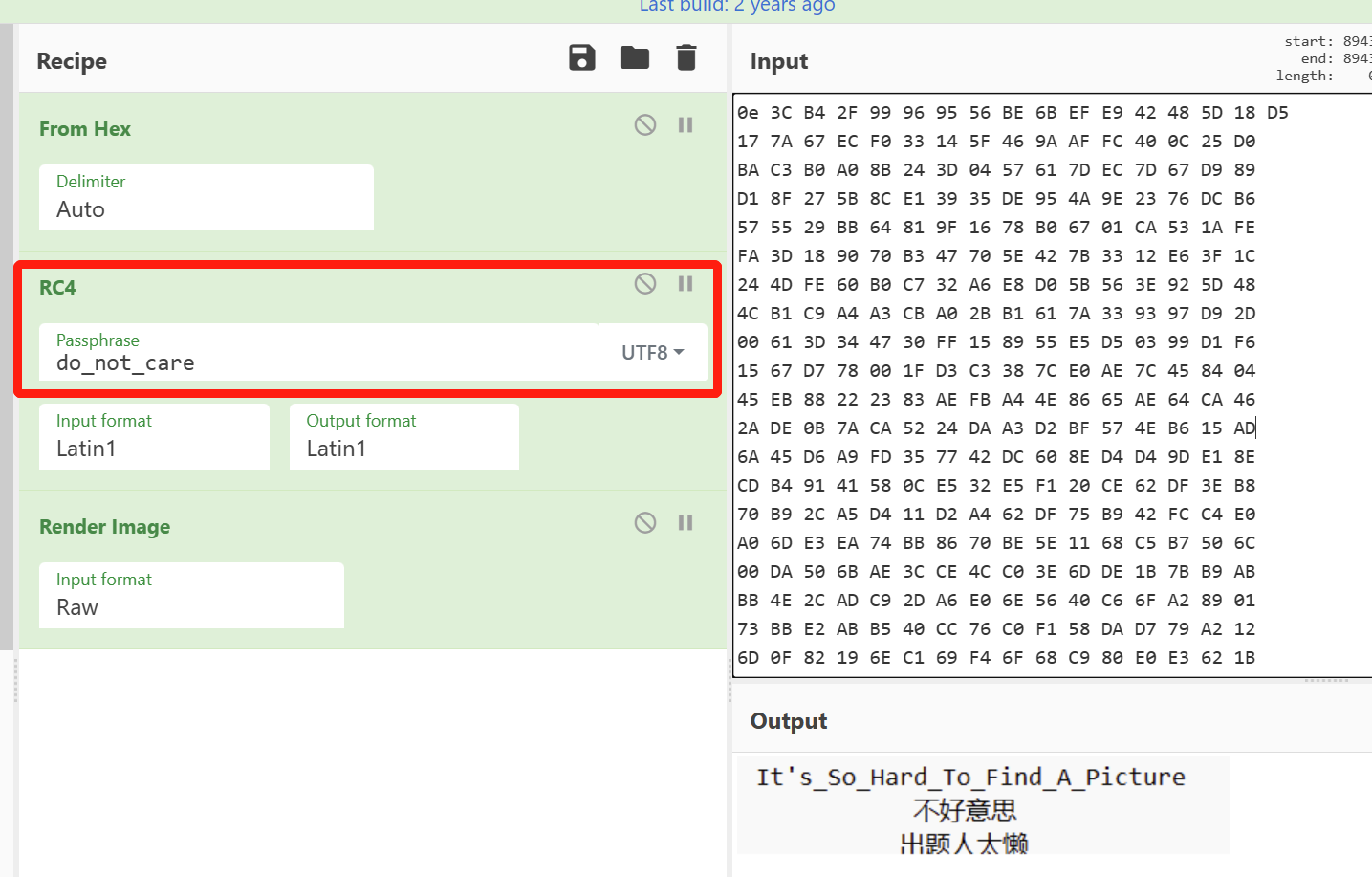
### OpenSSL

将加密文件改为txt格式，在OpenSSL的bin目录下打开cmd，输入：.\openssl.exe enc -d 加密类型 -md md5 -pass pass:密码 -in 文件名



### RC4

cyberchef根据key进行加密，加密两次就等于解密结果，密文一般叫raw



### ECB加密

ECB加密是16位一组，每组相互独立，加密后每组为32位，例如：({"first\_name":"A1.00000000000000","last\_name":"last","is\_admin":0}对应的ECB格式可以将字符串拆分为5组，也就是：

