

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/llwky/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

一：一眼就解密 base64 SEITX1NUUkIOR30=

二：看我回旋踢 synt{：凯撒密码

三：password

四：变异凯撒 ASCII

五：Quoted-printable =E9=82=A3

六 Rabbit加密 U2FsdGVkX1/

七：篱笆墙的影子：栅栏加密

八：RSA

九：丢失的MD5 unicode

十：Alice与Bob素数分解 使用yafu工具，md5

十一：rsarsa

十二：凯撒大帝

十三：windows系统密码 md5加密 :::

十四：信息化时代下的步伐 数字转中文

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。

十六：凯撒？替换？呵呵 暴力破解网站

十七 猪圈密码

十八：RSA1

欧拉函数

欧拉定理

模反元素

RSA算法

十九：old fashion 爆破工具

二十 js表情包转换

二十一：Cipher

二十二：摩斯密码01版

二十三 HEX密码 666c61677b57336c63306d655f54305f4354467d

二十四 base family

二十三 HEX密码 666c61677b57336c63306d655f54305f4354467d

二十四 base family

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 SEITX1NUUkIOR30=

ZmxhZ3tUSEVfRkxBR19PRI9USEITX1NUUkIOR30=

有等于号是base64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)

开发工具 > 凯撒密码在线计算

凯撒密码加密 维吉尼亚密码计算 栅栏密码加密 猪圈密码加密 仿射密码加密 摩斯密码翻译器

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

加密位移： 13 加密> 解密>

转换后：
flag{5cd1004d-86a5-46d8-b720-beb5ba0417e1}

凯撒密码最早由古罗马军事统帅盖乌斯·尤利乌斯·凯撒在军队中用来传递加密信息，故称凯撒密码。此为一种位移加密手段，只对26个（大小写）字母进行位移加密，规则相当简单，容易被破解。下面是明文字母表移回3位的对比：
明文字母表 X Y Z A B C D E F G H I J K L M N O P Q R S T U V W
密文字母表 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
然后A变成D，B变成E，Z变成C。
字母最多可移动25位（按字母表）。通常为向后移动，如果您想向前移动1位，则相当于向后移动25位，位移选择为25位。

工具简介：
凯撒密码，作为最古老的对称加密系统之一，通过把字母移动一定位数来加密和解密字符串。加密时，明文中的所有字母在字母表上向后（或向前）移动一个固定的数字，然后替换为密文。

热门工具：
CRC校验工具
在线AES加密解密
在线时间戳转换
MD5在线加密
在线加密解密

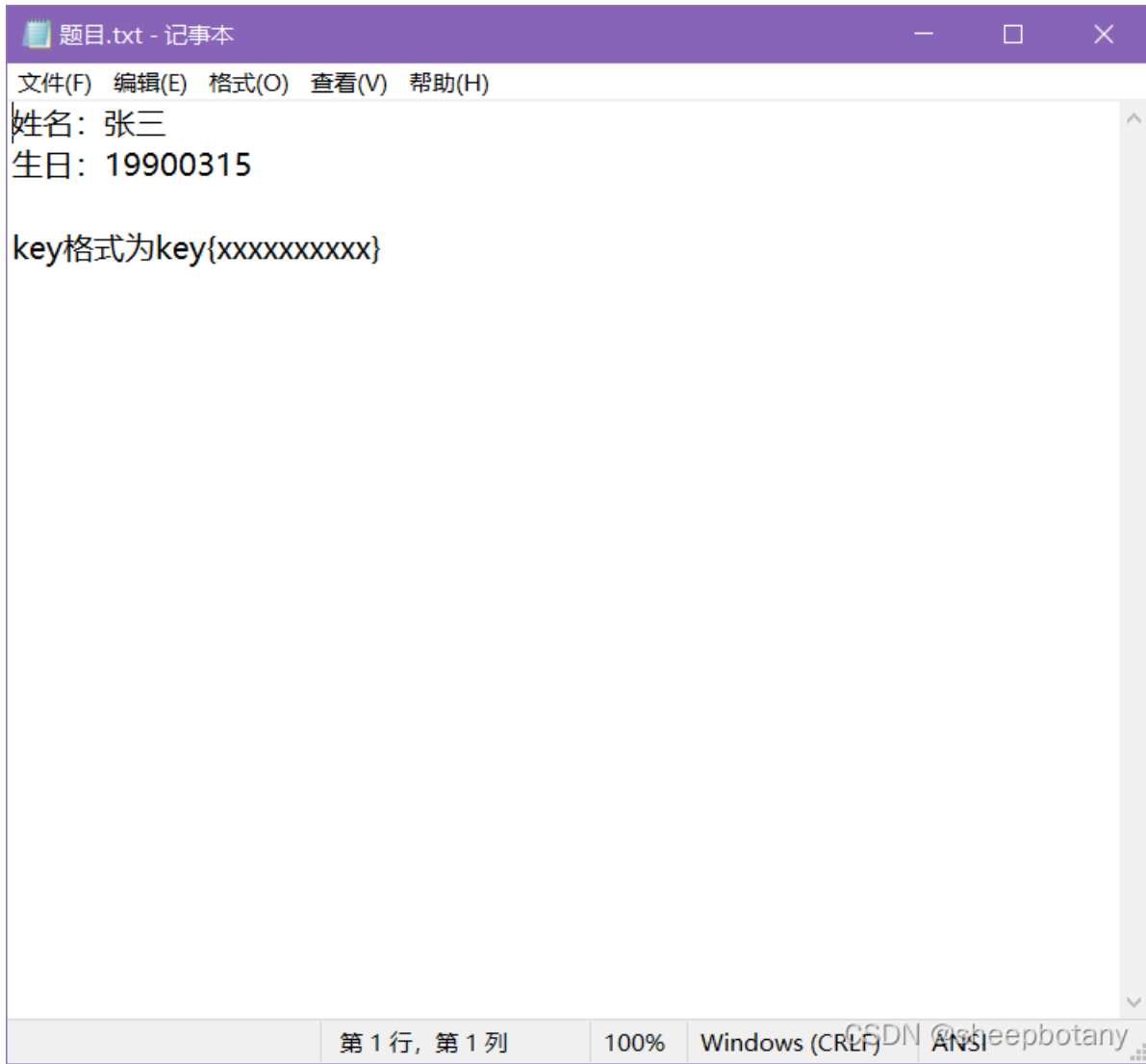
推荐工具：
异或校验/BCC校验计算
SHA1在线加密、校验工具
CRC校验工具
在线AES加密解密
JSON在线解析

