一些Crypto的基础题

原创

sheepbotany 已于 2022-04-06 13:34:45 修改 56 收藏

分类专栏： CTF 文章标签： crypto BUUCTF CTF ZJNUCTF

于 2022-04-05 10:27:36 首次发布

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/lllwky/article/details/123965134

版权

 CTF 专栏收录该内容

5 篇文章 0 订阅

订阅专栏

文章目录

前言

并非完全的原创，有些是参考了网上的wp，在这里做个整理，如果侵权可以私信联系。

一：一眼就解密 base64 SEITX1NUUklOR30=

ZmxhZ3tUSEVfRkxBR19PRl9USEITX1NUUklOR30=

有等于号是bace64的特征

CTF在线工具-在线base编码|在线base解码|base16编码|base32编码|base64编码 (hiencode.com)

二：看我回旋踢 synt{：凯撒密码

密码：synt{5pq1004q-86n5-46q8-o720-oro5on0417r1}

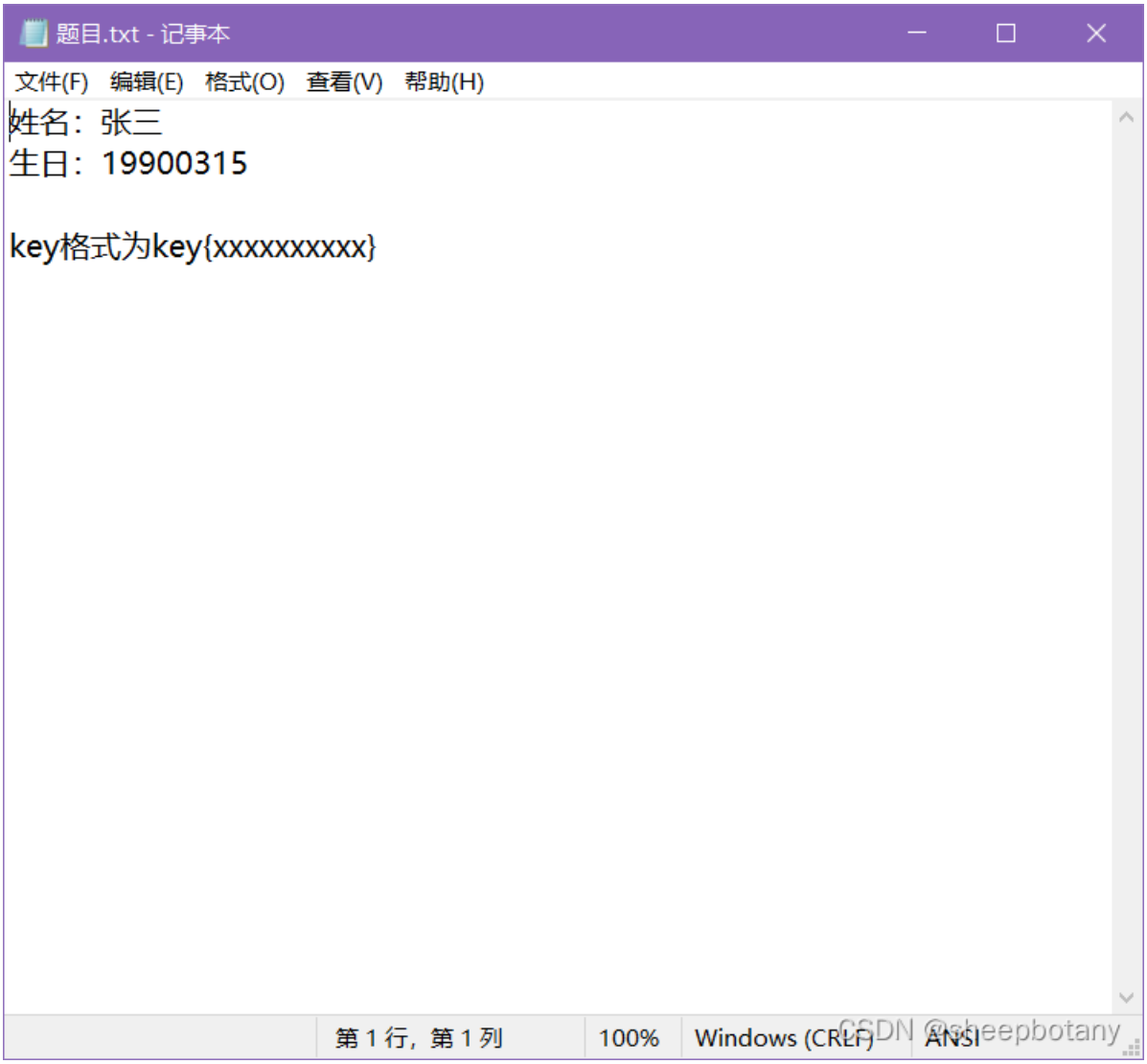
此为凯撒密码，网址为：

凯撒密码在线计算-ME2在线工具 (metools.info)

为什么加密位移为13：一个个试出来，如果显示为flag，则加密位移为13

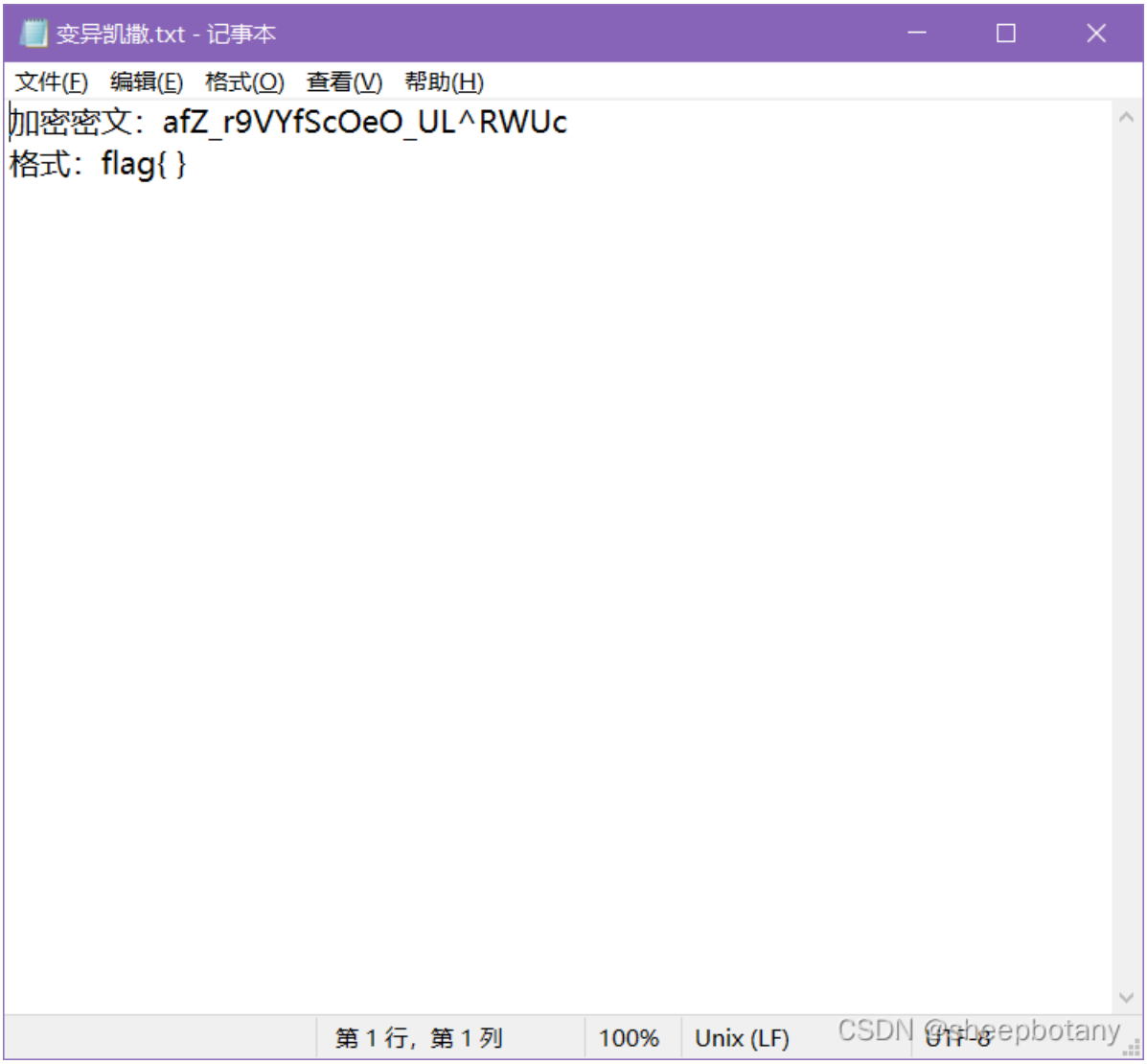
三：password

这个题目简直有毒，但是看题解分析密码有十个，张三19900315正好十个数字



flag{zs19900315}

四:变异凯撒 ASCII



在密码学中，恺撒密码（英语：Caesar cipher），或称恺撒加密、恺撒变换、变换加密，是一种最简单且最广为人知的加密技术。它是一种替换加密的技术，明文中的所有字母都在字母表上向后（或向前）按照一个固定数目进行偏移后被替换成密文。例如，当偏移量是3的时候，所有的字母A将被替换成D，B变成E，以此类推。

前三个字母afZ_对应flag，而凯撒密码也意味着字母的对应是符合顺序规律的

我们查看ASCII表

ASCII表

（ American Standard Code for Information Interchange 美国标准信息交换代码 ）

高四位 / 低四位		ASCII控制字符 0000						ASCII控制字符 0001						ASCII打印字符 0010		ASCII打印字符 0011		ASCII打印字符 0100		ASCII打印字符 0101		ASCII打印字符 0110		ASCII打印字符 0111		
		0						1						2		3		4		5		6		7		
		十进制	字符	Ctrl	代码	转义字符	字符解释	十进制	字符	Ctrl	代码	转义字符	字符解释	十进制	字符	十进制	字符	十进制	字符	十进制	字符	十进制	字符	十进制	字符	Ctrl
0000	0	0		^@	NUL	\0	空字符	16	►	^P	DLE		数据链路转义	32		48	0	64	@	80	P	96	`	112	p	
0001	1	1	☺	^A	SOH		标题开始	17	◄	^Q	DC1		设备控制 1	33	!	49	1	65	A	81	Q	97	a	113	q	
0010	2	2	☻	^B	STX		正文开始	18	↕	^R	DC2		设备控制 2	34	"	50	2	66	B	82	R	98	b	114	r	
0011	3	3	♥	^C	ETX		正文结束	19	‼	^S	DC3		设备控制 3	35	#	51	3	67	C	83	S	99	c	115	s	
0100	4	4	♦	^D	EOT		传输结束	20	¶	^T	DC4		设备控制 4	36	$	52	4	68	D	84	T	100	d	116	t	
0101	5	5	♣	^E	ENQ		查询	21	§	^U	NAK		否定应答	37	%	53	5	69	E	85	U	101	e	117	u	
0110	6	6	♠	^F	ACK		肯定应答	22	▬	^V	SYN		同步空闲	38	&	54	6	70	F	86	V	102	f	118	v	
0111	7	7	•	^G	BEL	\a	响铃	23	↨	^W	ETB		传输块结束	39	'	55	7	71	G	87	W	103	g	119	w	
1000	8	8	◘	^H	BS	\b	退格	24	↑	^X	CAN		取消	40	(	56	8	72	H	88	X	104	h	120	x	
1001	9	9	○	^I	HT	\t	横向制表	25	↓	^Y	EM		介质结束	41	)	57	9	73	I	89	Y	105	i	121	y	
1010	A	10	◙	^J	LF	\n	换行	26	→	^Z	SUB		替代	42	*	58	:	74	J	90	Z	106	j	122	z	
1011	B	11	♂	^K	VT	\v	纵向制表	27	←	^[	ESC	\e	溢出	43	+	59	;	75	K	91	[	107	k	123	{	
1100	C	12	♀	^L	FF	\f	换页	28	∟	^\	FS		文件分隔符	44	,	60	<	76	L	92	\	108	l	124	|	
1101	D	13	♪	^M	CR	\r	回车	29	↔	^]	GS		组分隔符	45	-	61	=	77	M	93	]	109	m	125	}	
1110	E	14	♫	^N	SO		移出	30	▲	^^	RS		记录分隔符	46	.	62	>	78	N	94	^	110	n	126	~	
1111	F	15	☼	^O	SI		移入	31	▼	^-	US		单元分隔符	47	/	63	?	79	O	95	_	111	o	127	⌂	ESC键代码：DEL