# 第一组{"first\_name":"A

# 第二组1.00000000000000

# 第三组","last\_name":"l

# 第四组ast","is\_admin":

# 第五组0}

)，json中1.00000000000000=1，所以可以构造：(

# 第一组{"first\_name":"A

# 第二组1.00000000000000

# 第三组","last\_name":"l

# 第四组ast","is\_admin":

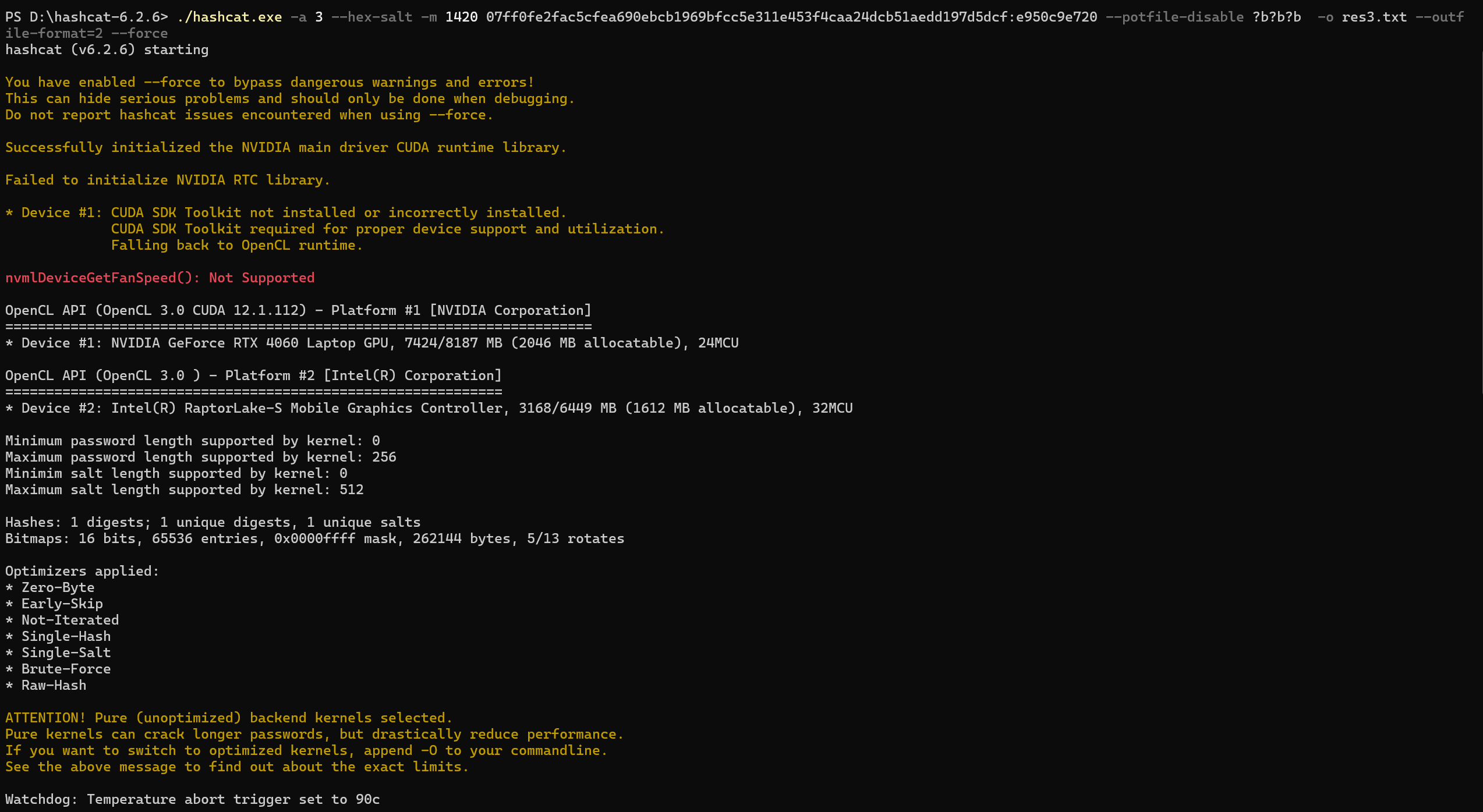
# 第五组1.00000000000000

# 第六组0}

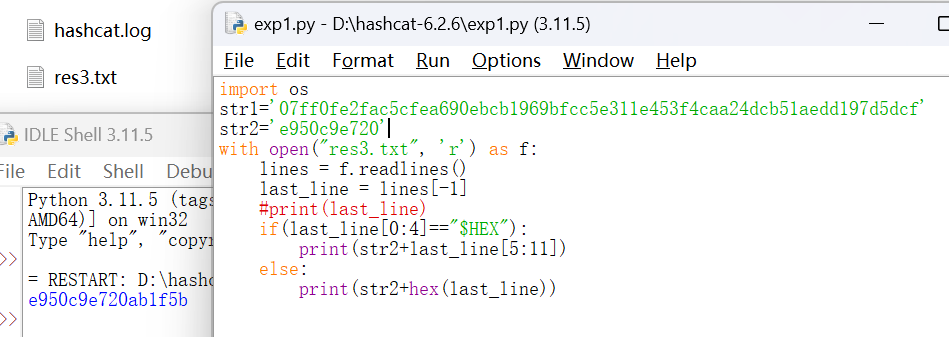
来实现{"first\_name":"A1.00000000000000","last\_name":"last","is\_admin":1}，对应ECB字符串前128位+32到64位的字符串+128位后的字符串)

### hashcat爆破

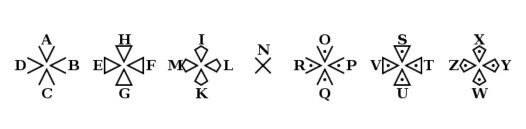
在hashcat-6.2.6文件夹打开cmd，输入：./hashcat.exe -a 3 --hex-salt -m hash加密的16进制值:16进制前缀值 --potfile-disable ?b?b?b -o res3.txt --outfile-format=2 --force，得到res3.txt文件



之后在当前文件夹运行exp.py脚本(注意修改hash加密的16进制值和16进制前缀值为对应值)



### 圣堂武士密码



### Cube密码(魔方密码)

题目会给出双方公钥和发送信息，例如：

Mr. A public key: [B' U', F B F, R' D, B D']

Mr. G public key: [R D L', D U' B, U F', L' F]

Mr. A sends: [B D' R' D R D L' D' R D B', B D' R' D D U' B D' R D B', B D' R' D U F' D' R D B', B D' R' D L' F D' R D B']

Mr. G sends: [U F' R D L' B' U' L D' R' F U', U F' R D L' F B F L D' R' F U', U F' R D L' R' D L D' R' F U', U F' R D L' B D' L D' R' F U']

可得：

(a1, a2, a3)=[B' U', F B F, R' D, B D']

(B-1 a1 B,B-1 a2 B,B-1 a3 B,B-1 a4 B)=[U F' R D L' B' U' L D' R' F U', U F' R D L' F B F L D' R' F U', U F' R D L' R' D L D' R' F U', U F' R D L' B D' L D' R' F U']

这里B-1 a1 B中的B' U' 是a1的值，那么B-1也就是U F' R D L'，同理：

B-1 = U F' R D L'  
B=L D' R' F U'(也就是B-1倒序后且是否有’互换得到)

A-1=BD'R'D  
A=D'RDB'

则公共密钥e = A-1 B-1 A B = B D' R' D U F' R D L' D' R D B' L D' R' F U'