CSDN @sheepbotany

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

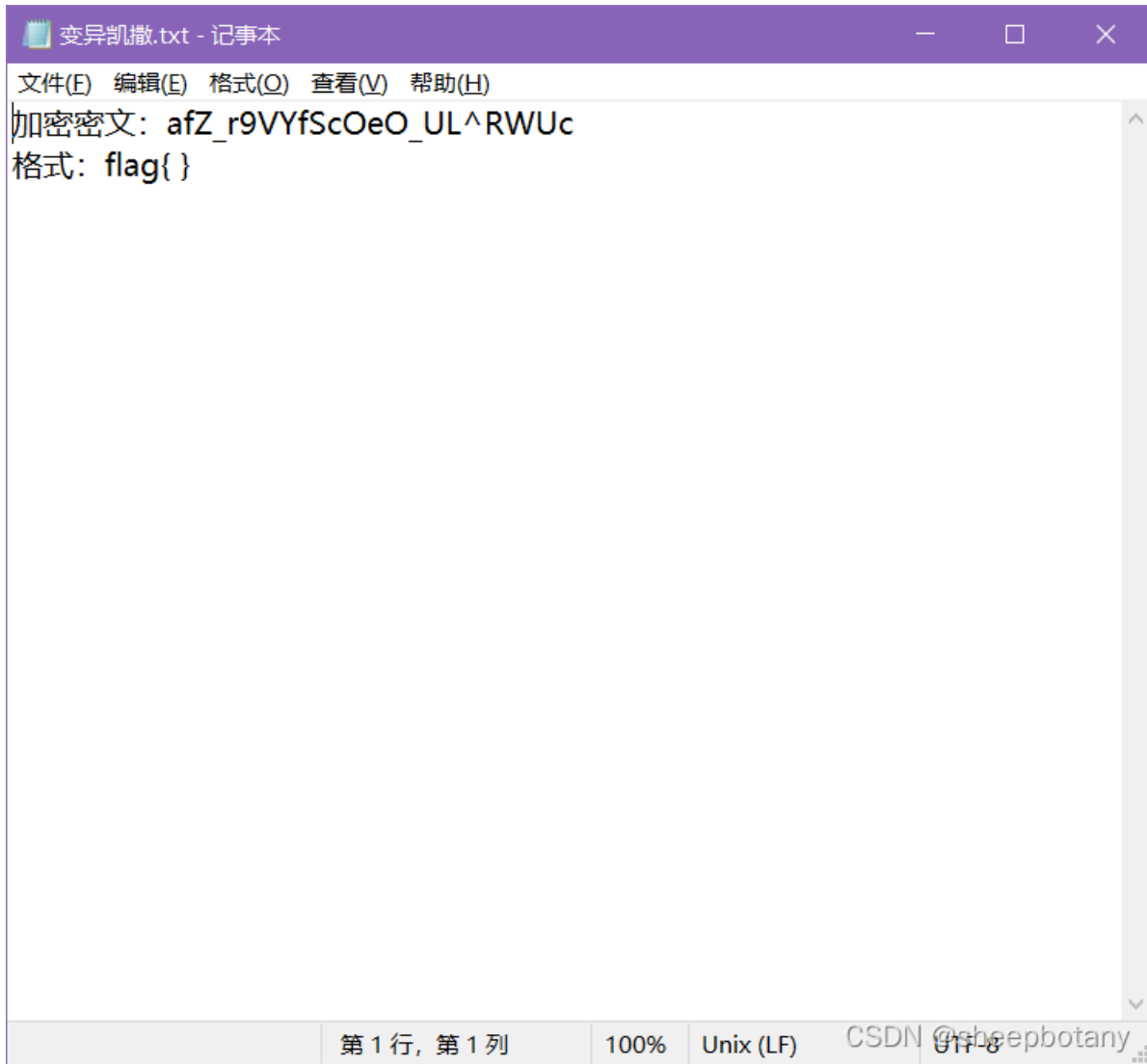
三：password

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



```
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
加密密文: afZ_r9VYfScOeO_UL^RWUc
格式: flag{ }

第 1 行, 第 1 列 100% Unix (LF) CSDN @sheepbotany UTF-8
```

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	ASCII控制字符												ASCII打印字符												
	0000				0001				0010		0011		0100		0101		0100		0111						
	0				1				2		3		4		5		6		7						
低四位	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	☹	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	⊕	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	♥	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	♠	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	♣	ENQ		查询	21	§	^U	NAK		否定应答	37	%	53	5	69	E	85	U	101	e	117	u	
0110	6	6	♠	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	•	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	⏏	BS	\b	退格	24	↑	^X	CAN		取消	40	(56	8	72	H	88	X	104	h	120	x	
1001	9	9	○	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	⏏	LF	\n	换行	26	→	^Z	SUB		替代	42	*	58	:	74	J	90	Z	106	j	122	z	
1011	B	11	♂	VT	\v	纵向制表	27	←	^[ESC	\e	溢出	43	+	59	;	75	K	91	[107	k	123	{	
1100	C	12	♀	FF	\f	换页	28	└	^[_	FS		文件分隔符	44	,	60	<	76	L	92	\	108	l	124		
1101	D	13	♪	CR	\r	回车	29	↔	^_]	GS		组分隔符	45	-	61	=	77	M	93]	109	m	125	}	
1110	E	14	🎵	SO		移出	30	▲	^^	RS		记录分隔符	46	.	62	>	78	N	94	^	110	n	126	~	
1111	B	15	🎵	SI		移入	31	▼	^.	US		单元分隔符	47	/	63	?	79	O	95	_	111	o	127	?	代码: DEL

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

```

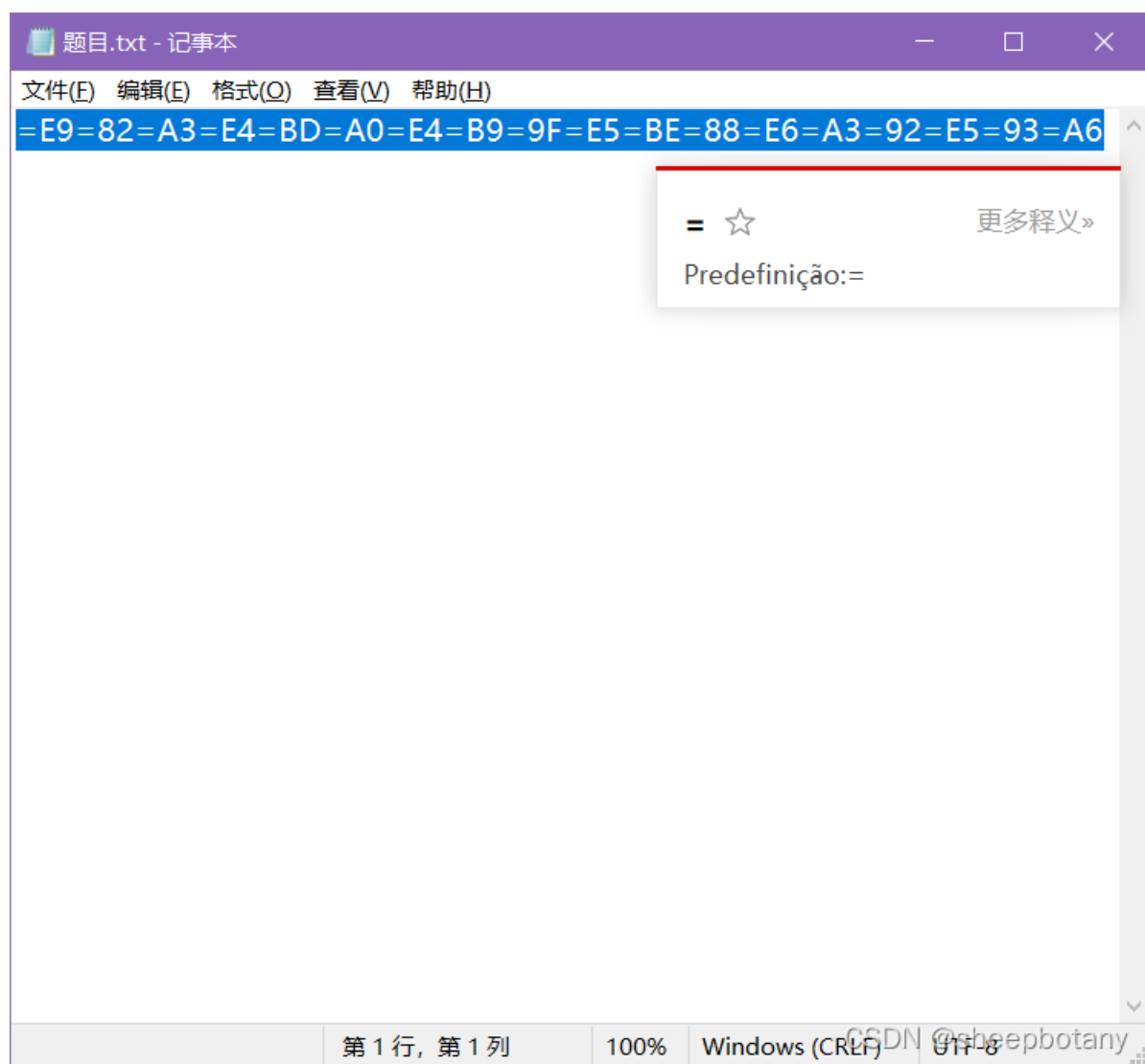
ciphertext = 'afZ_r9VYfScOeO_UL^RWUc'
j = 5
for i in ciphertext:
    print(chr(ord(i) + j), end='')
    j += 1

```

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)