CSDN @sheepbookmy

a:97 f:102 Z:90 _:95

f:102 l:108 a:97 g:103

分别相差：5 6 7 8

afZ_r9VYfScOeO_UL^RWUc

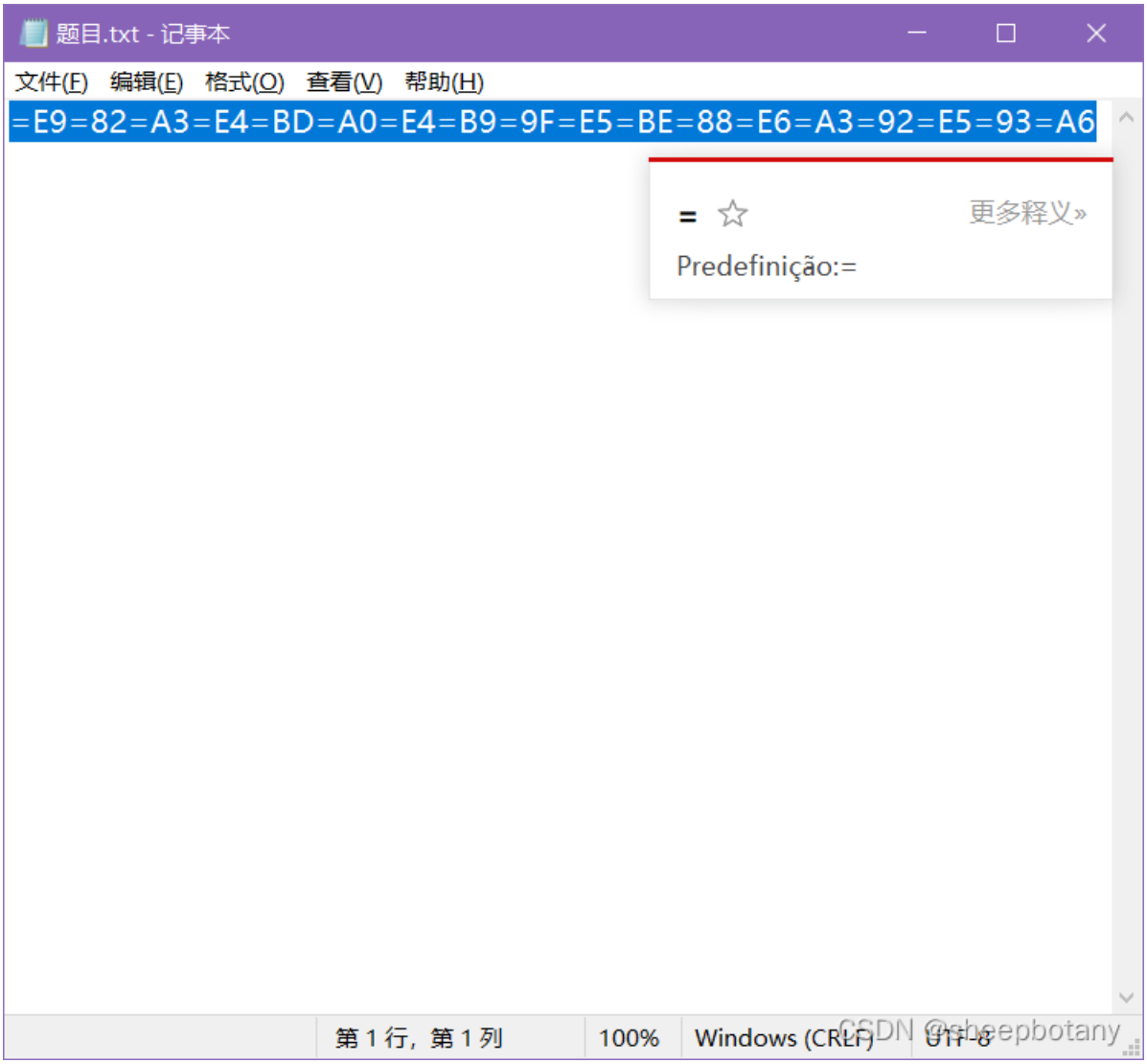
写出脚本

```
ciphertext = 'afZ_r9VYfScOeO_UL^RWUc'
j = 5
for i in ciphertext:
    print(chr(ord(i) + j), end='')
    j += 1
```

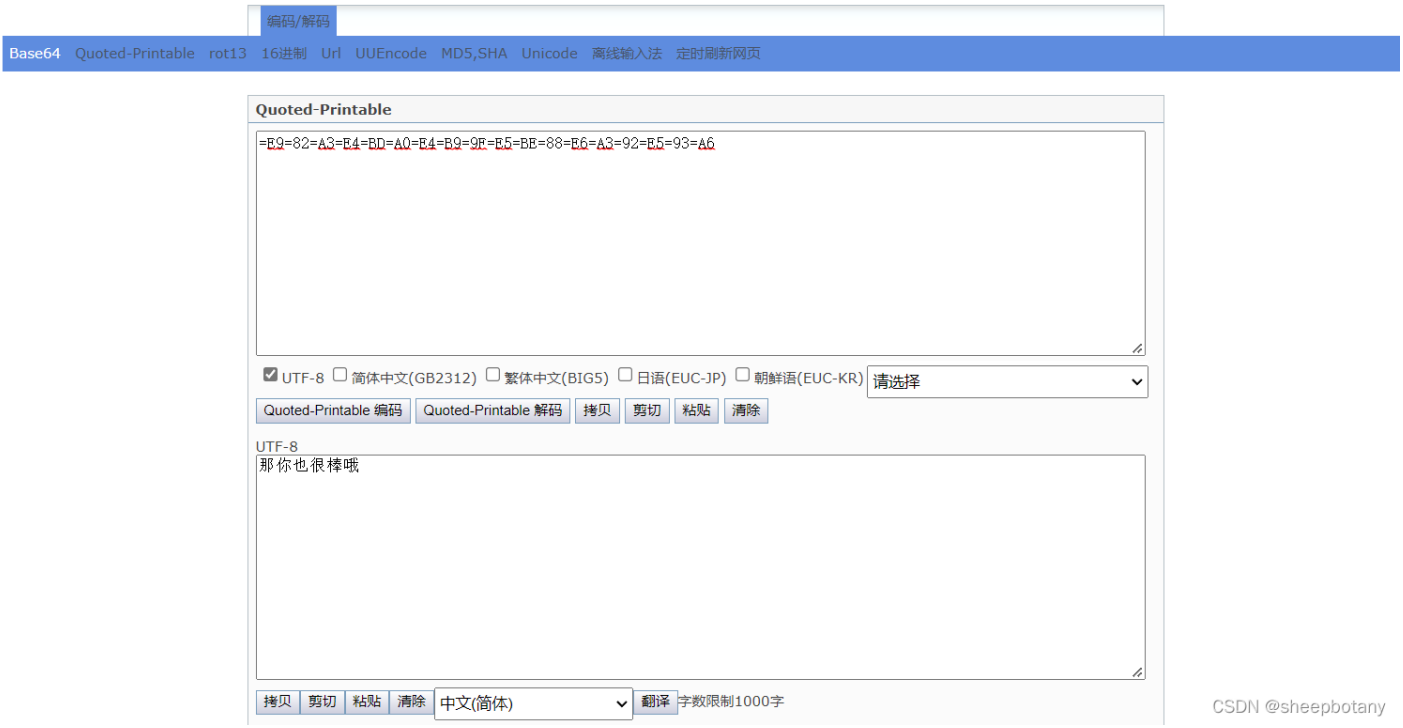
最后求出flag：flag{Caesar_variation}

五： Quoted-printable =E9=82=A3

打开看到是这个样子



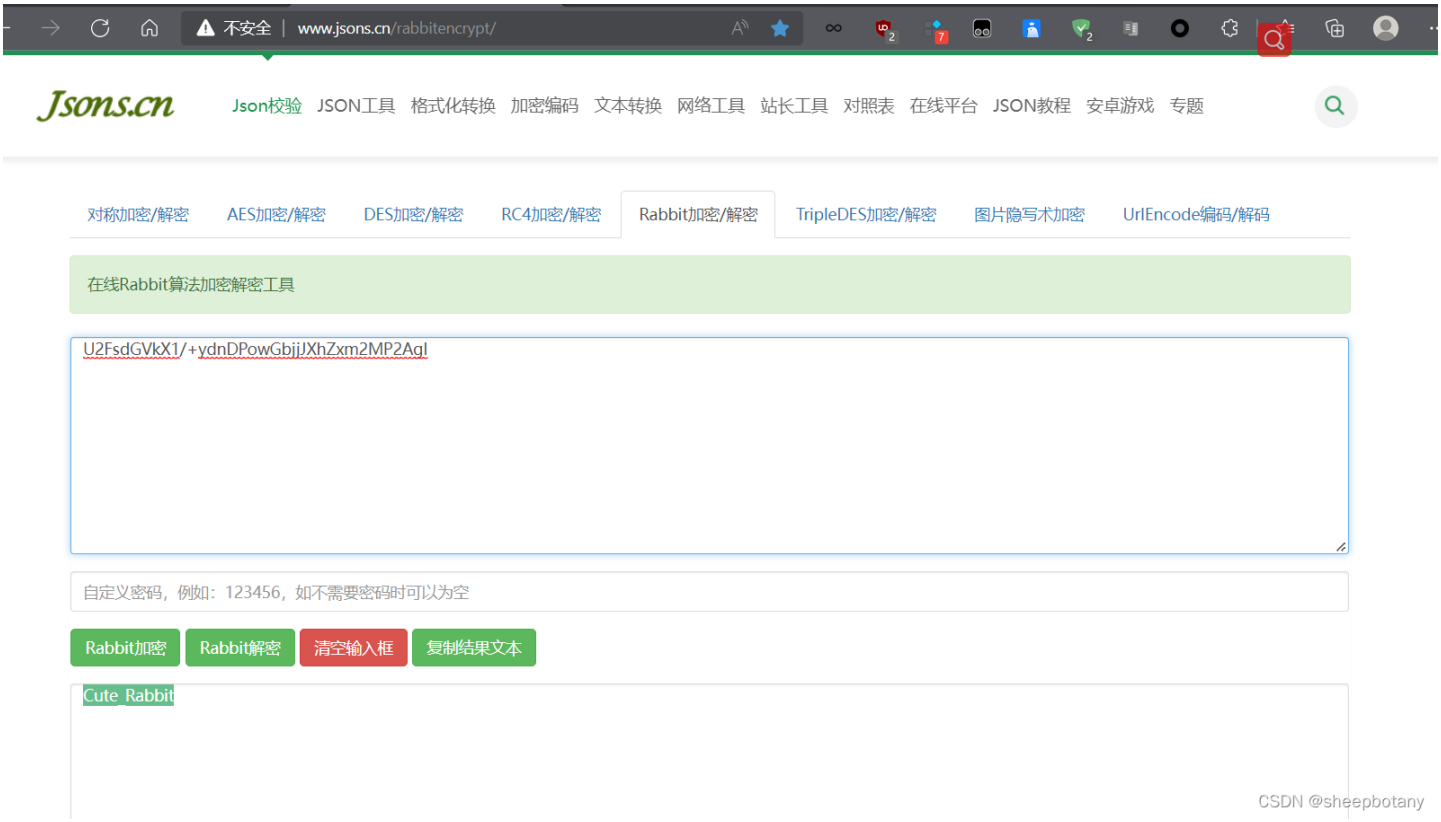
网络管理员在线工具 - Quoted-Printable (mxcz.net)



CSDN @sheepbotany

六 Rabbit加密 U2FsdGVkX1/

Rabbit加密-Rabbit解密-在线Rabbit加密解密工具 (jsons.cn)



CSDN @sheepbotany

七：篱笆墙的影子：栅栏加密

felhaagv{ewtehtehfilnakgw}

栅栏密码在线加密解密 - 千千秀字 (qqxiuzi.cn)