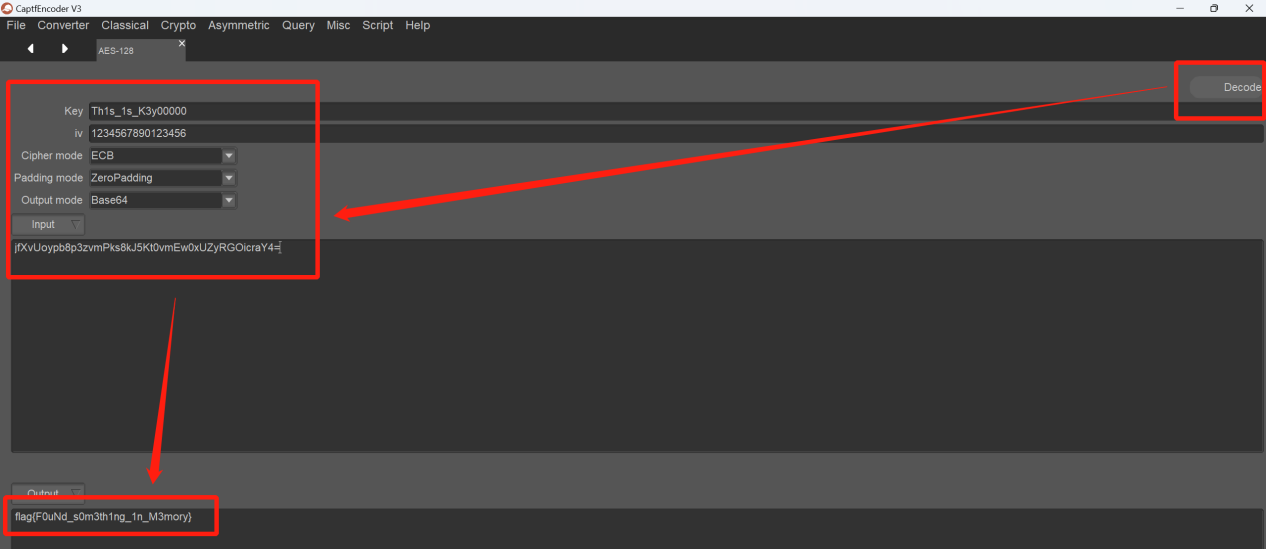
### JSFuck

JSFuck解密脚本



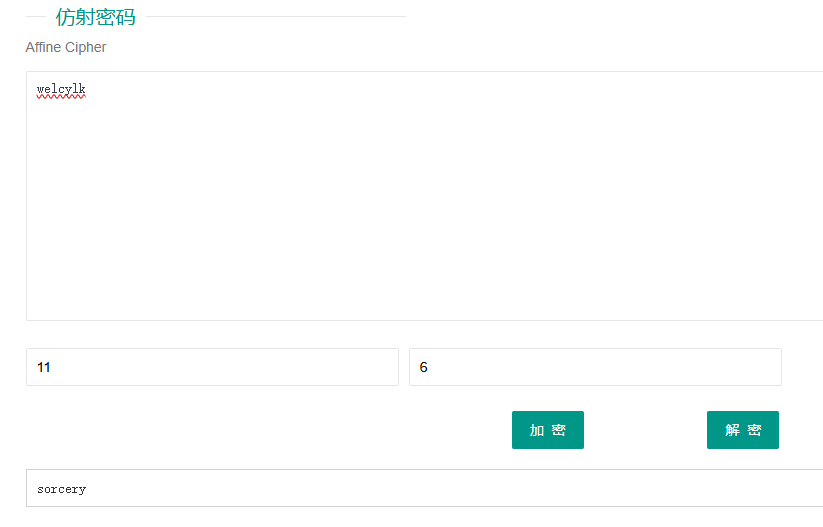
### AES

使用软件CaptfEncoder解密



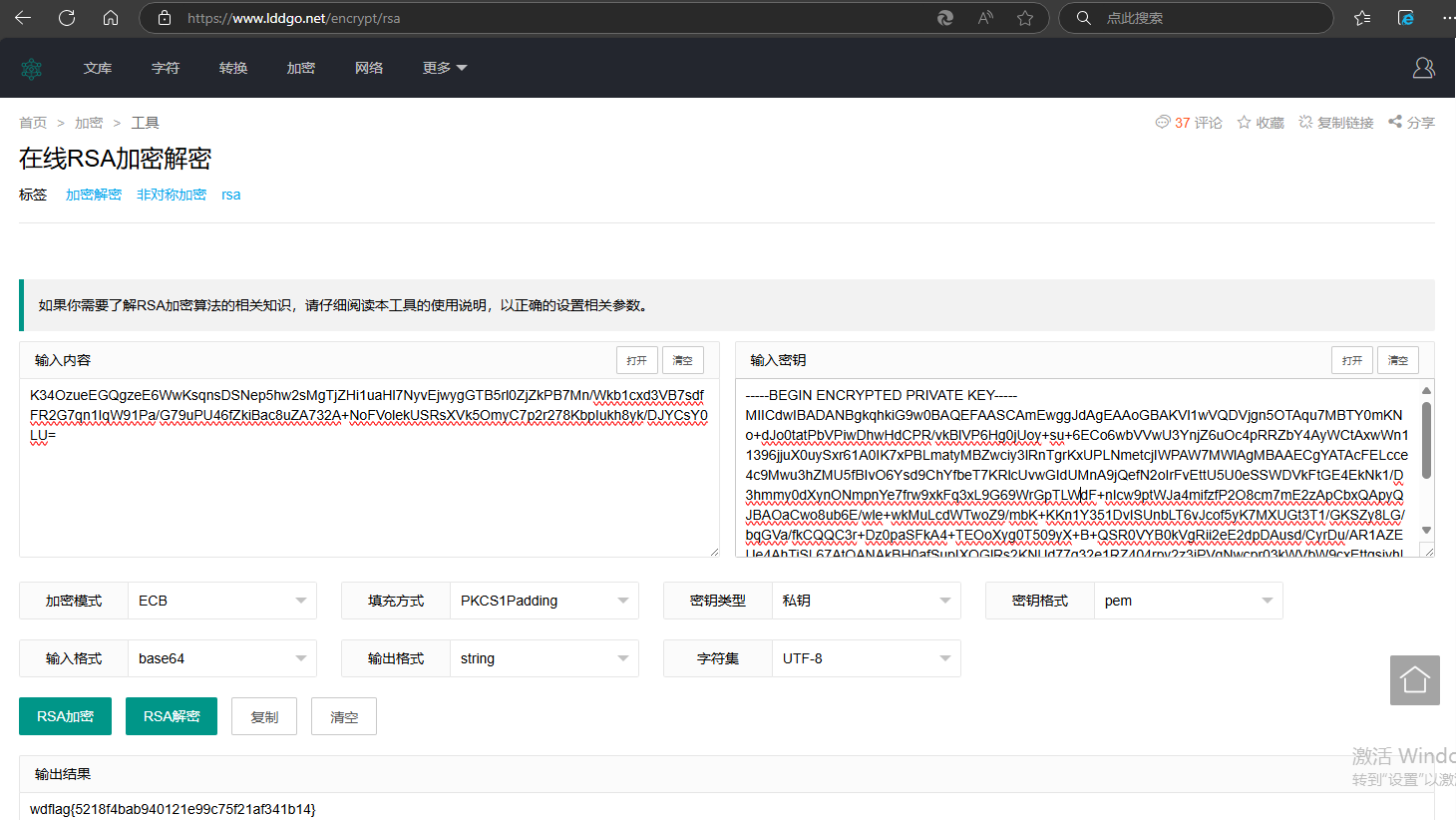
### Affine Cipter(仿射密码)

加密方式c=am+b (mod 26)，例如e(x)=11x+6(mod26)，密文：welcylk



### 在线RSA解密

访问：https://www.lddgo.net/encrypt/rsa



### 其他各种编码

注意字符窜反转，如果乱套啥都有可以试试uuencode:https://www.qqxiuzi.cn/bianma/uuencode.php

剩下可以去<http://www.hiencode.com/>找

## Python脚本

### 词频统计解码



### Base64解码



### base64套娃

注意根据需求文件修改文件名



### base16&base32&base64&base85套娃



### 各种base编码解码测试

注意根据需求修改加密字符串



### 大数递归

注意根据需求修改递归函数的大数



### Shamir’s Secret密码

有一堆MD5两两构成：

(C81E728D9D4C2F636F067F89CC14862C, 31E96A93BF1A7CE1872A3CCDA6E07F86)

(ECCBC87E4B5CE2FE28308FD9F2A7BAF3, ADF6E4F1052BDE978344743CCDCF5771)

(E4DA3B7FBBCE2345D7772B0674A318D5, 0668FBCFE4098FEA0218163AC21E6531)

解密脚本(根据上面解密的MD5结果使用)：



### LSFR爆破(B-M算法)

脚本如下(根据题目修改爆破位数)：



### [Diffie–Hellman密钥交换协议](https://cloud.tencent.com/developer/article/1670498)(DF)

已知私钥，协商数据，保证长度的质数求解，例如：私钥=9360，协商数据=57687185873717832710418532982088，保证长度的质数为=72542982052896163041354492265957。则答案=pow(B,a,p)=pow(协商数据,私钥,保证长度的质数)=37799067929880674766269861874334