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{ewtehtehflnakgw}
```

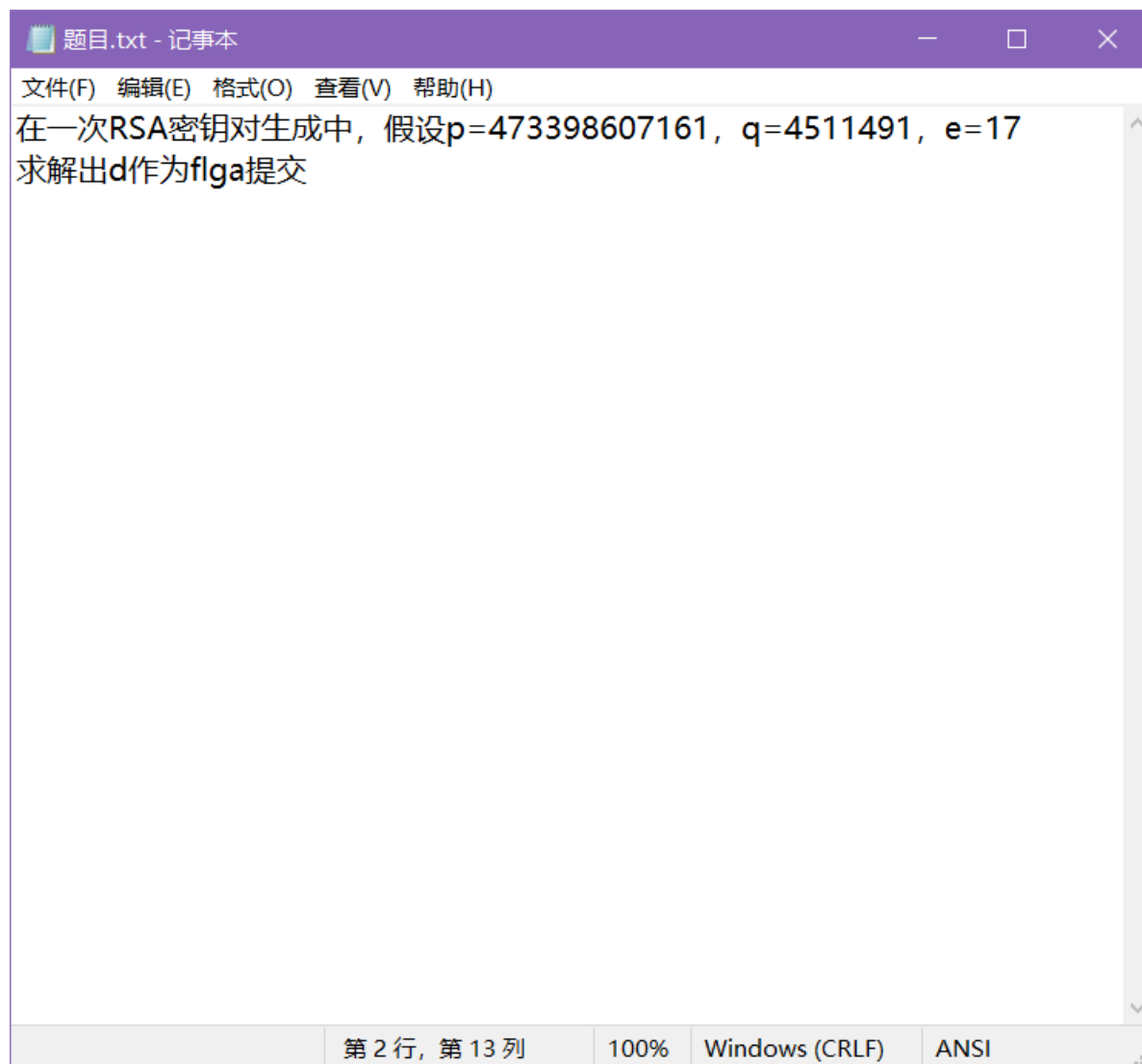
flag, f与l之间有一个字母，所以栅栏数目为2,我们直接分离后变成

```
flag{wethinkw
```

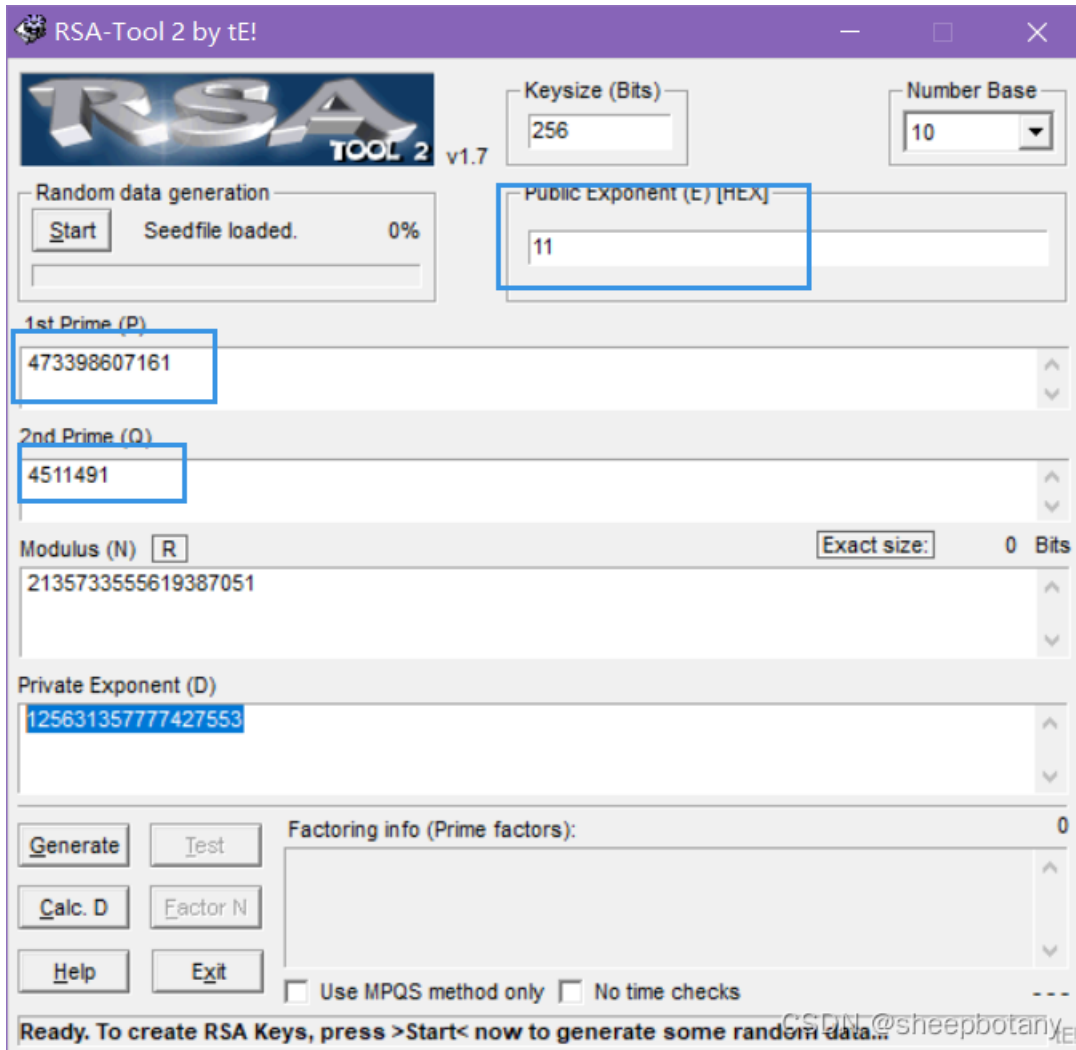
```
ehavetheflag}
```

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{12563135777427553}

九：丢失的MD5 unicode

打开来发现是python代码

```
D: > study > CTF > Solution > Crypto > 丢失的MD5 > md5.py > ...
1 import hashlib
2 for i in range(32,127):
3     for j in range(32,127):
4         for k in range(32,127):
5             m=hashlib.md5()
6             m.update('TASC'+chr(i)+'03RJM'+chr(j)+'WDJKX'+chr(k)+'ZM')
7             des=m.hexdigest()
8             if 'e9032' in des and 'da' in des and '911513' in des:
9                 print des
```

CSDN @sheepbotany

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)+'03RJM'+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)+'03RJM'+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')+'03RJM'.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

题目

解题快手榜

×

Alice与Bob

1

密码学历史中，有两位知名的杰出人物，Alice和Bob。他们的爱情经过置换和轮加密也难以混淆，即使是没有身份认证也可以知根知底。就像在数学王国中的素数一样，孤傲又热情。下面是一个大整数:98554799767,请分解为两个素数，分解后，小的放前面，大的放后面，合成一个新的数字，进行md5的32位小写哈希，提交答案。注意：得到的flag请包上flag{}提交

Flag

提交

CSDN @sheepbotany

使用指令

