CTF Crypto(密码学)总结

原创

Sn0w/ 于 2019-04-16 10:35:30 发布 15872 收藏 80

分类专栏： CTF_Writeup 文章标签： CTF密码学总结

本文链接：https://blog.csdn.net/qq_43431158/article/details/89301571

CTF_Writeup 专栏收录该内容

32 篇文章 4 订阅

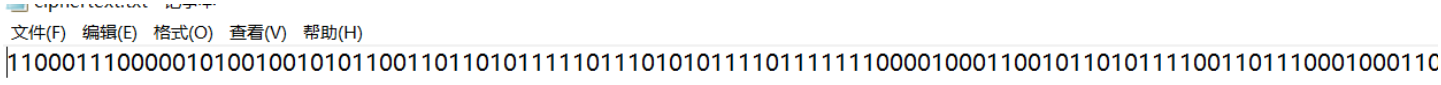
订阅专栏

最近接触了一些密码学的题，感觉特别有意思，写下博客来记录一下，以免忘记

一：哈夫曼树

哈夫曼树（也称为最优二叉树），虽然（目前）没学，但是百度、谷歌大法无敌。

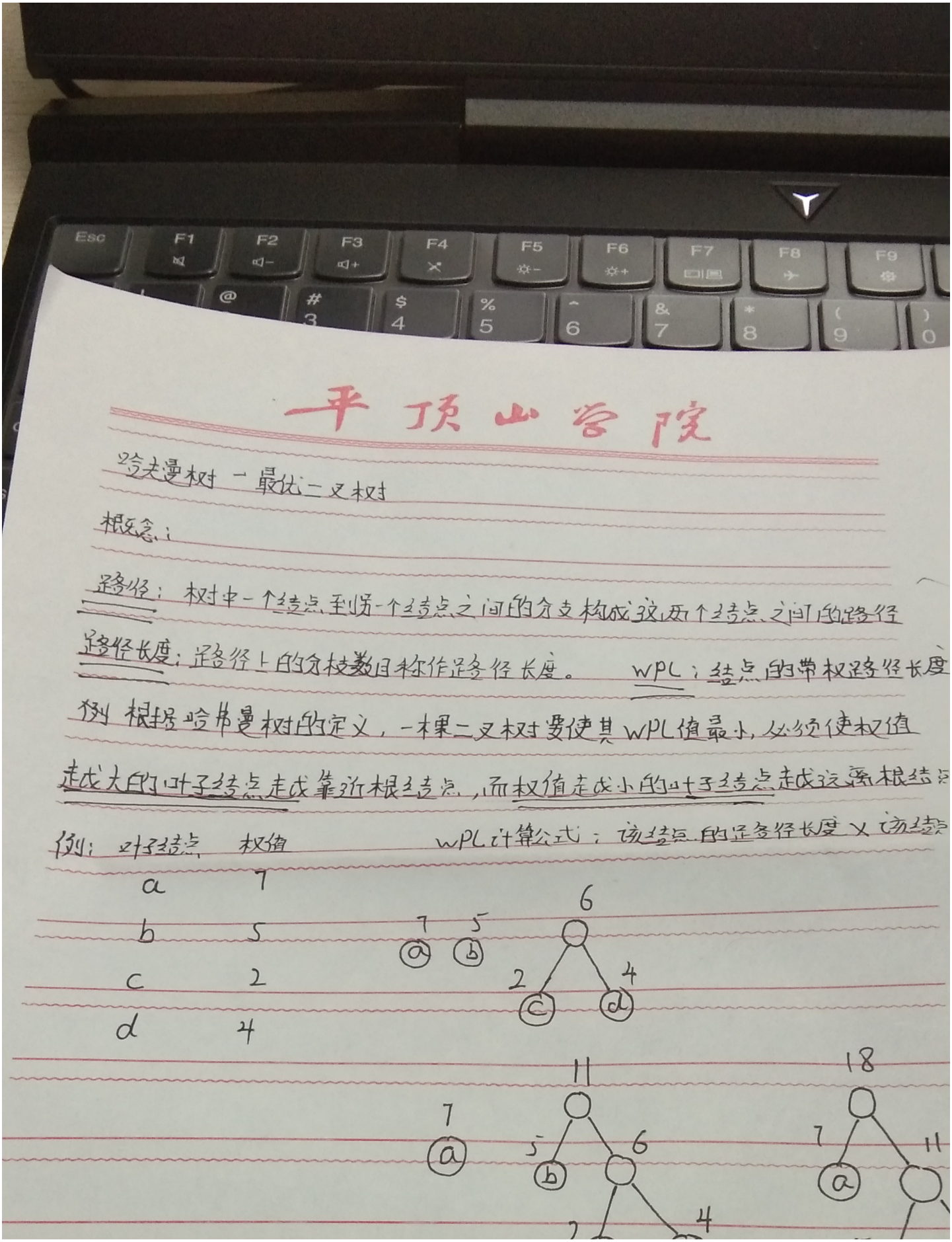
查查原理，再去做题。

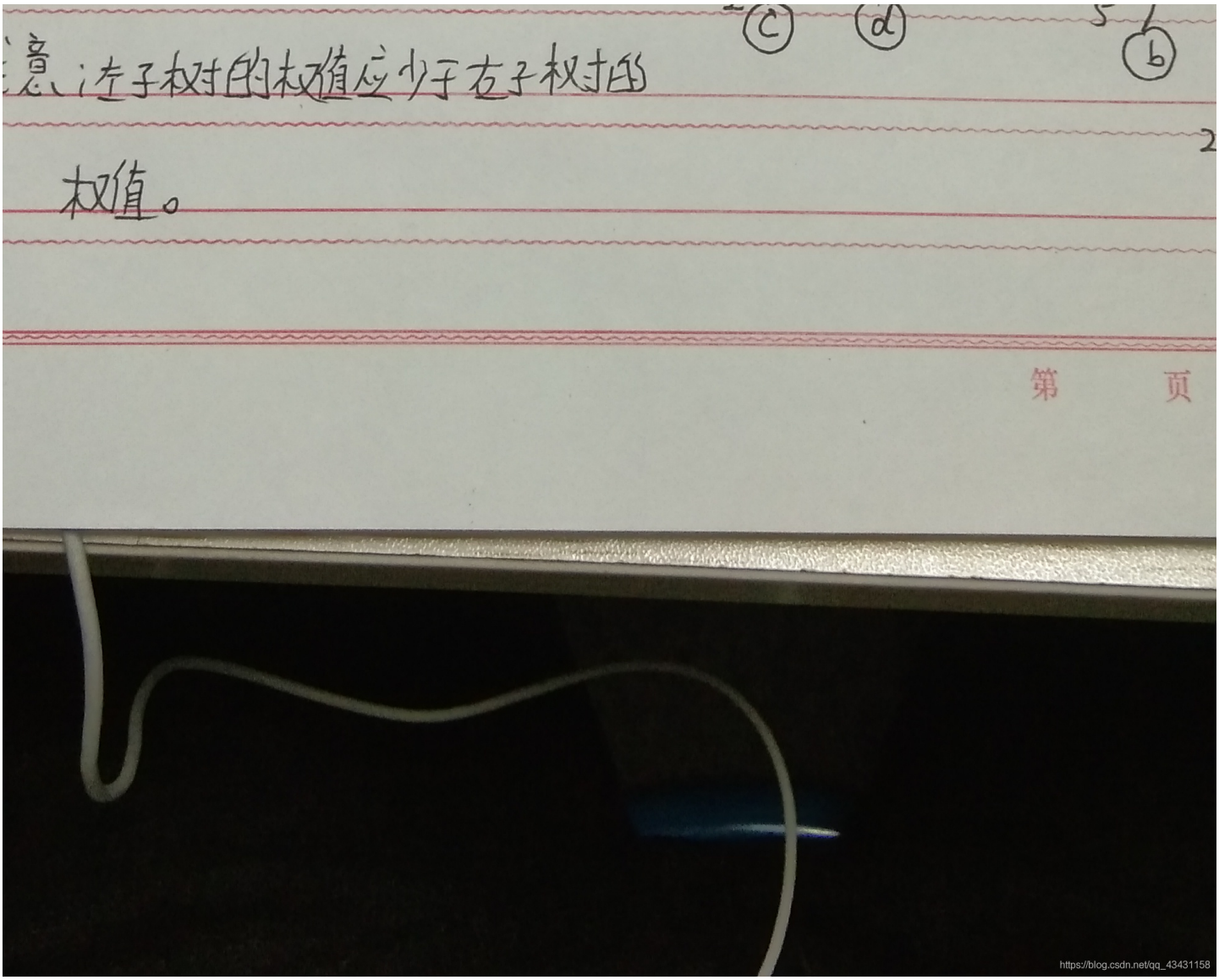