### boneh and durfee(DSA)(加强版wiener)

注意修改参数值



### ECDSA(椭圆曲线参数)&&恶意签名&RSA加密模板

题目：，解题脚本：

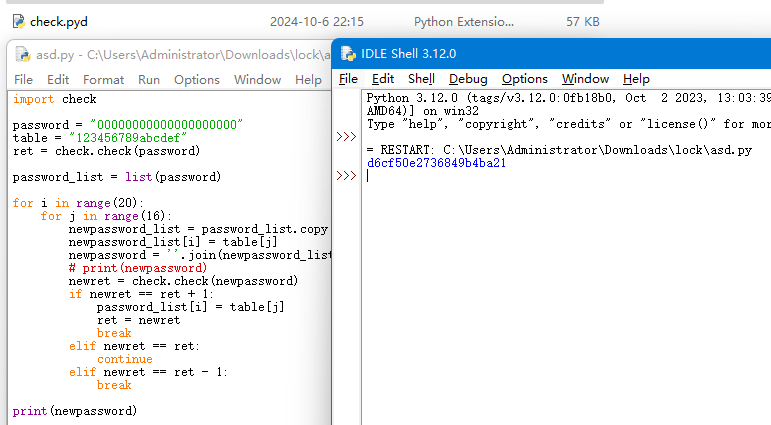
### TEA解密

注意修改参数值



### pyc脚本

pyc文件可以用python直接import引用



## Python写法

查看python包使用方法：

help(包名)

查看python包函数：

dir(包名)

MD5：

import hashlib

s = 'T'

res = hashlib.md5(s.encode('utf-8')).hexdigest().upper()

字符串替换：

temp1 = s.replace('?', str(chr(65 + i)), 1) #把第一个？替换为str(chr(65 + i)

读文件：

with open(filename, 'r') as f:

line = f.read()

idx = line.index(':') 定位某个字符(':')

dec\_data = int(line[:idx - 1]) 取某个字符(':')前的数值

hex\_data += f'{dec\_data:04x}' 数字(dec\_data)转16进制

next\_file = line[-36:] 取内容后36位字符

写文件： with open(zipfile, 'wb') as ff: 文件路径字符串(zipfile)

ff.write(binascii.unhexlify(hex\_data)) 16进制转二进制写进内容到文件判断素数：

gmpy2.is\_prime()

判断奇数：

gmpy2.is\_even()

判断偶数：

gmpy2.is\_odd()

求幂：

\*\*

正常除法：

//

对a开b次方：

gmpy2.iroot(a,b)

最小公倍数(gmpy2.lcm(a,b))乘最大公约数(gmpy2.gcd(a,b))等于两数乘积

模逆：

gmpy2.invert(a,c)对a，求b，使a\*b=1(mod c)

ASCII转字符：

chr(11)

字符转ASCII：

ord('a')

取字符串长度：

len(str)