```
选择C:\Windows\System32\cmd.exe
D:\study\CTF\CTFtools\Crypto\yafu-1.34 (1)>yafu-x64.exe "factor(@" -batchfile 1.txt

=== Starting work on batchfile expression ===
factor(98554799767)
=====
fac: factoring 98554799767
fac: using pretesting plan: normal
fac: no tune info: using qs/gnfs crossover of 95 digits
div: primes less than 10000
fmt: 1000000 iterations
Total factoring time = 0.0195 seconds

***factors found***

P6 = 966233
P6 = 101999

ans = 1

eof; done processing batchfile
D:\study\CTF\CTFtools\Crypto\yafu-1.34 (1)>_
```

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

https://www.cmd5.com

CMD5 本站针对md5、sha1等全球通用公开的加密算法进行反向查询，通过穷举字符组合的方式，创建了明文密文对应查询数据库，创建的记录约90万亿条，占用硬盘超过500TB，查询成功率95%以上，很多复杂密文只有本站才可查询。自2006年已稳定运行十余年，国内外享有盛誉。

首页 解密范围 批量解密 会员 Wo

密文:

类型: 自动 [帮助]

查询结果:
md5(101999966233,32) = d450209323a847c8d01c6be47c81811a
md5(101999966233,16) = 23a847c8d01c6be4

CSDN @sheepbotany

直接输入即可，不需要选择类型

十一: rsarsa

题目描述:

```
题目描述.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
Math is cool! Use the RSA algorithm to decode the secret message, c, p, q,
and e are parameters for the RSA algorithm.

p =
96484230290105156765905517400104265349457376392357398006439
89352039852507298491399561035009163427050370107570733633350
911691280297777160200625281665378483
q =
11874843837980297032092405848653656852760910154543380907650
04019070428335890920857825106304773244399223064790388751006
5547947313543299303261986053486569407
e = 65537
c =
83208298995174604174773590298203639360540024871256126892889
66134574240331492986193910049266660564731664657648652621745
70063768422808697285817267464015837058999417682141387422596
89334840735633553053887641847651173776251820293087212885670
18036740680740676592363897316137581739273774783276275169010
4423869019034

Use RSA to find the secret message
第 6 行, 第 11 列 100% Unix (LF) CSDN @sheepbotany UTF-8
```

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

566320475711906605675203410288611948624114284168625070347625872299951386056498369602206199034563927
521159432993353851632162337446246238488742353033096363934467363472386277930227252609864669579747530
041292106804014323774449841951450098019673911966155244888536202329259923875632707462979091121174513
98527453977

给出了C，说明需要用到python的快速求幂取模运算