每组数字为2加密后：

flag{wethinkwehavetheflag}

暴力破解

栅栏密码(Rail-fence Cipher)就是把要加密的明文分成N个一组，然后把每组的第1个字符组合，每组第2个字符组合…每组的第N(最后一个分组可能不足N个)个字符组合，最后把他们全部连接起来就是密文，这里以2栏栅栏加密为例。

felhaagv{ewtehtehfilnakgw}

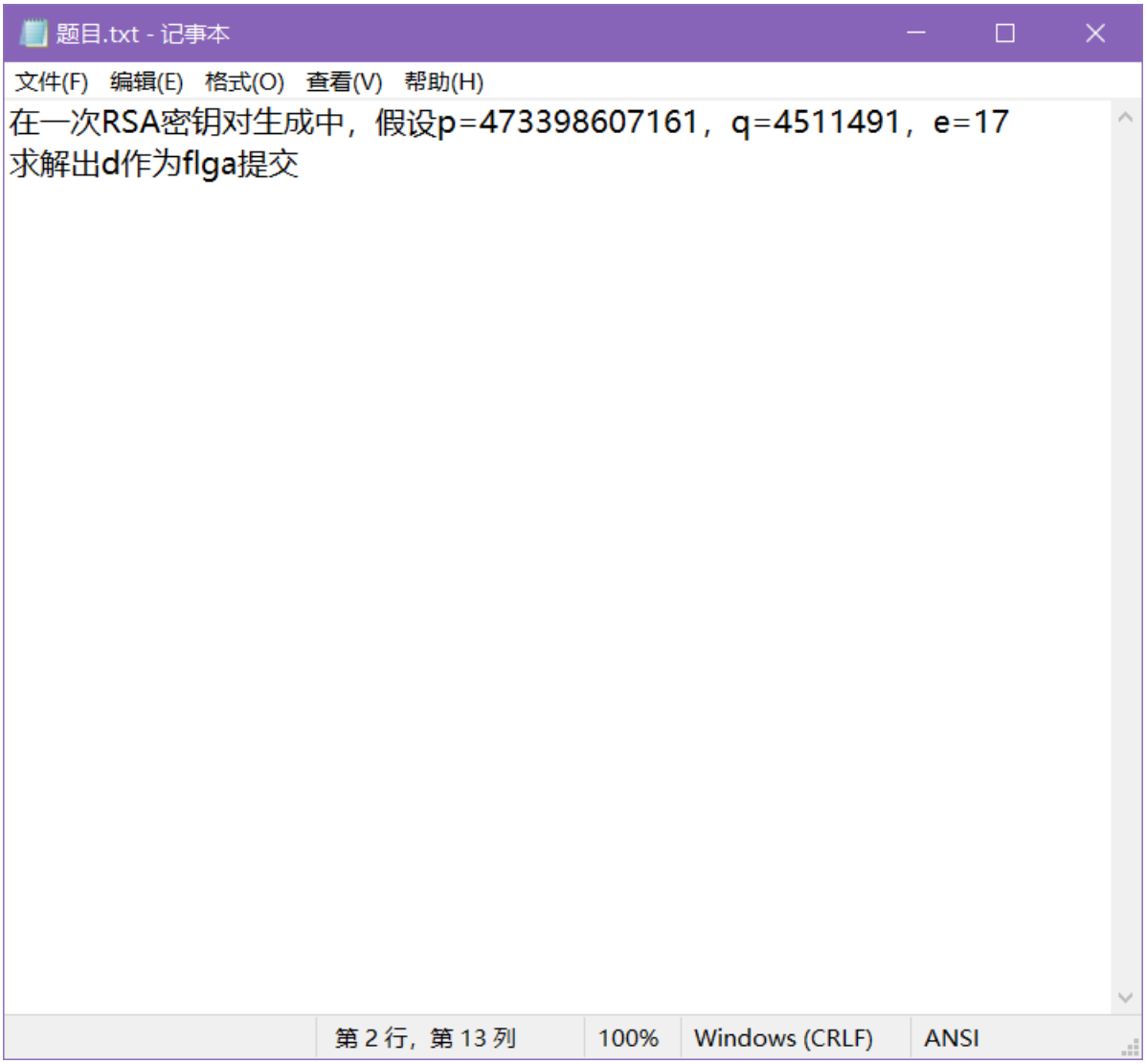
flag，f与l之间有一个字母，所以栅栏数目为2,我们直接分离后变成

flag{wethinkw

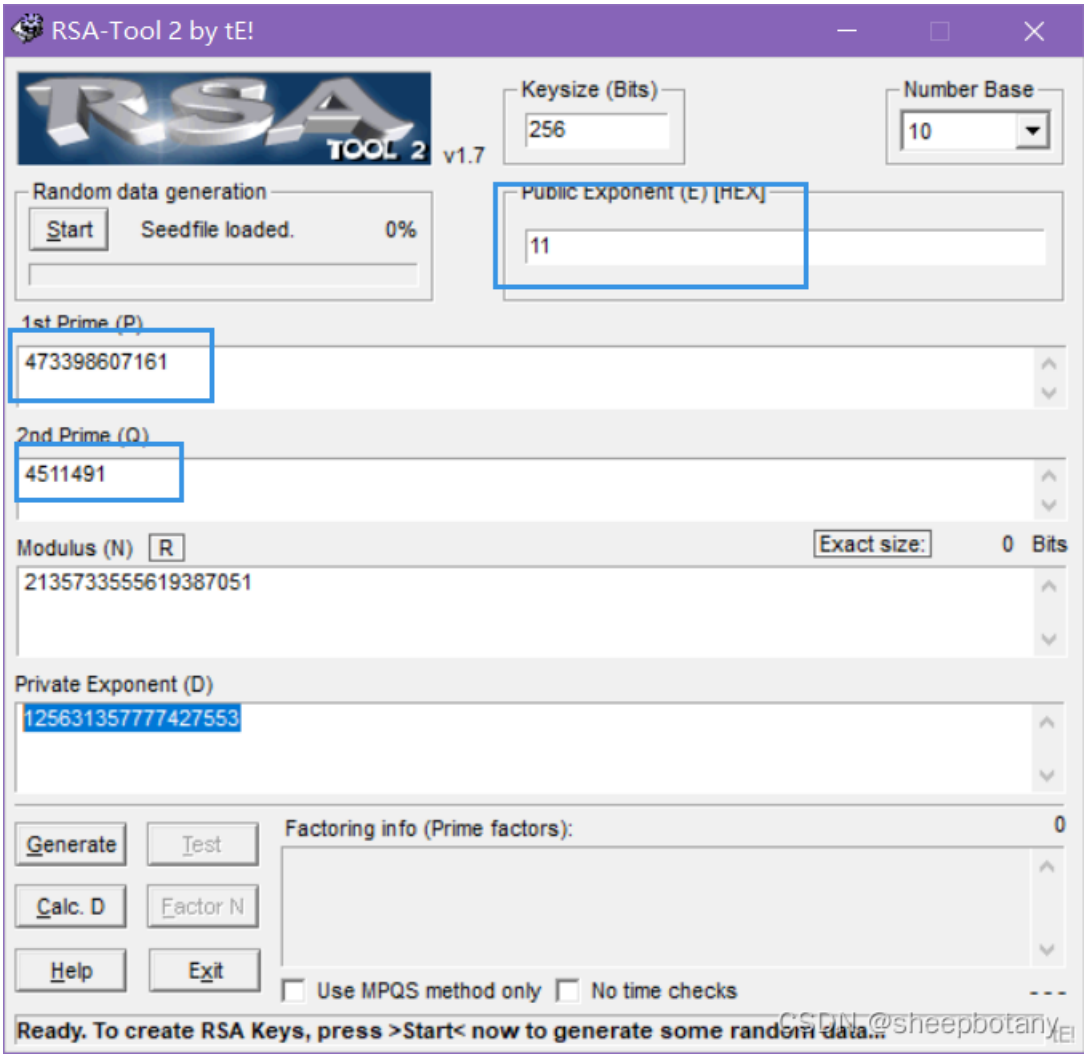
ehavetheflag}

八：RSA

此题主要了解RSA如何使用



打开RSAtools，输入的e要转换为16进制，输入R和Q并按CAL.D即可得到D



flag{125631357777427553}

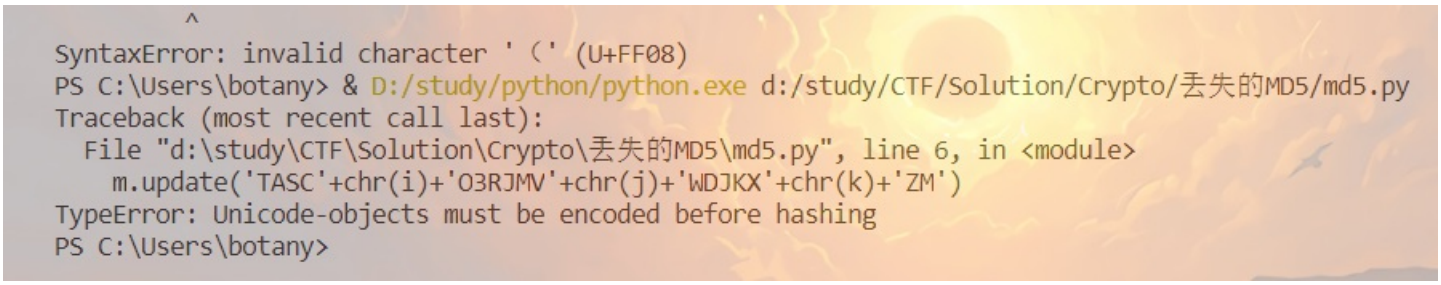
九：丢失的MD5 unicode

打开来发现是python代码

我们把语法修正一下

```
import hashlib
for i in range(32,127):
    for j in range(32,127):
        for k in range(32,127):
            m=hashlib.md5()
            m.update('TASC'+chr(i)+'O3RJMV'+chr(j)+'WDJKX'+chr(k)+'ZM')
            des=m.hexdigest()
            if 'e9032' in des and 'da' in des and '911513' in des:
                print(des)
```

运行后发现报错



```
            ^
SyntaxError: invalid character '（' (U+FF08)
PS C:\Users\botany> & D:/study/python/python.exe d:/study/CTF/Solution/Crypto/丢失的MD5/md5.py
Traceback (most recent call last):
  File "d:\study\CTF\Solution\Crypto\丢失的MD5\md5.py", line 6, in <module>
    m.update('TASC'+chr(i)+'O3RJMV'+chr(j)+'WDJKX'+chr(k)+'ZM')
TypeError: Unicode-objects must be encoded before hashing
PS C:\Users\botany>
```

就是在使用hashing之前需要对unicode进行编码

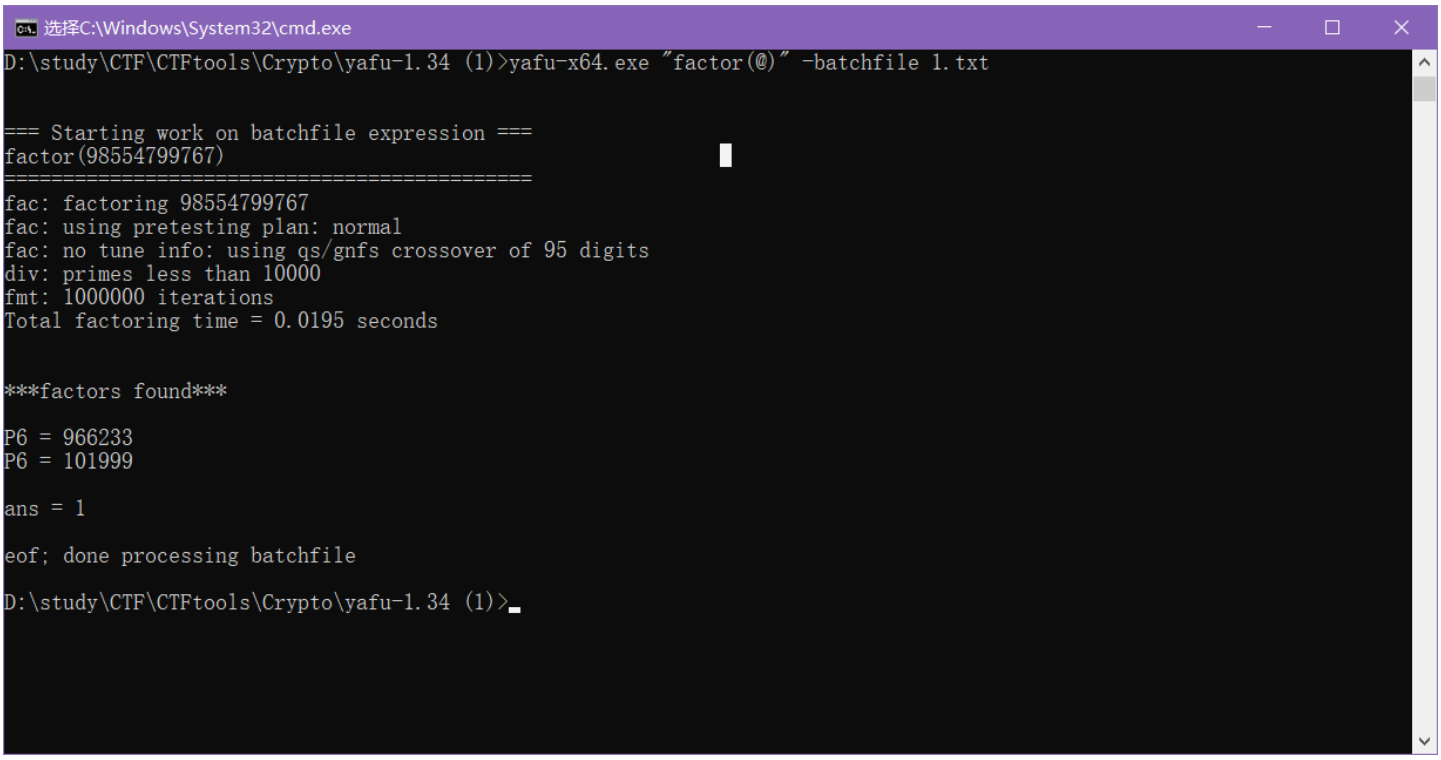
将字符转化为utf-8即可

```
import hashlib
for i in range(32,127):
    for j in range(32,127):
        for k in range(32,127):
            m=hashlib.md5()
            m.update('TASC'.encode('utf-8')+chr(i).encode('utf-8')+'O3RJMV'.encode('utf-8')+chr(j).encode('utf-8
')+'WDJKX'.encode('utf-8')+chr(k).encode('utf-8')+'ZM'.encode('utf-8'))
            des=m.hexdigest()
            if 'e9032' in des and 'da' in des and '911513' in des:
                print(des)
```