BASE64编码4位一爆破

json.dumps()：json.dumps将一个Python数据结构转换为JSON

[-1]代表取字符串最后一位

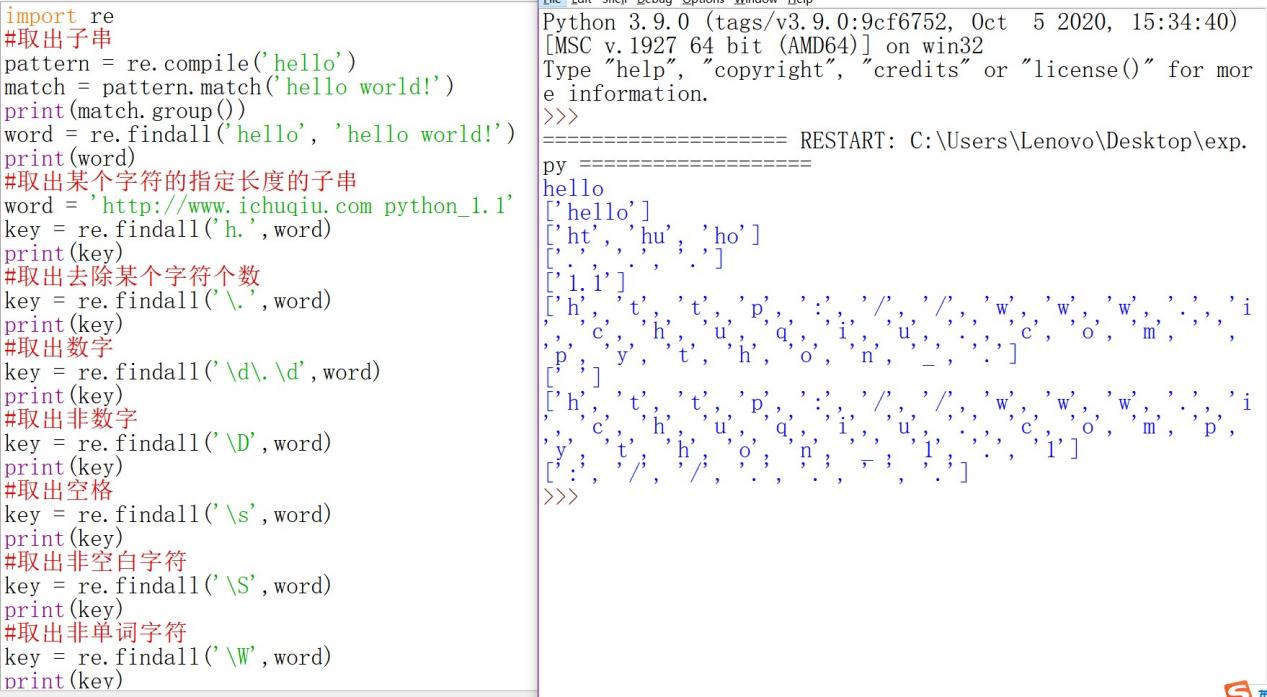
bin(i)取得数字i的二进制字符串

[::-1]涉及到将数字或字符串倒序输出

base36.dumps(c)将c转为36进制（import base36即可）

gettrandbits(32)生成32字节随机数

正则表达式：



bytes()方法，将数字类型数组转换为字符串:

lst = [72, 101, 108, 108, 111, 44, 32, 87, 111, 114, 108, 100, 33]

b = bytes(lst)

print(b) # 输出：b'Hello, World!'

数字转字节数组转16进制：ciphertext = [123],bytes(ciphertext).hex()

bytes(ciphertext)得到:b’{,再加上.hex()可以得到16进制数:7b

二进制数：binary = bin(i)

二进制数中某一位的个数：binary.count('1')

字符串连接：''.join([path, next\_file])

建立表结构数组（下表与值一一对应）：cipherdic = {'M':'ACEG','R':'ADEG','K':'BCEG','S':'BDEG'}

二维数组(bins)变一维数组(长宽比388：100)：flag = np.array(bins,np.uint8).reshape(388,100)

数组(flag)变图片：Image.fromarray(flag).save('flag.bmp')

读取带参数的文件：y=eval(open("attachment.txt","r").read())

循环传递文件中参数值得到结果：print([chr(y.subs(x,i)) for i in range(57)])

建立大跟堆a，存入数值1：

import heapq

heapq.heappush(a, 1)

列表变成大根堆：

a=[3,6,1]

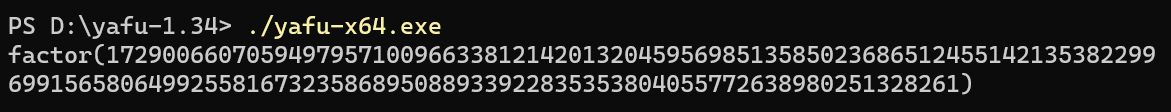
heapify(a) #将a变成堆之后，可以对其操作，a为[1,3,6]

heappop(a) #堆首部元素出堆，a为[3,6]

## RSA

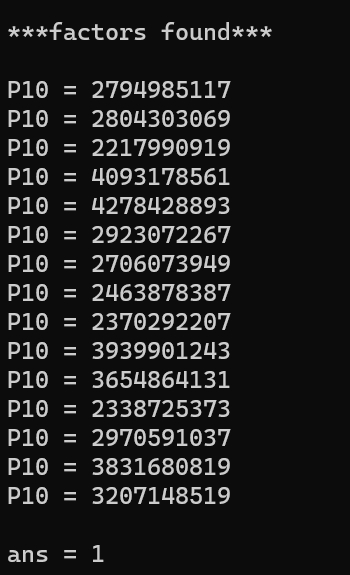
### 1.yafu

在yafu文件夹打开cmd，输入./yafu-x64.exe，之后输入factor(n值)即可分解



### 2.参数r

已知r = (x \* p + q) // n以及n的值，可求p = gcd(n, r)



如果算式a\*算式b=已知值，且算式a\*算式c=已知值，那么算式a的值为两个已知值的gcd

## Sagemath

右键粘贴代码后回车运行