```
p=96484230290105156765905517400104265349457376392357398006439893520398525072984913995610350091634270503701075707  
3363335091169128029777160200625281665378483  
q=11874843837980297032092405848653656852760910154543380907650040190704283358909208578251063047732443992230647903  
887510065547947313543299303261986053486569407  
n=p*q  
C=83208298995174604174773590298203639360540024871256126892889661345742403314929861939100492666605647316646576486  
5262174570063768422808697285817267464015837058999417682141387422596893348407356335530538876418476511737762518202  
93087212885670180367406807406765923638973161375817392737747832762751690104423869019034  
d=56632047571190660567520341028861194862411428416862507034762587229995138605649836960220619903456392752115943299  
3353851632162337446246238488742353033096363934467363472386277930227252609864669579747530041292106804014323774449  
841951450098019673911966155  
M=pow(C, d, n)  
print(M)
```

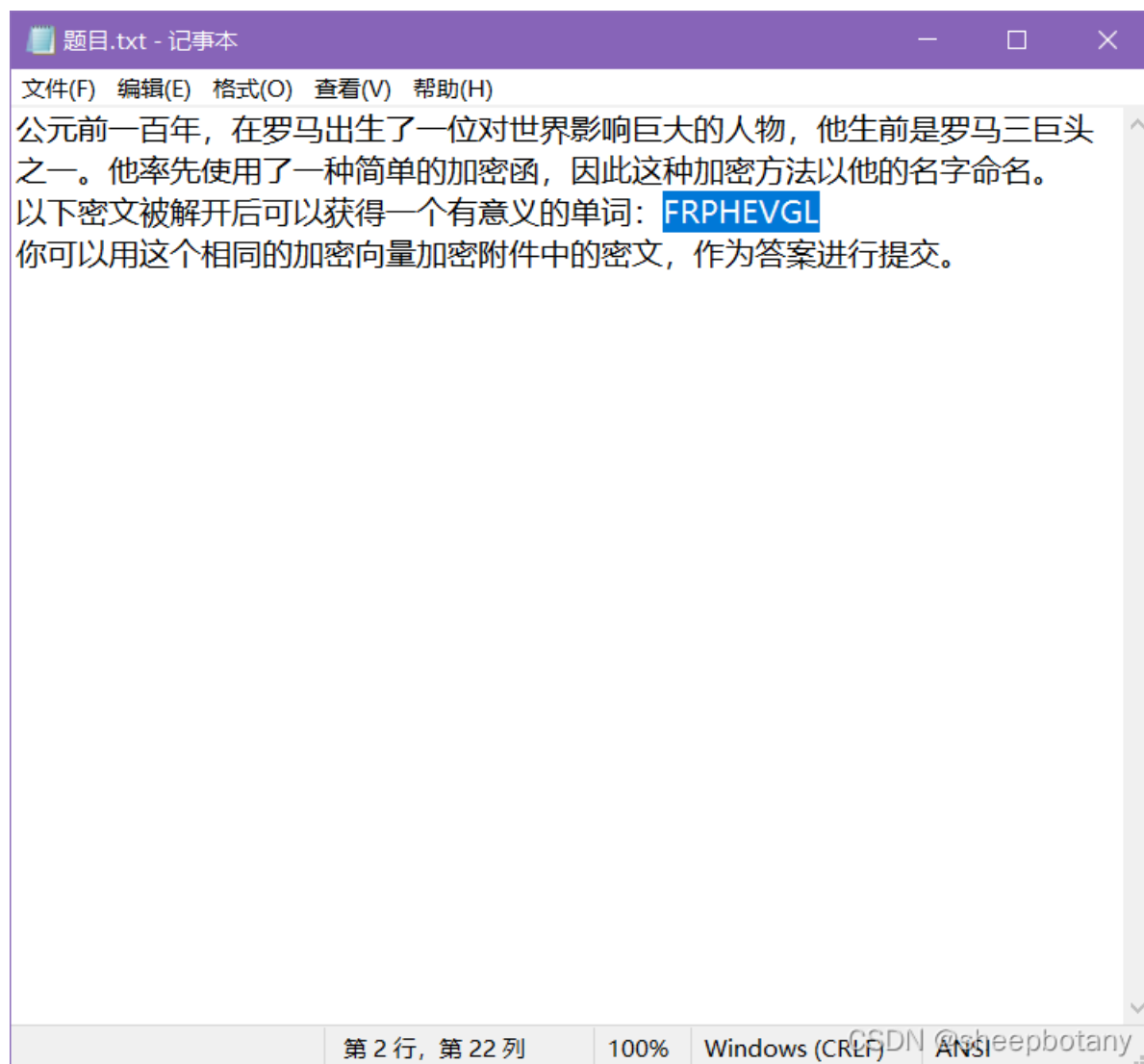
最后得到

5577446633554466577768879988

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

凯撒密码加密解密

ComeChina

位移 13 加密 解密

PbZRpuvan

CSDN @sheepbotany

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

密文: a7fcb22a88038f35a8f39d503e7f0062

类型: NTLM [帮助]

查询 加密

查询结果:
good-luck

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

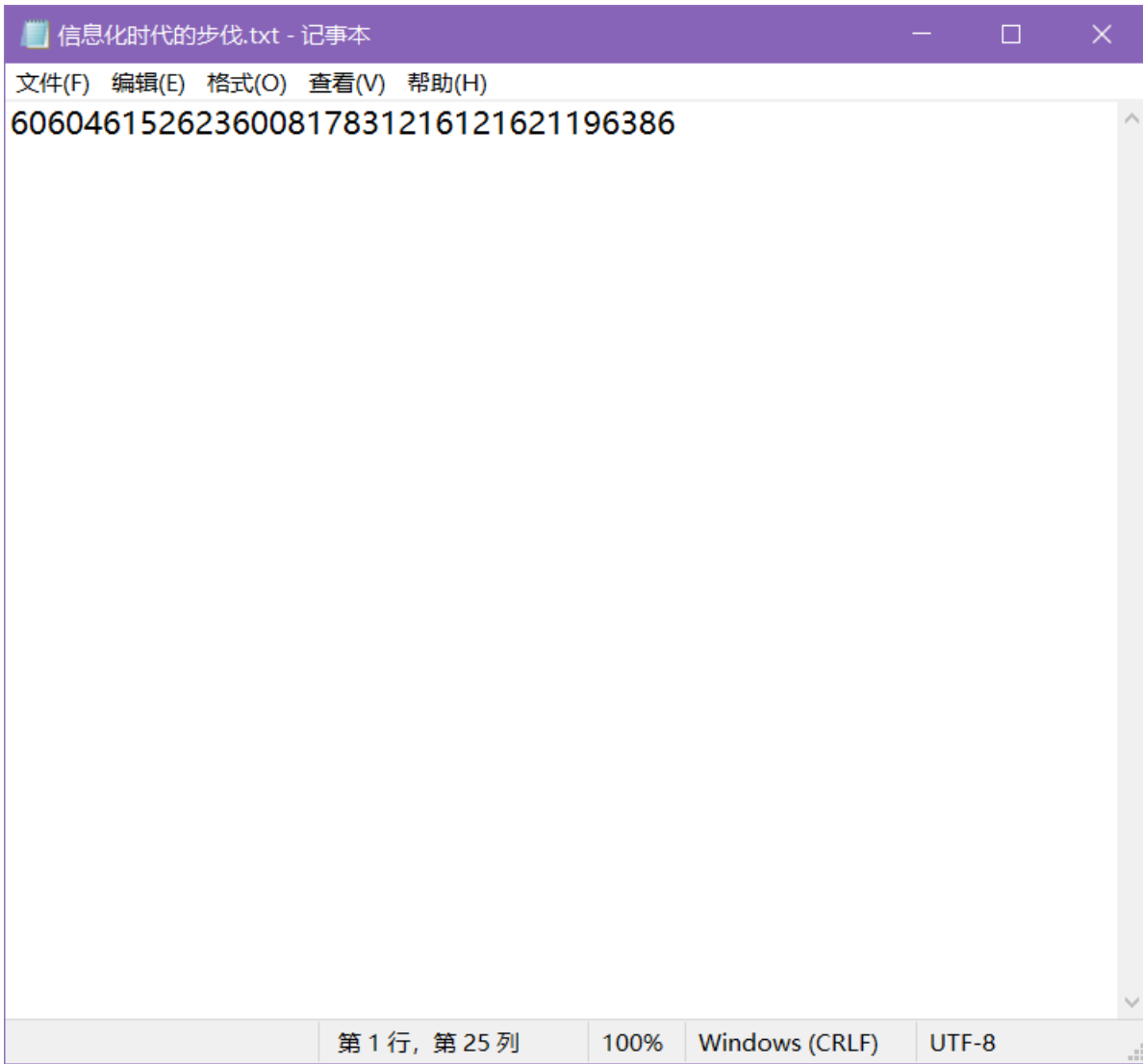
1

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)



606046152623600817831216121621196386

中文查询电码

电码反查中文

中文电码反查汉字结果:

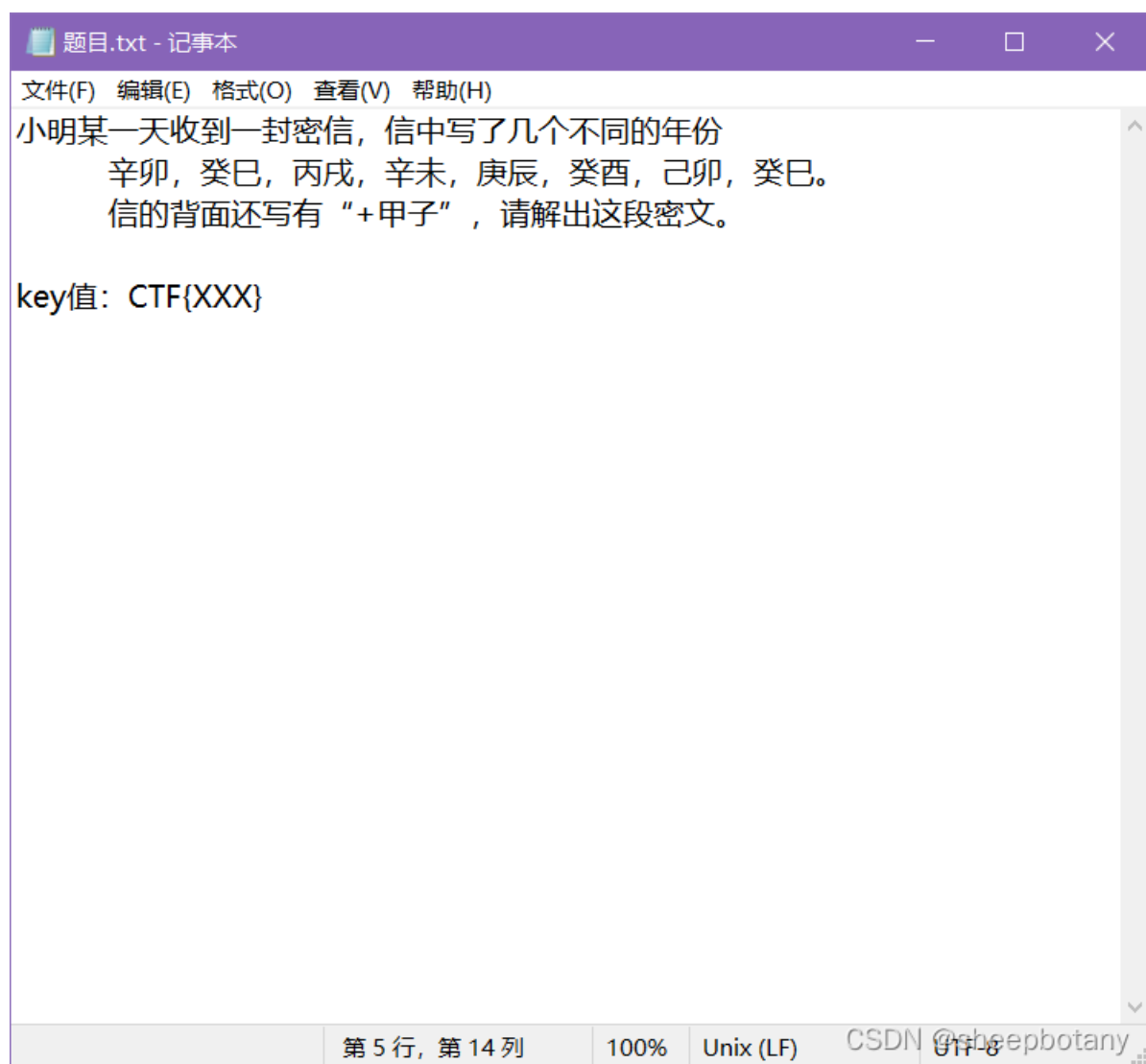
- 6060: 计
- 4615: 算
- 2623: 机
- 6008: 要
- 1783: 从
- 1216: 娃
- 1216: 娃
- 2119: 抓
- 6386: 起

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) CSDN @sheepbotany
UTF-8

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

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 XZSDMFLZ

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

栅栏密码

Railfence Cipher

XZSDMELZ

2

移除标点 (Remove Punctuation)

加密

解密

xmzfsldz

然后再丢到凯撒密码一个个试

转换前:

xmzfsldz

加密位移:

5

加密>

解密>

转换后:

shuangyu

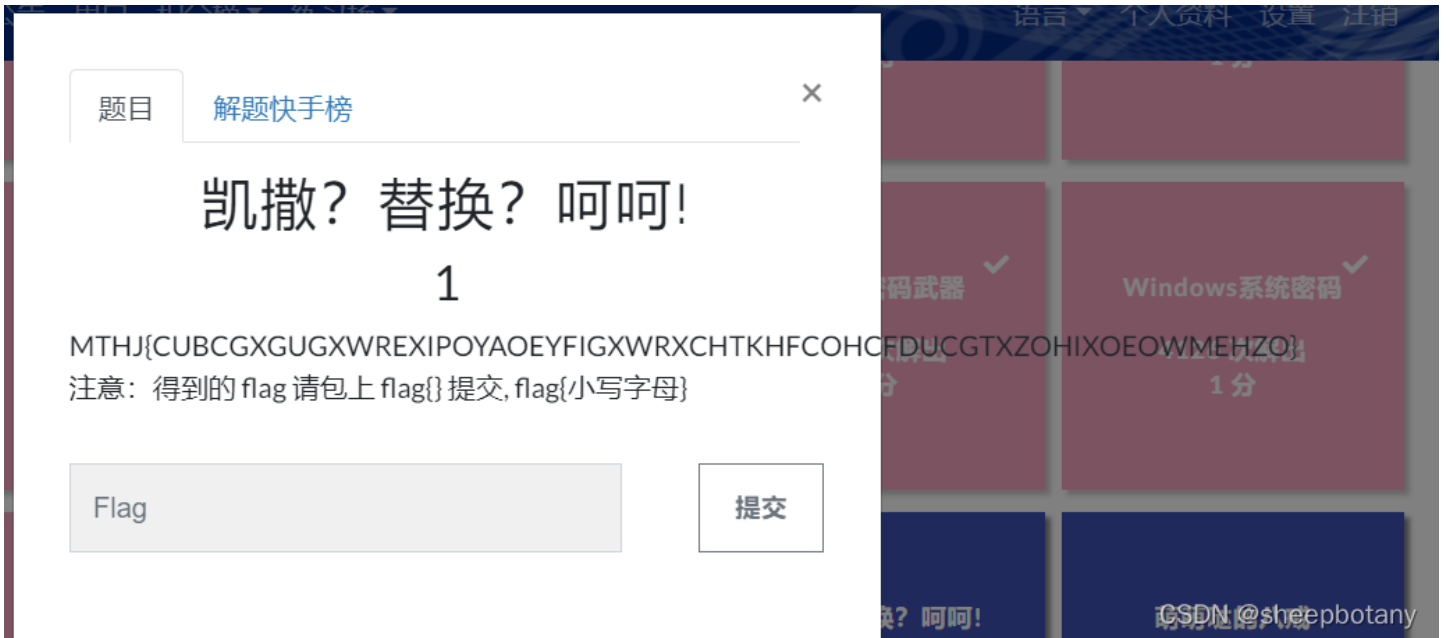
flag{SHUANGYU}

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{CUBCGXGUGXWREXIPYOAOEYFIGXWRXCHTKHFCHCFDUCGTZXOHIXOEOWMEHZO}



来个暴力破解网站喽

[quipqiup - cryptoquip and cryptogram solver](https://quipqiup.com)



选择第一个去掉空格就是flag

flag{substitutioncipherdecryptionisalwayseasyjustlikeapieceofcake}

十七 猪圈密码

题目描述:

题目

解题快手榜

×

萌萌哒的八戒

1

萌萌哒的八戒原来曾经是猪村的村长，从远古时期，猪村就有一种神秘的代码。请从附件中找出代码，看看萌萌哒的猪八戒到底想说啥 注意：得到的 flag 请包上 flag{} 提交

76ad2edd-8...

Flag

提交

CSDN @sheepbotany

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 \(hiencode.com\)](#)

猪圈密码

Pigpen Cipher

┌	┐	└	┘	□	◻	└	┘	┌	┐
└	┘	┌	┐	◻	□	└	┘	┌	┐
∨	∩	∪	∧	∩	∪	∩	∪	:	
∴	∵	∴	∵	:	=	[\]	
.	-	'	{	}		∞	∕	+	

明文: whenthepigwanttoeat

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 $\varphi(n)$ 表示若n为质数, $\varphi(n)=n-1$ 。若n是指数的某一次方即 $n=p^k$, 则 $\varphi(p^k)=p^k-p^{k-1}$ 若 $n=pq$ (两个质数)则 $\varphi(n)=\varphi(pq)=\varphi(p)\varphi(q)$

欧拉定理

如果两个正整数a和n互质, 则a的 $\varphi(n)$ 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 $da=1 \pmod n$

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 $\varphi(n)$
- 4: 随机选取整数e, e与 $\varphi(n)$ 互质
- 5: 计算出e对于 $\varphi(n)$ 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/llwky/botany/main/img/image-20220401163349449.png>)]