a:4
d:9
g:1
f:5
l:1
0:7

5:9
{:1
}:1

经过一番查找，懂了原理，就总结了一下





简单说：

叶子结点：权值

a : 4

d ： 9

g : 1

f : 5

l : 1

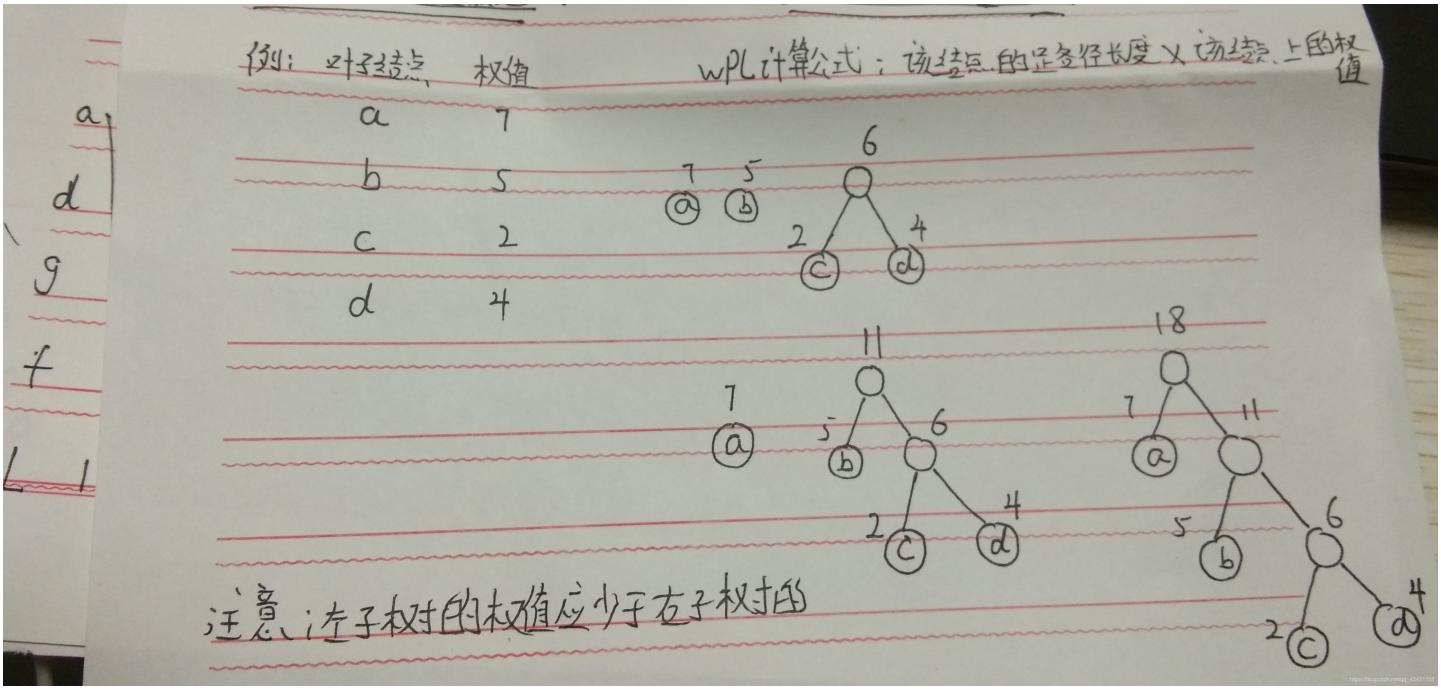
0 : 7

5 : 9

{ : 1

} : 1

画图时最上面的是根，而最优二叉树的规则则是需要权值大的尽量放在上面
例如：
叶子结点：权值
a 7
b 5
c 2
d 4

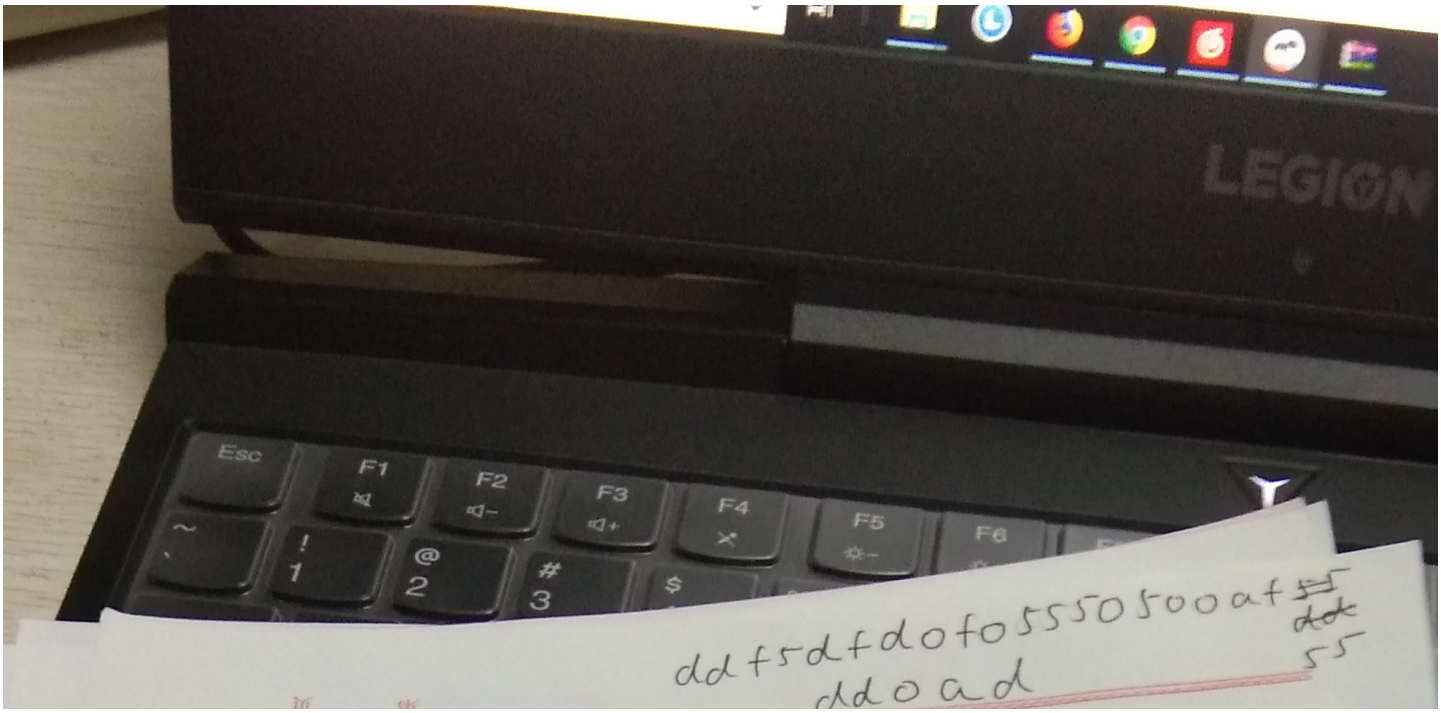


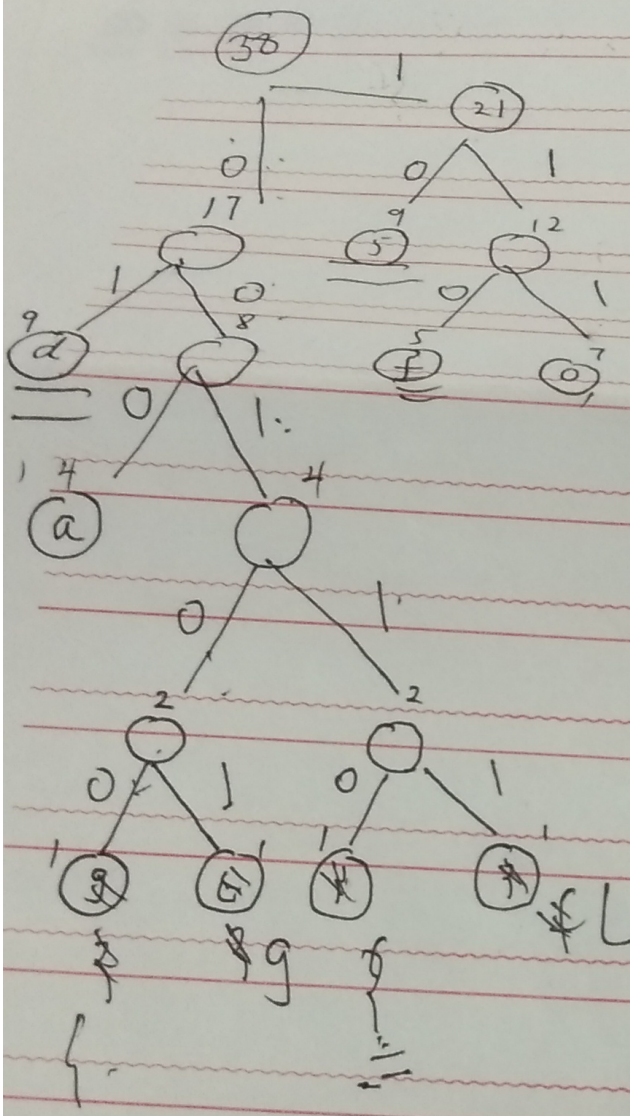
搞懂了这个，但是这个题中还给了我们一堆数

```