十：Alice与Bob素数分解 使用yafu工具，md5

题目描述

使用指令

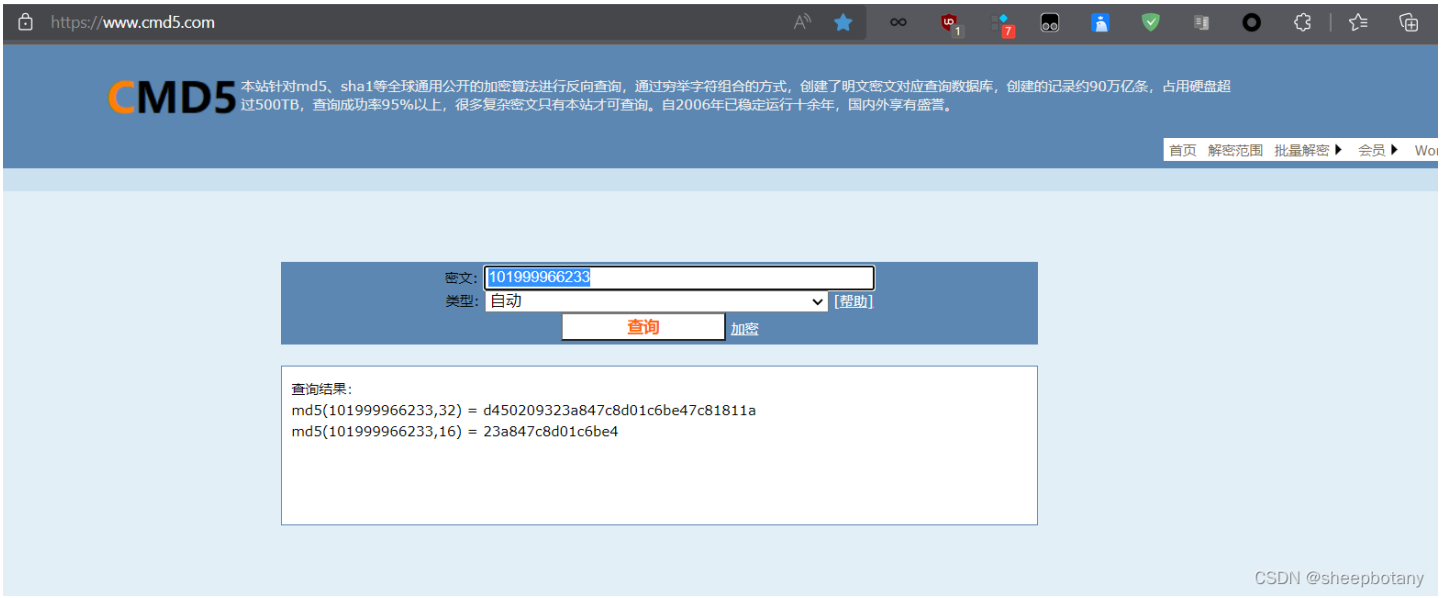


下一步：md5的32位小写hash，意思是进行md5加密且选择32位的那一个

网站

md5在线解密破解,md5解密加密 (cmd5.com)

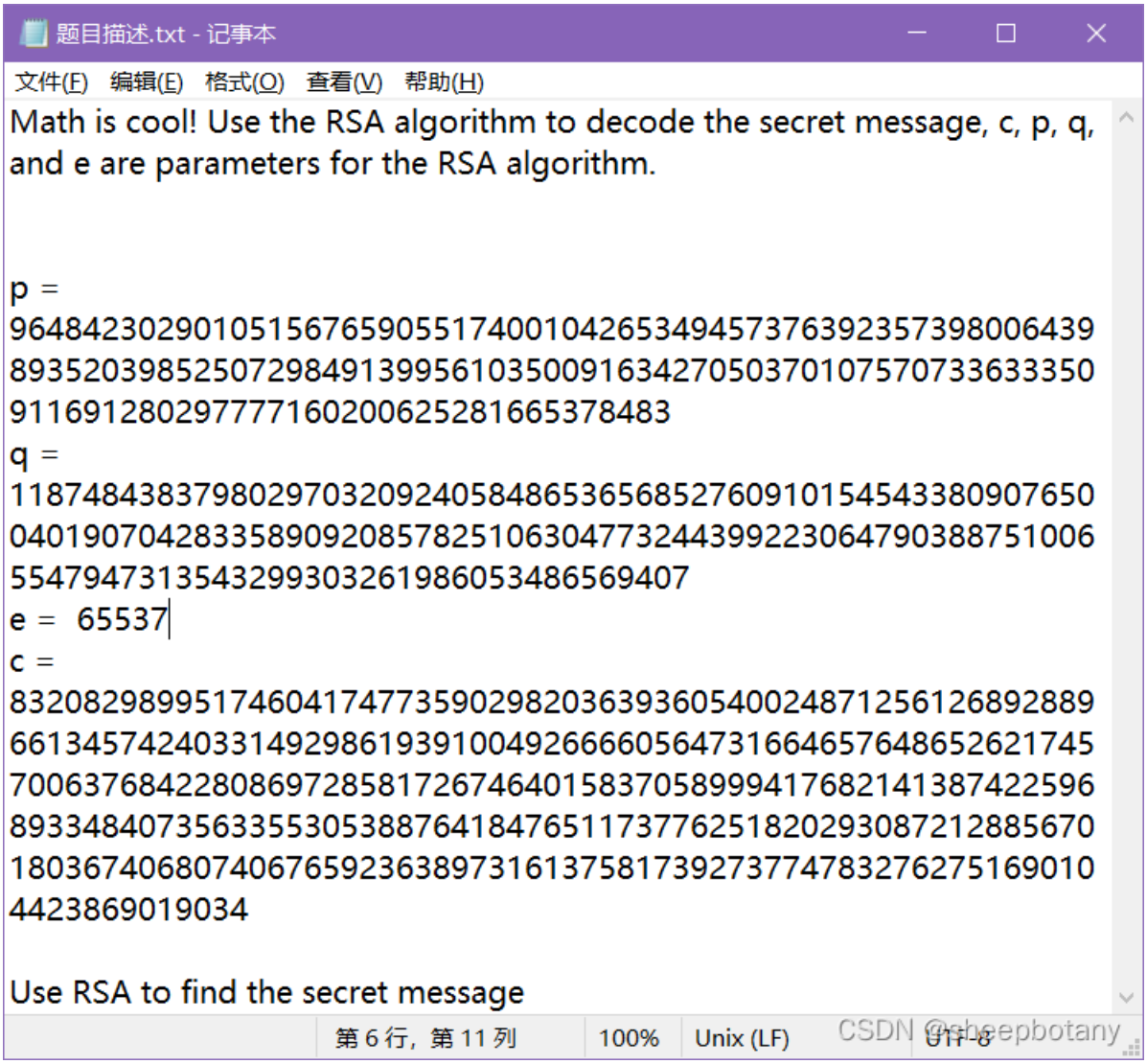
101999 966233



直接输入即可，不需要选择类型

十一：rsarsa

题目描述：



一般情况下都是选择十进制，rsa工具要求出D

得到D，一定要黏贴完成

56632047571190660567520341028861194862411428416862507034762587229995138605649836960220619903456392752115943299335385163216233744624623848874235303309636393446736347238627793022725260986466957974753004129210680401432377444984195145009801967391196615524488853620232925992387563270746297909112117451398527453977

给出了C，说明需要用到python的快速求幂取模运算

```
p=964842302901051567659055174001042653494573763923573980064398935203985250729849139956103500916342705037010757073363335091169128029777716020062528166537848 3
q=11874843837980297032092405848653656852760910154543380907650040190704283358909208578251063047732443992230647903887510065547947313543299303261986053486569407
n=p*q
C=83208298995174604174773590298203639360540024871256126892889661345742403314929861939100492666605647316646576486526217457006376842280869728581726746401583705899941768214138742259689334840735633553053887641847651173776251820293087212885670180367406807406765923638973161375817392737747832762751690104423869019034
d=56632047571190660567520341028861194862411428416862507034762587229995138605649836960220619903456392752115943299335385163216233744624623848874235303309636393446736347238627793022725260986466957974753004129210680401432377444984195145009801967391196615 5
M=pow(C,d,n)
print(M)
```

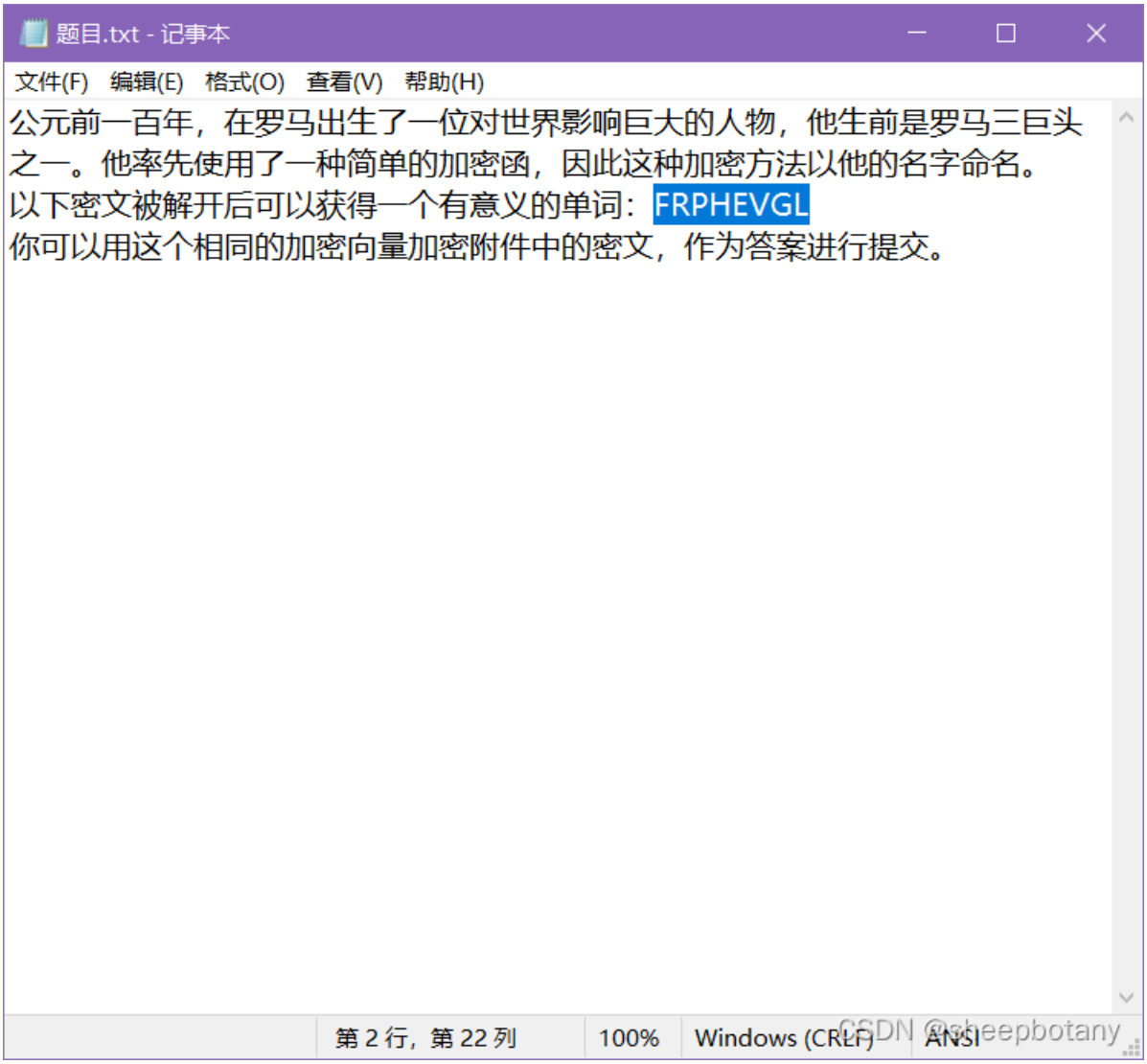
最后得到

557744663355446657776887998 8

十二：凯撒大帝

看题目意思是用凯撒解密将FRPHEVGL解密后会得到一个我们熟悉的单词，然后同解密的方式加密ComeChina可以得到flag

然后脑袋想想估计不会是很复杂的偏移，直接拖到网站好了



一个个解密在偏移量到13的时候出现单词SECURITY，觉得就是他了，然后把comeChina进行加密得到flag

十三：windows系统密码 md5加密 :::

Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

密码是：与:::之间，windows密码一般是md5加密

[外链图片转存失败,源站可能有防盗链机制,建议将图片保存下来直接上传(img-fmQYgJa6-1649124329248)(https://raw.githubusercontent.com/lllwky/botany/main/img/image-20220331235441007.png)]

每个密码都试一下得到flag

十四：信息化时代下的步伐 数字转中文

题目 解题快手榜

信息化时代的步伐

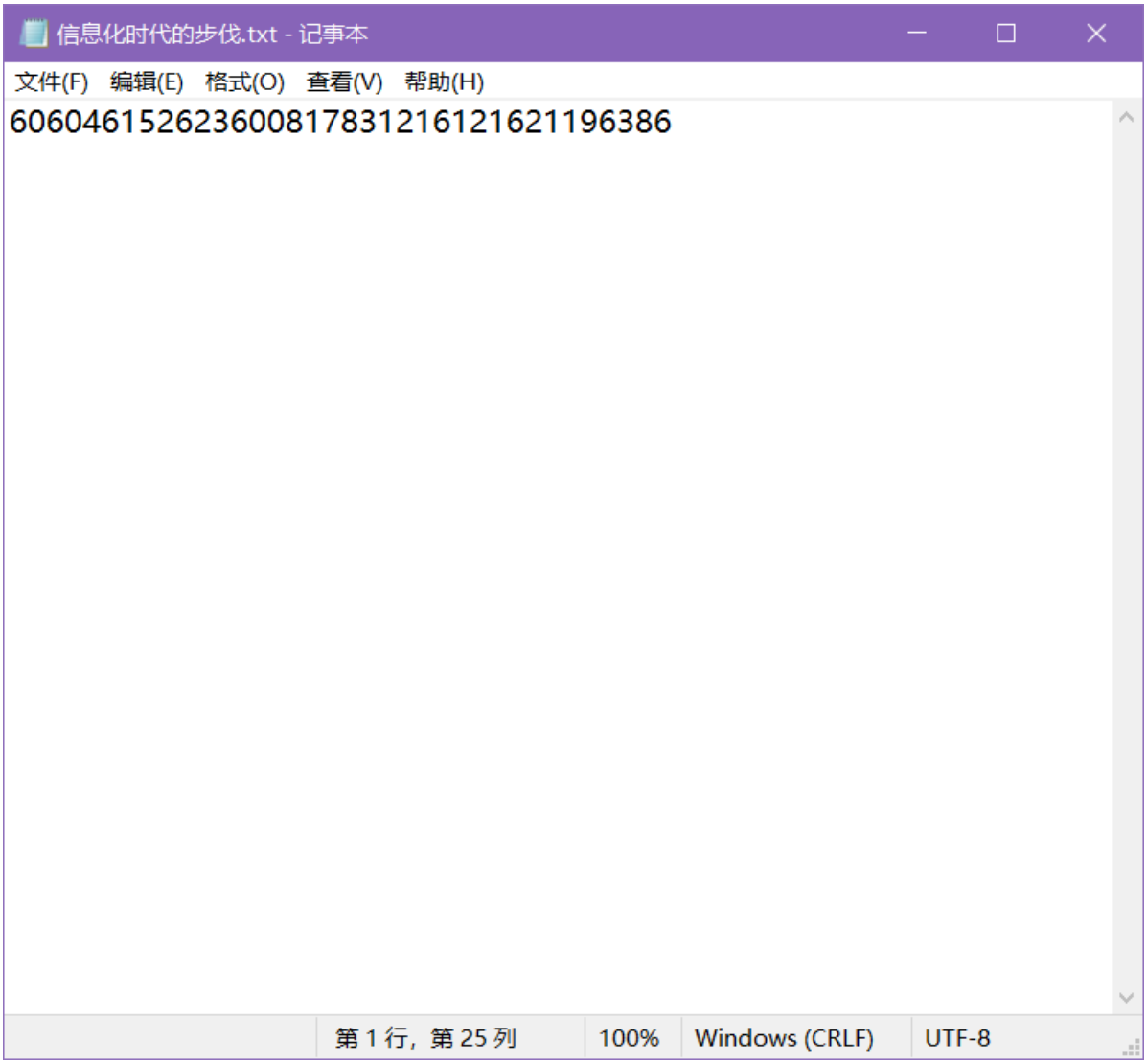
1

也许中国可以早早进入信息化时代，但是被清政府拒绝了。附件中是数十年后一位伟人说的话的密文。请翻译出明文(答案为一串中文！)注意：得到的 flag 请包上 flag{} 提交

a9bbf4f5-ef...

Flag

提交



数字转中文使用中文电码工具

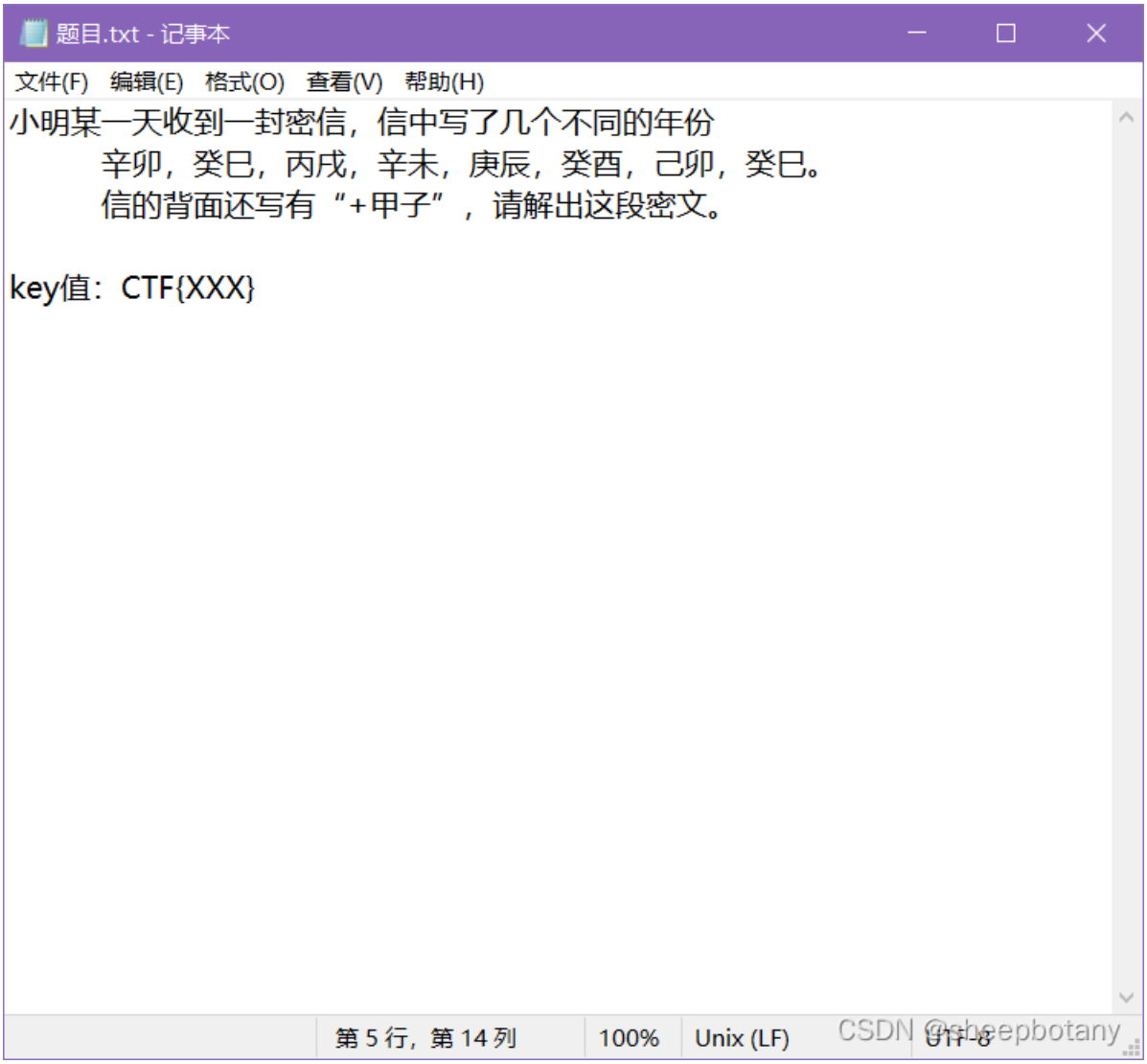
中文电码查询 Chinese Commercial Code - 标准电报码免费在线查询|姓名电码|美国签证电码 (mcdvisa.com)

CSDN @sheepbotany

十五：传统知识＋古典密码 栅栏密码与凯撒密码 辛卯，癸巳，丙戌，辛未，庚辰，癸

酉，己卯，癸巳。

题目描述


题目.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
小明某一天收到一封密信，信中写了几个不同的年份
辛卯，癸巳，丙戌，辛未，庚辰，癸酉，己卯，癸巳。
信的背面还写有“+甲子”，请解出这段密文。
key值：CTF{XXX}
第 5 行，第 14 列
100%
Unix (LF)
UTF-8
CSDN @sheepbotany

01 甲子	11甲戌	21甲申	31 甲午	41甲辰	51甲寅
02 乙丑	12 乙亥	22乙酉	32 乙未	42乙巳	52 乙卯
03 丙寅	13丙子	23 丙戌	33丙申	43丙午	53丙辰
04丁卯	14丁丑	24丁亥	34丁酉	44丁未	54丁巳
05戊辰	15戊寅	25戊子	35戊戌	45戊申	55 戊午
06己巳	16己卯	26己丑	36 己亥	46 己酉	56 己未
07庚午	17 庚辰	27庚寅	37 庚子	47 庚戌	57 庚申
08辛未	18 辛巳	28 辛卯	38 辛丑	48 辛亥	58 辛酉
09壬申	19壬午	29 壬辰	39 壬寅	49 壬子	59 壬戌
10癸酉	20癸未	30 癸巳	40 癸卯	50 癸丑	60 癸亥