```
p = 8637633767257008567099653486541091171320491509433615447539162437911244175885667806398411790524083553445158113502227745206205327690939504032994699902053229
q = 12640674973996472769176047937170883420927050821480010581593137135372473880595613737337630629752577346147039284030082593490776630572584959954205336880228469
dp = 6500795702216834621109042351193261530650043841056252930930949663358625016881832840728066026150264693076109354874099841380454881716097778307268116910582929
dq = 78347226367353449019532580386470672380574033551303889137911760438881683674556098098256795673512201963002175438762767516968043599582527539160811120550041
c = 24722305403887382073567316467649080662631552905960229399079107995602154418176056335800638887527614164073530437657085079676157350205351945222989351316076486573599576041978339872265925062764318536089007310270278526159678937431903862892400747915525118983959970607934142974736675784325993445942031372107342103852

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 $da=1 \pmod n$

最后的结果

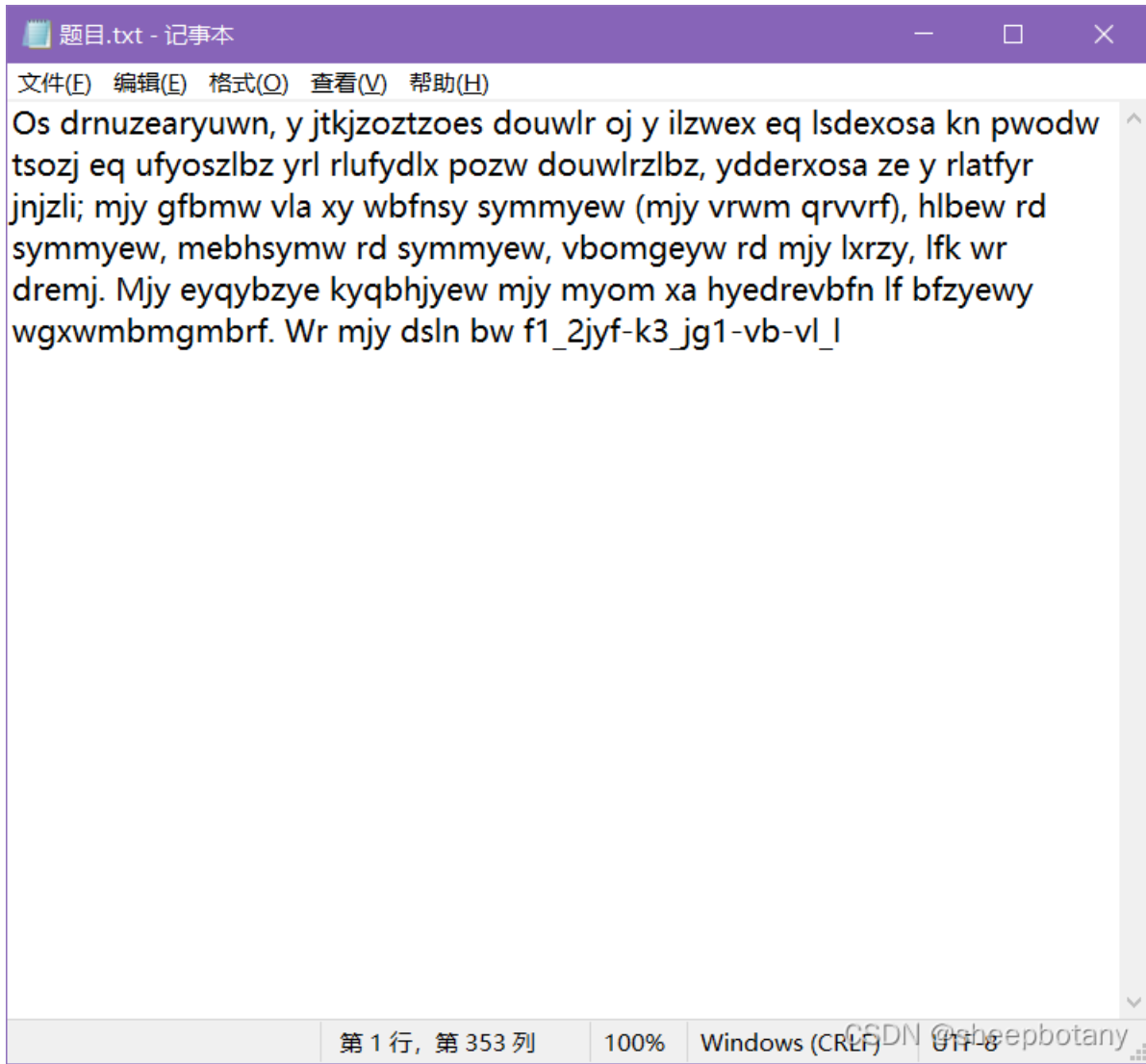
```
PS D:\study\CTF\python> & D:/study/python/python.exe d:/study/CTF/python/test.py
0x6e6f784354467b57333163306d335f37305f4368316e343730776e7d
```