11000111000001010010010101100110110101111101110101011110111111100001000110010110101111001101110001000110
```

这些代表上面意思那？？经过查找发现
发现原来这是**哈夫曼树编码**详细的介绍

那我们先来完成第一步，画树。





f: 110

c: 00111

a: 000

g: 00101

r: 00100

一开始没画对，画了三四遍，才算画出来，不过不太熟练，还得练。
画的时候最好从下到上画，先把权值小的画出来，一步一步往上画。

既然画出来了，那就用哈夫曼树编码来把每个数字或字符用编码的方式表示出来。
通过画也发现在同一分支中，哪个权值大，那么哪个就是1。
例如:
17下的d（权值为9）和权值为8的相比，那么d的路径就表示为1.

接下来就是安装这样的方法把那么字符都用编码表示出来

```
f:110
l:00111
a:000
g:00101
.....
```

下面都这样表示
接下来就开始进行比对

```
1100011100000101001001010110011011010111110111010101111011111110000100011001011010111100110111000100011 0
```

一般CTF题的提交格式都是**flag{...}**
所以我们这里就首先看第一个是不是**f**
110 恰好对应 **f**
00111 恰好对应 **l**
000 恰好对应 **a**
00101 恰好对应 **g**
前面对应了几乎就没啥子问题了，但是还有一点比较坑的有的因为权值相等，需要在转换的时候看是否应该换一下位置。
例如：
{ 和 **}** 权值相等，在转化时看是否需要进行换位置。

我们再观察我们上面画的图，其中**5**和**d**的权值也相同，所以如果提交的答案不对的话，就尝试一下换下位置。
这道题是西湖论剑的题，下面有进入决赛大佬的WP。
关于西湖题的wp

二：传统知识+古典密码

传统知识+古典密码　分值：10

来源：霜羽　难度：易　参与人数：9979人　Get Flag：42

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}

在实验吧上做了一道很有意思的题目。
首先就想了解一下传统知识吧

六十甲子顺序表

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

六十甲子顺序表

在百度上找到六十甲子顺序表，就先对应着把数字写出来。

辛卯28，癸巳30，丙戌23，辛未8，庚辰17，癸酉10，己卯16，癸巳30。
“+甲子60”
（这里有一个疑问，按图来说甲子不应该是1吗？？？ 为什么会+60。。。其实这里面还是对传统文化的不熟悉，查查百度，如果还晕的话，记住就行了）