CSDN @sheepbotany

2830230817101630+60即每个数字都加60

88 90 83 68 77 70 76 90

两个数字对应一个字母，想到ASCII表

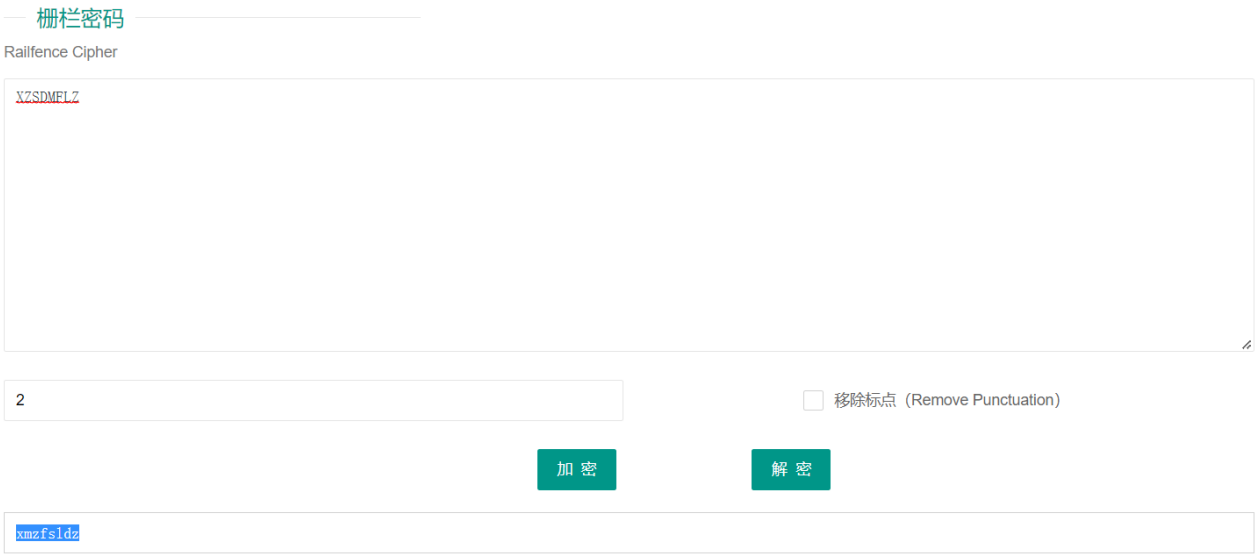
查表可得 X Z S D M F L Z

古典加密一般为栅栏密码与凯撒密码，都丢进去试试

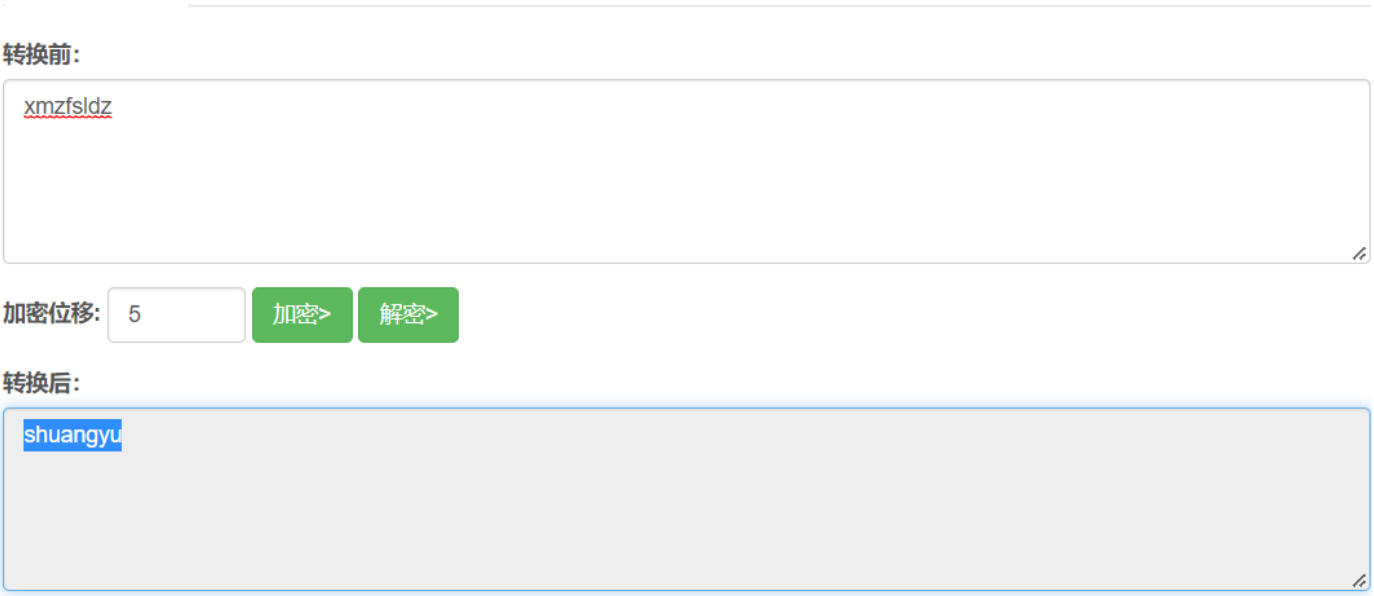
不知道为什么上一个栅栏密码解答和网络上的题解不太一样

CTF在线工具-在线栅栏密码加密|在线栅栏密码解密|栅栏密码算法|Railfence Cipher (hiencode.com)

这个题目天干地支都是以2计数，所以栅栏密码为2



然后再丢到凯撒密码一个个试



flag{SHUANGYU}

记住是大写且要包上flag

十六：凯撒？替换？呵呵 暴力破解网站

这个题目与好野蛮

MTHJ{CUBCGXGUGXWREXIPOYAOEYFIGXWRXCHTKHFCOHCFDUCGTXZOHIXOEOWMEHZO}

来个暴力破解网站喽

quipqiup - cryptoquip and cryptogram solver

选择第一个去掉空格就是flag

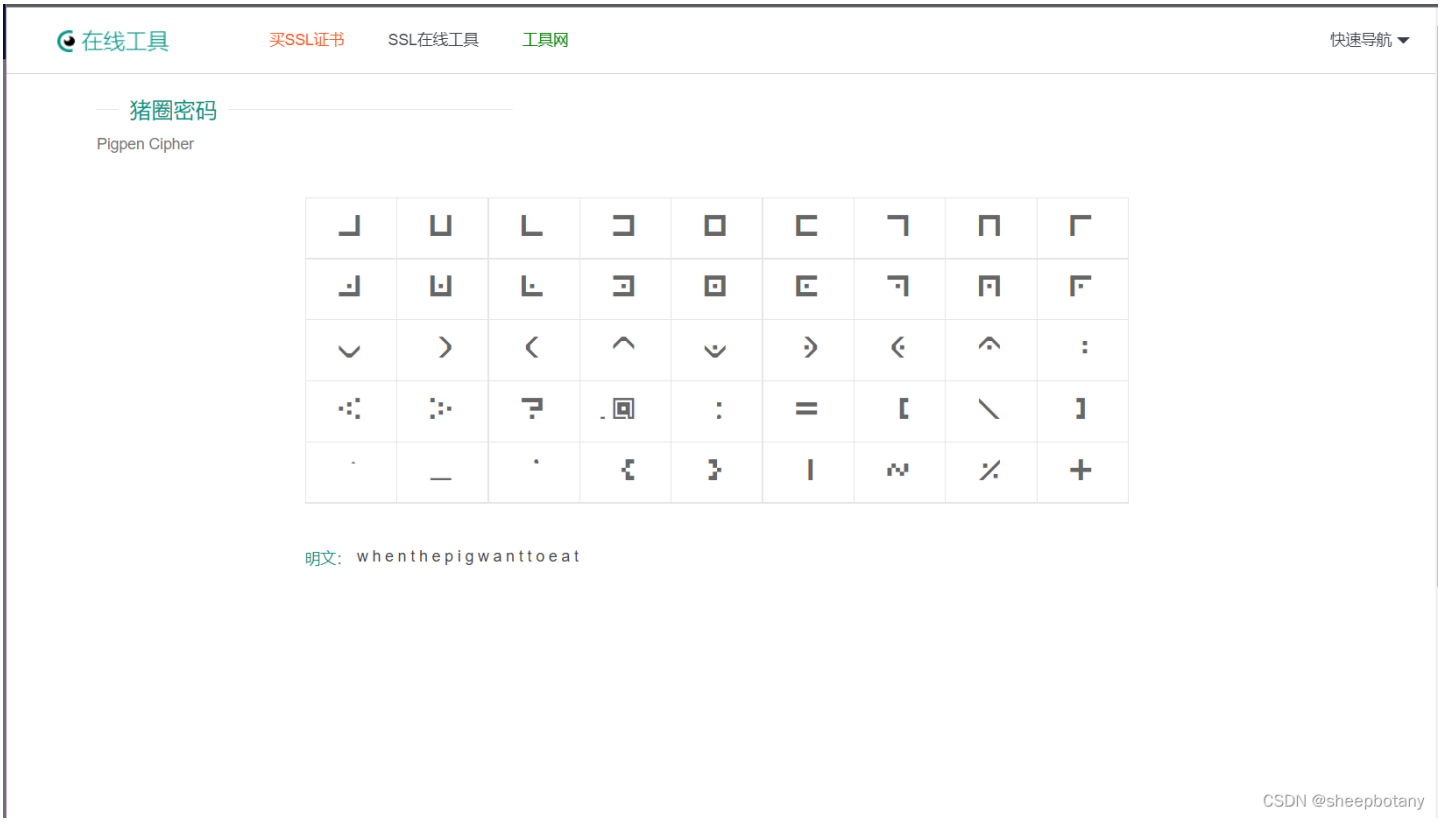
flag{substitutioncipherdecryptionisalwayseasyjustlikeapieceofcake}

十七 猪圈密码

题目描述：

打开发现是一张图片

CTF在线工具-在线猪圈密码加密|在线猪圈密码解密|猪圈密码算法|Pigpen Cipher (hiencode.com)



真是可爱的一道题啊

十八：RSA1

RSA算法原理 - 知乎 (zhihu.com)

之前只是学会了如何使用工具，这题开始认真学会RSA算法

互质关系：如果两个正整数，除了1以外，没有其他公因子，则称他们为互质关系

欧拉函数

任意给定正整数n，在小于等于n的正整数之中，有多少个与n构成互质关系，用 φ(n)表示

若n为质数，φ(n)=n-1。

若n是指数的某一次方即$n=p^{k,则φ(p}k)=p^{k-p}(k-1)$

若n=pq（两个质数）

则φ(n)=φ(pq)=φ§φ(q)

欧拉定理

如果两个正整数a和n互质，则a的φ(n)次方-1可以被n整除。

模反元素

如果a与n互为质数，则一定可以找到整数d使得pd-1能被n整除

记作da=1（mod n）

RSA算法

1：随机选取两个不相等的质数p和q

2：计算p与q的乘积n

3：计算n的欧拉函数φ(n)

4：随机选取整数e，e与φ(n)互质

5：计算出e对于φ(n)的模反元素d

题目如下

[外链图片转存失败,源站可能有防盗链机制,建议将图片保存下来直接上传(img-aZoq0ceo-1649124329261)(https://raw.githubusercontent.com/lllwky/botany/main/img/image-20220401163349449.png)]

```
p = 863763376725700856709965348654109117132049150943361544753916243791124417588566780639841179052408355344515811350222774520620532769093950403299469990205322 9
q = 126406749739964727691760479371708834209270508214800105815931371353724738805956137373376306297525773461470392840300825934907766305725849599542053368802284 69
dp = 650079570221683462110904235119326153065004384105625293093094966335862501688183284072806602615026469307610935487409984138045488171609777830726811691058292 9
dq = 783472263673553449019532580386470672380574033551303889137911760438881683674556098098256795673512201963002175438762767516968043599582527539160811120550041
c = 247223054038873820735673164676490806626315529059602293990791079956021544181760563358006388875276141640735304376570850796761573502053519452229893513160764865735995760419783398722659250627643185360890073102702785261596789374319038628924007479155251189839599706079341429747366757843259934459420313721073421038 52

import gmpy2
d = gmpy2.invert(q,p)
mp = pow(c,dp,p)
mq = pow(c,dq,q)                #求幂取模运算

m = (((mp-mq)*d)%p)*q+mq        #求明文公式

print(hex(m))           #转为十六进制
```