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

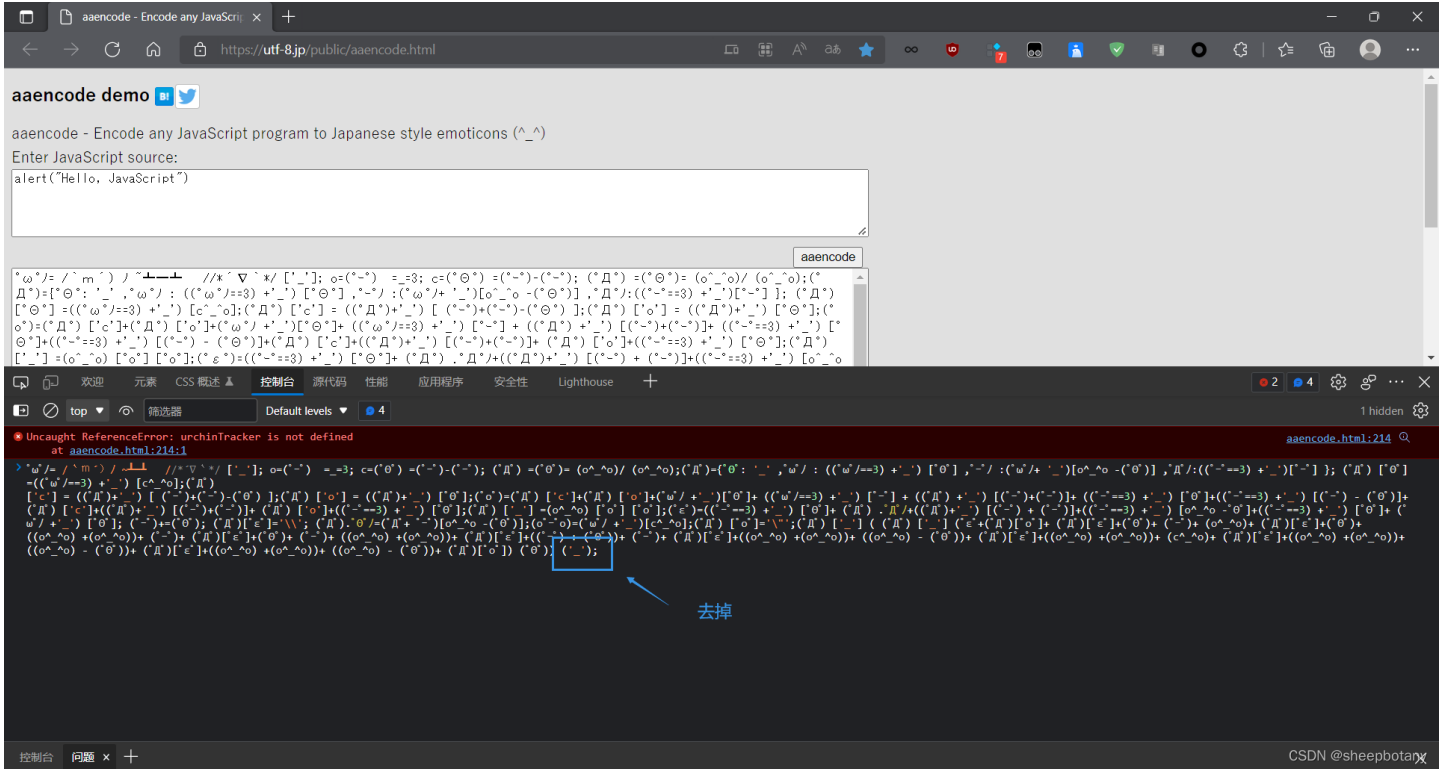
打开文件发现

```
emojs.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
|ω / = / ` m´) / ~ 1 1 // * ∇ ` * / [ ' _ ]; o = ( ° - ° ) = _ = 3 ; c = ( ° Θ ° ) = ( ° - ° ) - ( ° - ° );
( ° D ° ) = ( ° Θ ° ) = ( o ^ _ ^ o ) / ( o ^ _ ^ o ); ( ° D ° ) = { ° Θ ° : ' _ ' , ° ω / : ( ( ° ω / = 3 ) + ' _ ' ) [
° Θ ° ] , ° - ° / : ( ° ω / + ' _ ' ) [ o ^ _ ^ o - ( ° Θ ° ) ] , ° D ° / : ( ( ° - ° = 3 ) + ' _ ' ) [ ° - ° ] }; ( ° D ° ) [ ° Θ
° ] = ( ( ° ω / = 3 ) + ' _ ' ) [ c ^ _ ^ o ]; ( ° D ° )
[ ' c ' ] = ( ( ° D ° ) + ' _ ' ) [ ( ° - ° ) + ( ° - ° ) - ( ° Θ ° ) ]; ( ° D ° ) [ ' o ' ] = ( ( ° D ° ) + ' _ ' ) [ ° Θ ° ]; ( ° o ° ) = (
° D ° ) [ ' c ' ] + ( ° D ° ) [ ' o ' ] + ( ° ω / + ' _ ' ) [ ° Θ ° ] + ( ( ° ω / = 3 ) + ' _ ' ) [ ° - ° ] + ( ( ° D ° )
+ ' _ ' ) [ ( ° - ° ) + ( ° - ° ) ] + ( ( ° - ° = 3 ) + ' _ ' ) [ ° Θ ° ] + ( ( ° - ° = 3 ) + ' _ ' ) [ ( ° - ° ) - ( ° Θ ° ) ] + ( °
D ° ) [ ' c ' ] + ( ( ° D ° ) + ' _ ' ) [ ( ° - ° ) + ( ° - ° ) ] + ( ° D ° ) [ ' o ' ] + ( ( ° - ° = 3 ) + ' _ ' ) [ ° Θ ° ]; ( ° D ° )
[ ' _ ' ] = ( o ^ _ ^ o ) [ ° o ° ] [ ° o ° ]; ( ° ε ° ) = ( ( ° - ° = 3 ) + ' _ ' ) [ ° Θ ° ] + ( ° D ° ) . ° D ° / + ( ( °
D ° ) + ' _ ' ) [ ( ° - ° ) + ( ° - ° ) ] + ( ( ° - ° = 3 ) + ' _ ' ) [ o ^ _ ^ o - ° Θ ° ] + ( ( ° - ° = 3 ) + ' _ ' ) [ °
Θ ° ] + ( ° ω / + ' _ ' ) [ ° Θ ° ]; ( ° - ° ) + = ( ° Θ ° ); ( ° D ° ) [ ° ε ° ] = '\\'; ( ° D ° ) . ° Θ ° / = ( ° D ° + ° - °
) [ o ^ _ ^ o - ( ° Θ ° ) ]; ( ° - ° o ) = ( ° ω / + ' _ ' ) [ c ^ _ ^ o ]; ( ° D ° ) [ ° o ° ] = '\\"; ( ° D ° ) [ ' _ ' ] ( ( ° D
° ) [ ' _ ' ] ( ° ε ° + ( ° D ° ) [ ° o ° ] + ( ° D ° ) [ ° ε ° ] + ( ° Θ ° ) + ( ° - ° ) + ( o ^ _ ^ o ) + ( ° D ° ) [ ° ε ° ] + ( °
Θ ° ) + ( ( o ^ _ ^ o ) + ( o ^ _ ^ o ) ) + ( ° - ° ) + ( ° D ° ) [ ° ε ° ] + ( ° Θ ° ) + ( ° - ° ) + ( ( o ^ _ ^ o )
+ ( o ^ _ ^ o ) ) + ( ° D ° ) [ ° ε ° ] + ( ( ° - ° ) + ( ° Θ ° ) ) + ( ° - ° ) + ( ° D ° ) [ ° ε ° ] + ( ( o ^ _ ^ o )
+ ( o ^ _ ^ o ) ) + ( ( o ^ _ ^ o ) - ( ° Θ ° ) ) + ( ° D ° ) [ ° ε ° ] + ( ( o ^ _ ^ o ) + ( o ^ _ ^ o ) ) +
( c ^ _ ^ o ) + ( ° D ° ) [ ° ε ° ] + ( ( o ^ _ ^ o ) + ( o ^ _ ^ o ) ) + ( ( o ^ _ ^ o ) - ( ° Θ ° ) ) + ( ° D ° ) [
° ε ° ] + ( ( o ^ _ ^ o ) + ( o ^ _ ^ o ) ) + ( ( o ^ _ ^ o ) - ( ° Θ ° ) ) + ( ° D ° ) [ ° o ° ] ( ° Θ ° ) ( ' _ ' );
```