一甲子为60年

天干地支简称“干支”，取义于树木的干和枝

天干有十：甲、乙、丙、丁、戊（wù）、己、庚、辛、壬（rén）、癸（guǐ）；地支十二：子、丑、寅、卯（mǎo）、辰（chén）、巳（sì）、午、未（wèi）、申、酉（yǒu）、戌（xū）、亥。天干地支组合成如下六十个计时序号，作为纪年、月、日、时的名称，叫“干支纪年法”。

六十甲子顺序

1—10 甲子 乙丑 丙寅 丁卯 戊辰 己巳 庚午 辛未 壬申 癸酉 11—20 甲戌 乙亥 丙子 丁丑 戊寅 己卯

1~10 甲子 乙丑 丙寅 丁卯 戊辰 己巳 庚午 辛未 壬申 癸酉 11~20 甲戌 乙亥 丙子 丁丑 戊寅 己卯 庚辰 辛巳 壬午 癸未 21~30 甲申 乙酉 丙戌 丁亥 戊子 己丑 庚寅 辛卯 壬辰 癸巳 31~40甲午 乙未 丙申 丁酉 戊戌 己亥 庚子 辛丑 壬寅 癸卯 41~50甲辰 乙巳 丙午 丁未 戊申 己酉 庚戌 辛亥 壬子 癸丑 51 ~60甲寅 乙卯 丙辰 丁巳 戊午 己未 庚申 辛酉 壬戌 癸亥

用六十甲子依次纪年，六十年一个轮回。干支纪年法的新一年由立春开始，公元纪年的一年以立春为界前后分属不同的干支纪年，这一点不熟悉的人容易搞错，应特别注意。

处理完之后的数

88,90,83,68,77,70,76,90

转换一下ASCII码看看

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											ASCII打印字符												
		0000						0001					0010		0011		0100		0101		0110		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	⌂	^Backspace 代码：DEL