如果c与p互为质数，则一定可以找到整数d使得dp-1能被c整除

记作da=1（mod n）

最后的结果

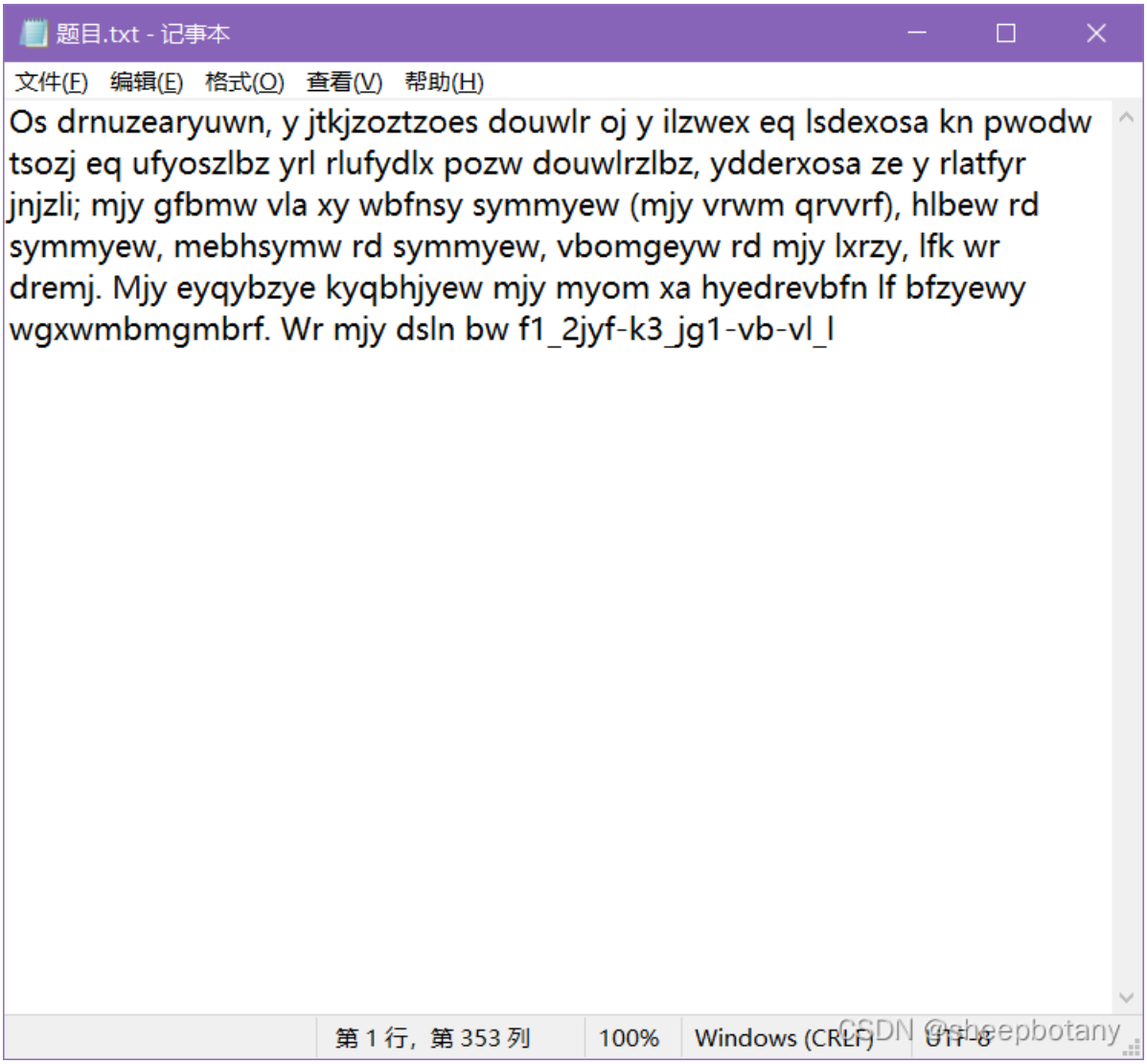
```
PS D:\study\CTF\python> & D:/study/python/python.exe d:/study/CTF/python/test.py
0x6e6f784354467b57333163306d335f37305f4368316e343730776e7d
```

再十六进制转文本

16进制转换，16进制转换文本字符串，在线16进制转换 | 在线工具 (sojson.com)

noxCTF{W31c0m3_70_Ch1n470wn}将noxCTF转换为flag{}

十九：old fashion 爆破工具

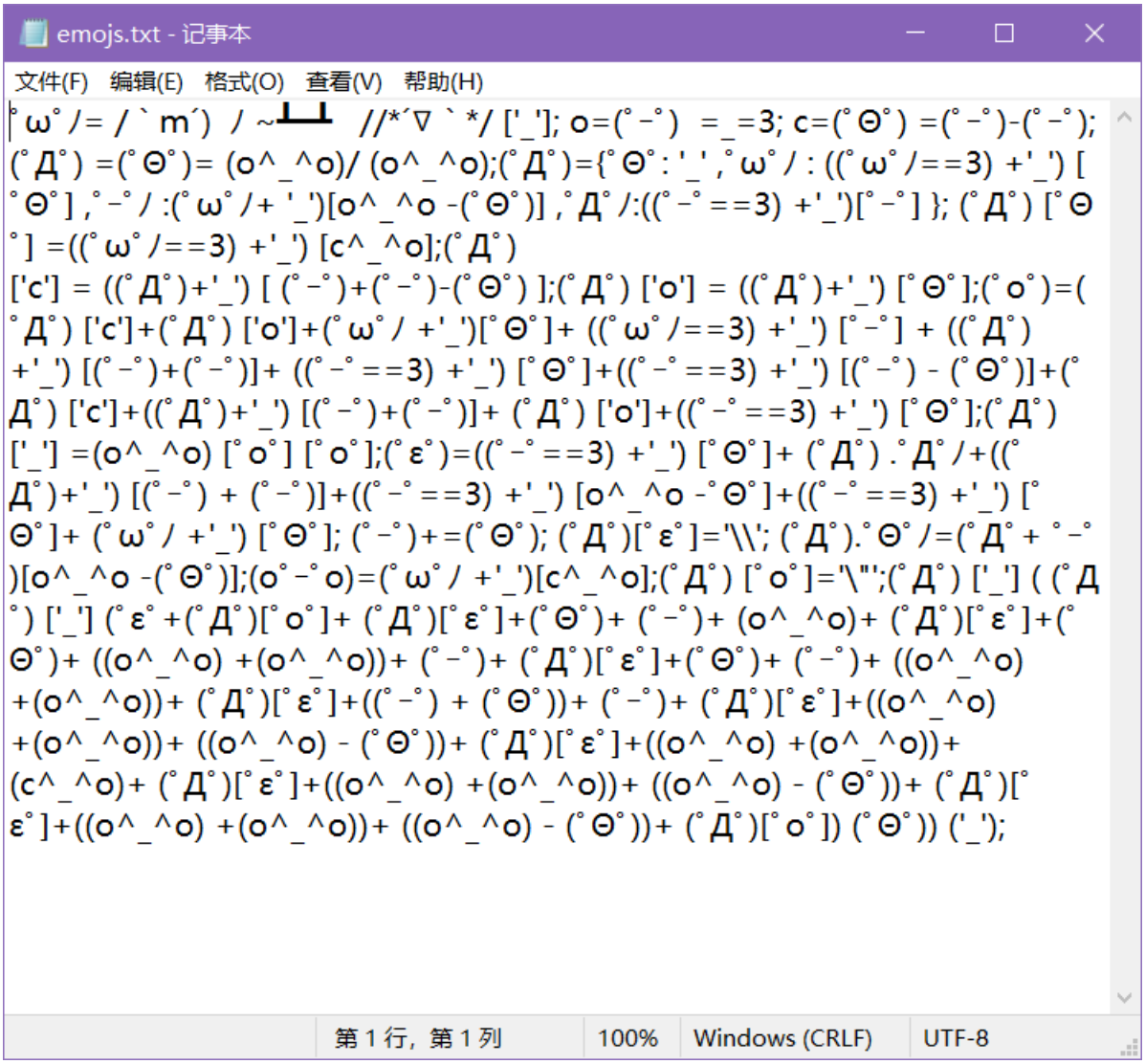


不会的统一用爆破工具吧

quipqiup - cryptoquip and cryptogram solver

二十 js表情包转换

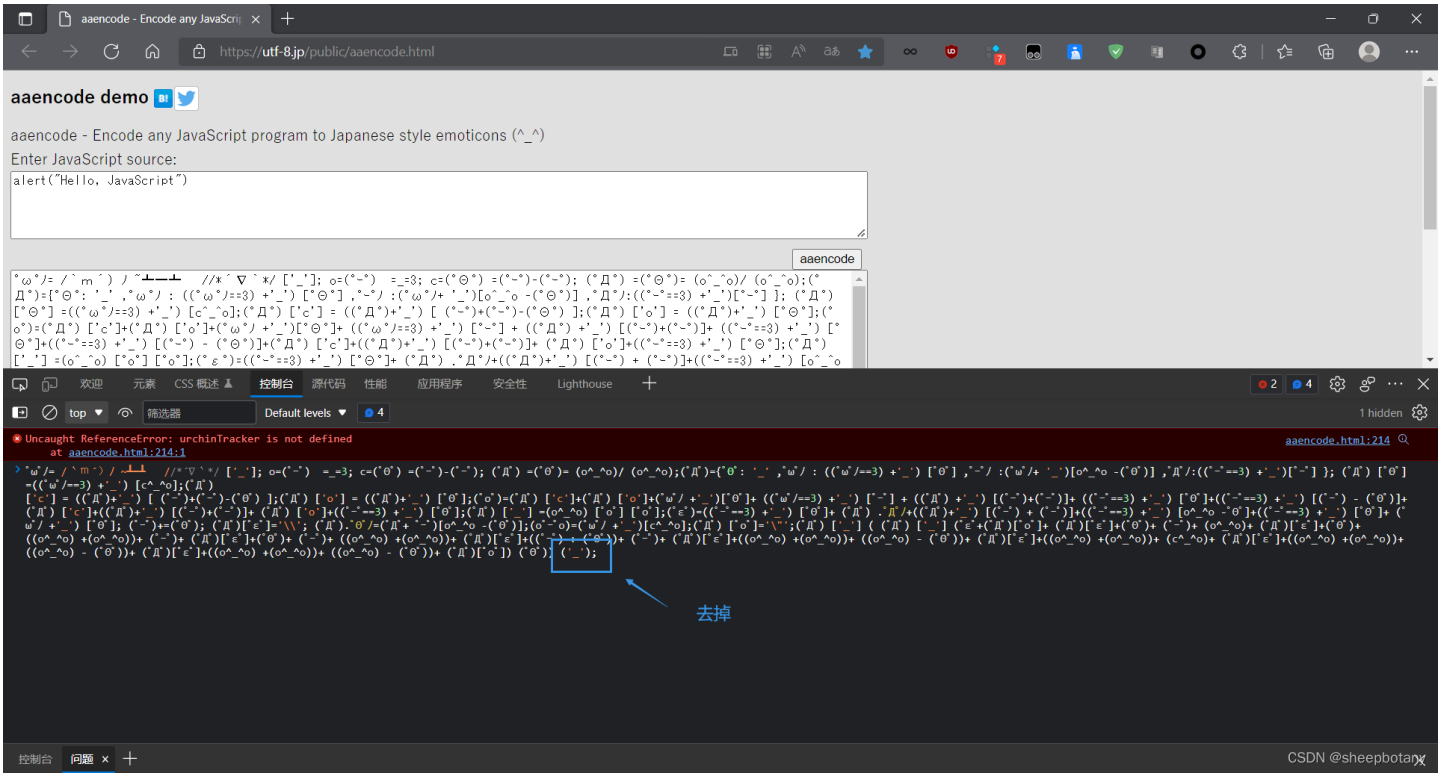
打开文件发现



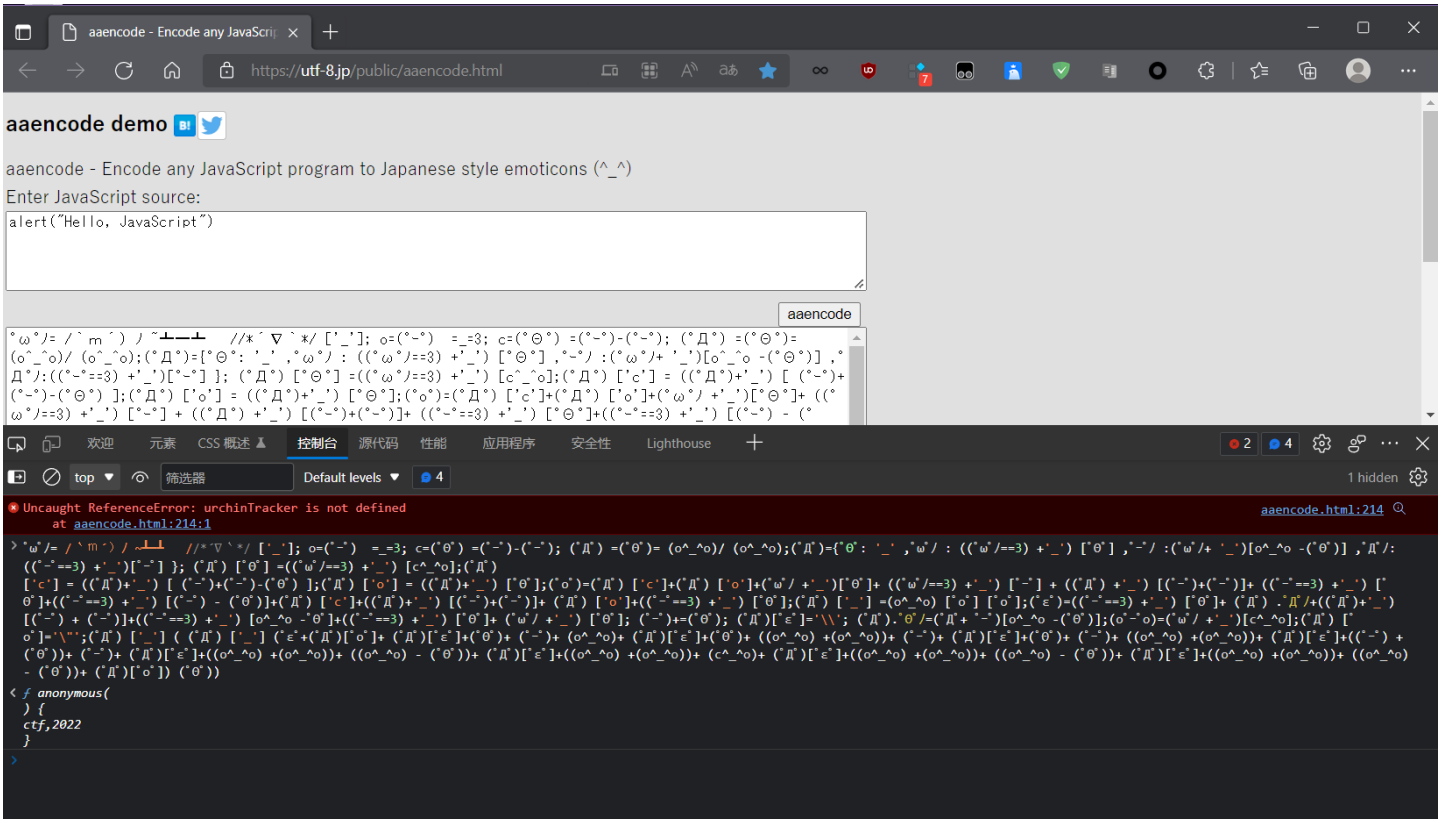
进入转换网站

aaencode - Encode any JavaScript program to Japanese style emoticons (–) (utf-8.jp)