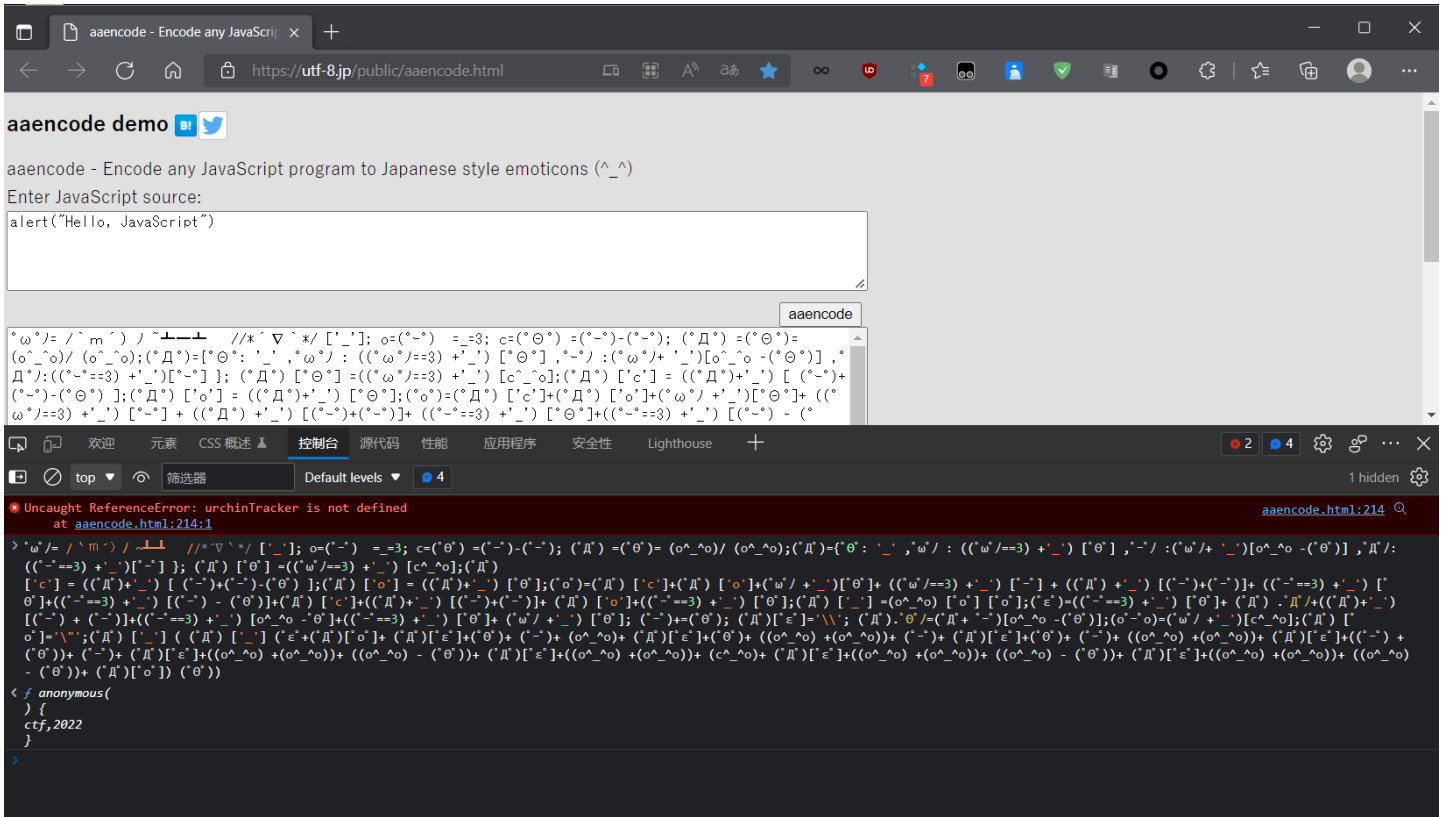
进入转换网站

[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

题目
解题快手榜
×

Cipher

1

还能提示什么呢? 公平的玩吧 (密钥自己找)

Dncnoqqfliqrpgeklwmppu 注意: 得到的 flag 请包上 flag{} 提交, flag{小写字母}

Flag

提交

CSDN @sheepbotany

打开破解网站

[Playfair Cipher \(rumkin.com\)](http://rumkin.com)

密钥根据题目公平的玩吧, 是playfair

rectangle and is encoded as "NV".

The resulting message is now "KC NV MP PO AB OC FQ NV" or "KCNVMPPOABOCFQNV" if you remove the spaces.

This encoder will do all of the lookups for you, but you still need to do a few things yourself.

1. Manually break apart double letters with X (or any other) characters. Some people break apart all doubles, others break all doubles that happen in the same two-letter chunk. This encoder requires neither in order to be more flexible.
2. Manually make the message length even by adding an X or whatever letter you want. If you don't, the encoder will automatically add an X for you.

All non-letters are ignored and not encoded. The one letter that you select to share a square in the cipher is translated. Numbers, spaces, and punctuation are also skipped. If you leave two letters together in a two-letter chunk, they will be encoded by moving down and right one square ("LL" becomes "RR") where as traditional Playfair ciphers will automatically insert an X for you.

This particular cipher was used by the future U.S. President, John F. Kennedy, Sr. He sent a [message](#) about a boat going down.

Encrypt

Translate the letter **J** into **I**

Encode double letters (down and right one spot) 密钥

Alphabet Key: - [Show Keymaker](#)

Tableau Used:

A	B	C	D	E
F	G	H	I	K
L	M	N	O	P
Q	R	S	T	U
V	W	X	Y	Z

Your message: 密文

[Add Spaces](#) - Adds a space after every other letter (only A-Z count) so you can see the letter pairs.
[Only Letters](#) - Removes all non-letters from the text.

This is your encoded or decoded text:

明文
 Type in your message and see the results here!

CSDN @sheepbotany

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

Challenge

38 Solves



Base family

1

解密下列字符串: zI1K1#5XxS&#bOWb"w#xNy[546.(!C

flag{b6a22494bc3}

Submit

CSDN @sheepbotany

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](#)

AmanCTF - BASE91编码解码

在线BASE91编码解码

```
zI1K1#5XxS&#bOWb"w#xNy[546.(!C
```

加密

解密

```
ZmxhZ3tiNmEyMjQ5NGJmM30=
```

得到base64再进入base64进行解密

Challenge

38 Solves

✕

Base family

1

解密下列字符串: zI1K1#5XxS&#bOWb"w#xNy[546.(!C

```
flag{b6a22494bc3}
```

Submit

解密工具集合

[在线工具 - Bugku CTF](#)