注：表中的ASCII字符可以用“Alt + 小键盘上的数字键”方法输入。 2013/08/08

XZSDMFLZ

没思路了。。。

看看题目咋提示的

古典密码

古典密码一般涉及的就是**替换**或**移位**

就先用栅栏密码试试了

一共8位： 可以分为2个字一组，也可以是4个字一组，都试试。

先用2个字为一组的，解出来栅栏密码在线解密

XMZFSLDZ

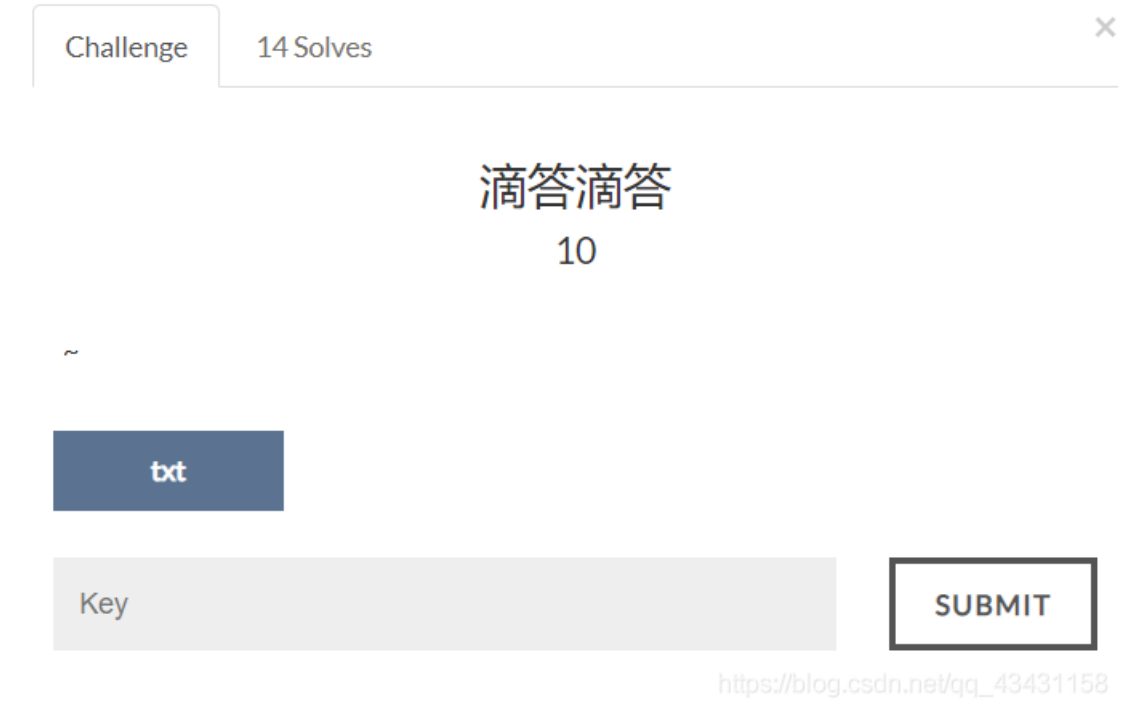
再用凯撒密码解密凯撒在线解密

发现有一串字母好像是有点意义的，拿出来试试。

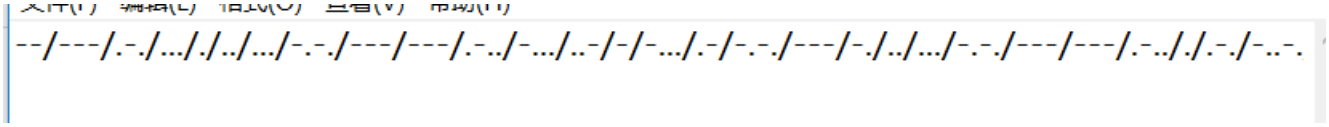
shuangyu

改为大写，因为我们输入的就是大写。
SHUANGYU
CTF{SHUANGYU}
提交结果正确，就不用再往下试了。
这个题有很多好玩的地方，需要了解传统的甲子表，需要了解栅栏密码，要了解凯撒密码。
wiki大佬关于密码学的WP
各种加密方式