按F12打开控制台



然后输出即可得到flag

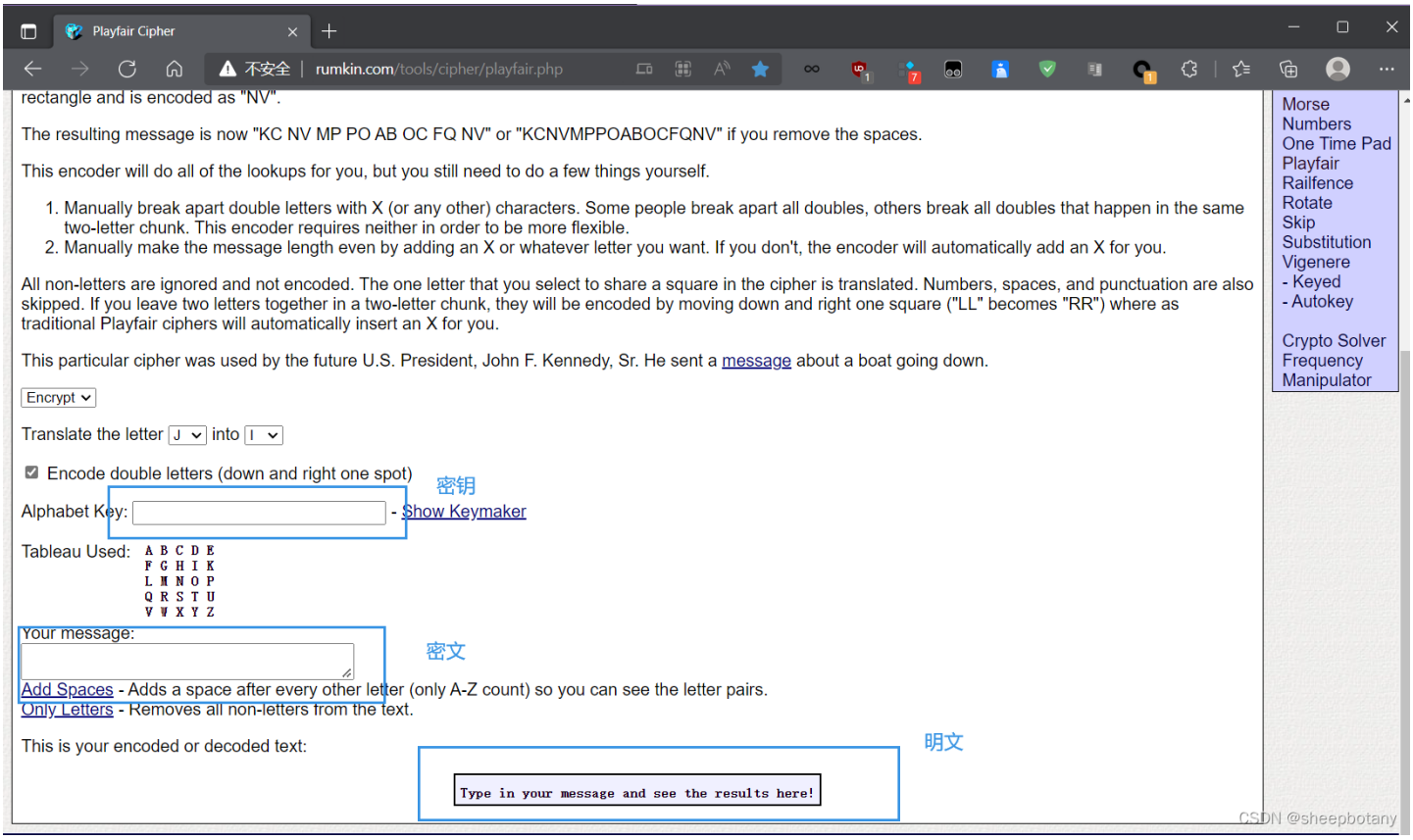


二十一：Cipher

打开破解网站

Playfair Cipher (rumkin.com)

密钥根据题目公平的玩吧，是playfair



flag{itisqstaproblegmavefip}

（要把大写改为小写）

二十二：摩斯密码01版

这题的题目找不到了，那就直接上代码吧

```
s = '0010 0100 01 110 1111011 11 11111 010 000 0 001101 1010 111 100 0 001101 01111 000 001101 00 10 1 0 010 0 0
00 1 01111 10 11110 101011 1111101'
b=s.replace('0', '.')
print(b.replace('1','-'))
```

然后再用网站进行破解

二十三 HEX密码 666c61677b57336c63306d655f54305f4354467d

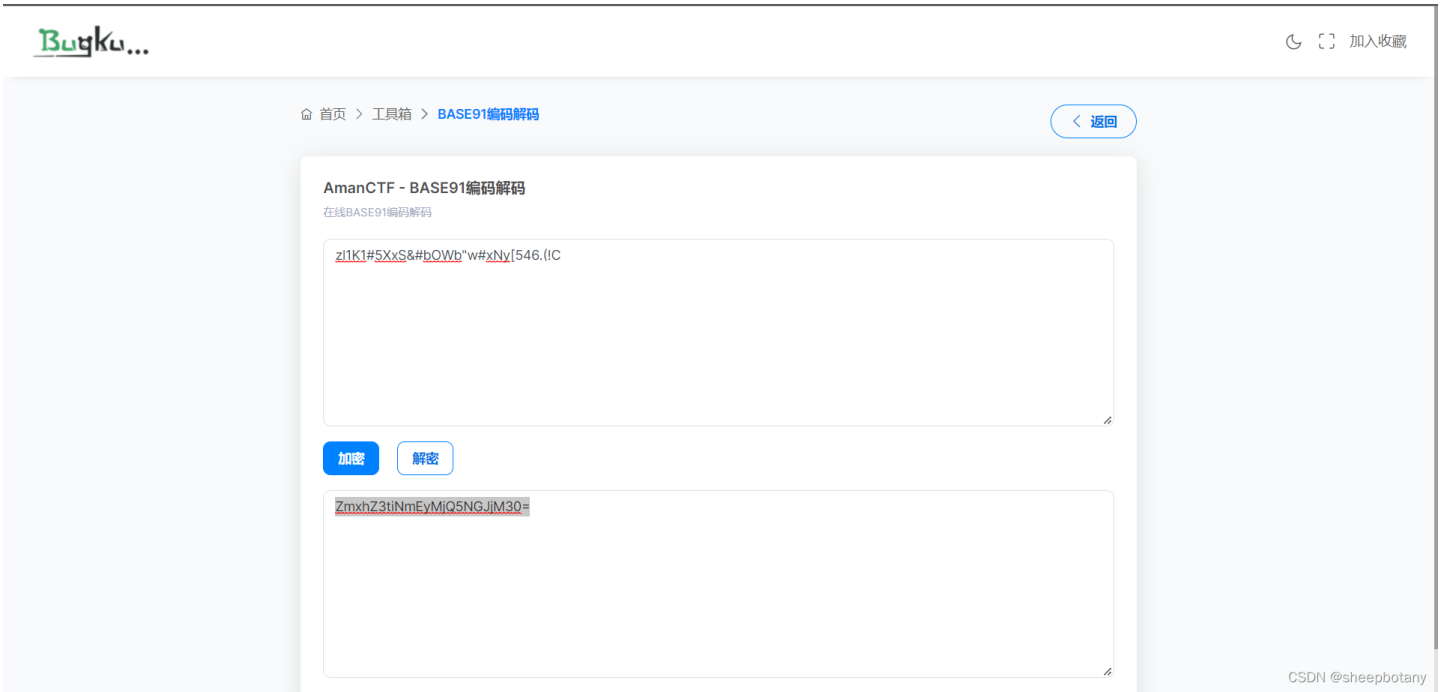
与base64很像但是没有=所以为hex

Hex编码/解码-在线工具 (toolbaba.cn)

二十四 base family

最后发现是base91

BASE91编码解码 - Bugku CTF



得到base64再进入base64进行解密

解密工具集合

在线工具 - Bugku CTF

int(b.replace('1','-'))

然后再用网站进行破解

二十三 HEX密码 666c61677b57336c63306d655f54305f4354467d

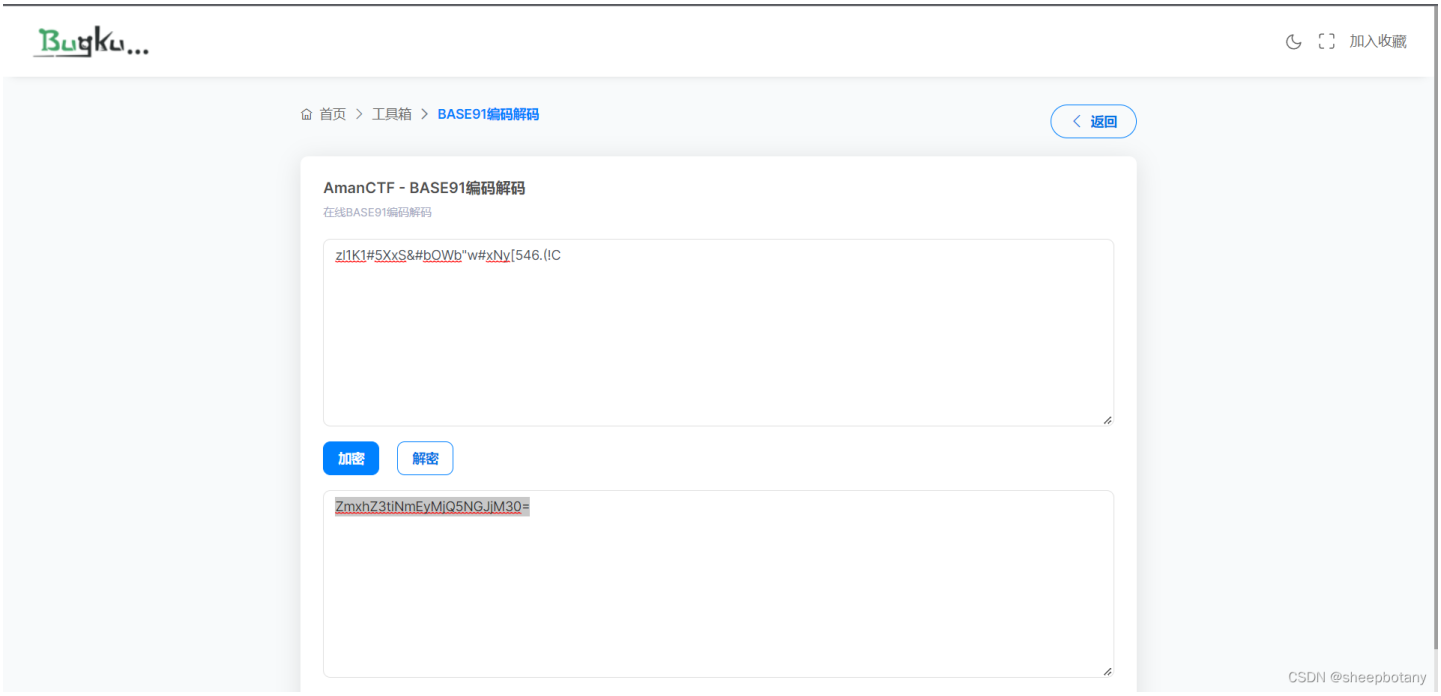
与base64很像但是没有=所以为hex

Hex编码/解码-在线工具 (toolbaba.cn)

二十四 base family

最后发现是base91

BASE91编码解码 - Bugku CTF



得到base64再进入base64进行解密

解密工具集合

在线工具 - Bugku CTF