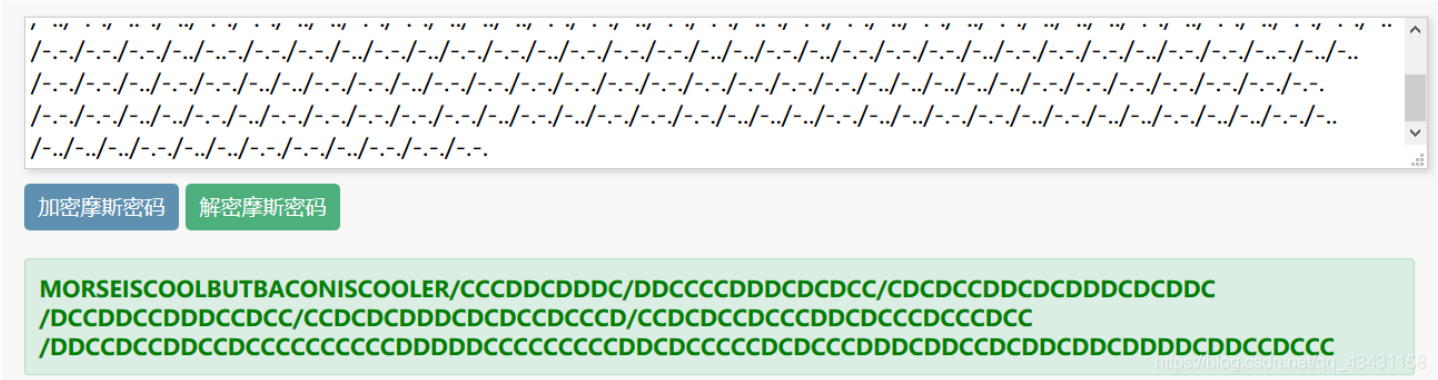
三、滴答滴答



下载起来，打开后是这样的



看过柯南的都应该知道这个是摩斯密码，所以拿去解一下密，看看会出现什么？
摩斯密码解密



后面的一堆C和D，但是前面我看到了MORSE（摩斯）后面的应该有意义，百度翻译看一下吧

MORSE IS COOL BUT BACON IS COOLER

摩尔斯很酷，但培根更酷

培根？？？，查一下。

原理

编辑

加密时，明文中的每个字母都会转换成一组五个英文字母。其转换依靠下表：

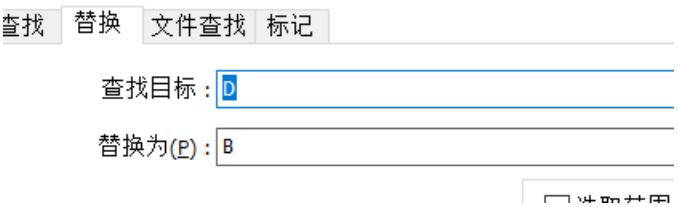
A/a	aaaaa	H/h	aabbb	O/o	abbba	V/v	babab
B/b	aaaab	I/i	abaaa	P/p	abbbb	W/w	babba
C/c	aaaba	J/j	abaab	Q/q	baaaa	X/x	babbb
D/d	aaabb	K/k	ababa	R/r	baaab	Y/y	bbaaa
E/e	aabaa	L/l	ababb	S/s	baaba	Z/z	bbaab
F/f	aabab	M/m	abbaa	T/t	baabb		
G/g	aabba	N/n	abbab	U/u	babaa		

加密者需使用两种不同字体，分别代表A和B。准备好一篇包含相同AB字数的假信息后，按照密文格式化假信息，即依密文中每个字母是A还是B分别套用两种字体。

解密时，将上述方法倒转。所有字体一转回A，字体二转回B，以后再按上表拼回字母。

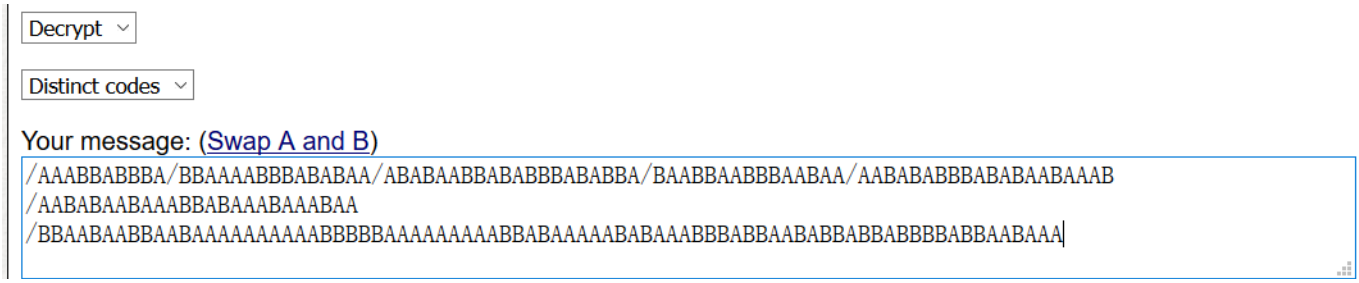
了解培根加密之后，我们就知道那一堆C和D有啥用处了

首先，我们先把C转化为A，D转化为B。



转化完成后，进行解密

培根加密解密



This is your encoded or decoded text:

DO YOU KNOW THE FOUR FENCE ZGIAHYANAUOZNXWI

结果出来了，百度翻译一下。

你知道四道栅栏吗?

当时在这里卡了，猛的一下不知道啥意思。。。还是太菜。经过学长提醒。。。
是**栅栏密码**，猛的一下明白了，原来**ZGIAHYANAUOZNXWI**这个就是密文，而且也提示了四道栅栏，所以每组四个字。

ZGIAHYANAUOZNXWI

每组字数 4 加密 解密

ZHANGYUXIAOWANZI

章鱼小丸子
至于提交就有点坑了，不用flag{}格式，直接提交就行。不过这道题确实很有意思，了解了摩斯密码，培根密码，栅栏密码。不过还得练，还是太菜，有的时候就是想不到。。。


即刻 @灵魂蹒跚独行