CTF密码学题目初探

原创

wsq柚子 于 2020-06-15 17:53:00 发布

分类专栏： CTF 文章标签： 密码学

本文链接：https://blog.csdn.net/hzy_wsq/article/details/106765000

CTF密码学题目初探（一）

密码学总结（一）

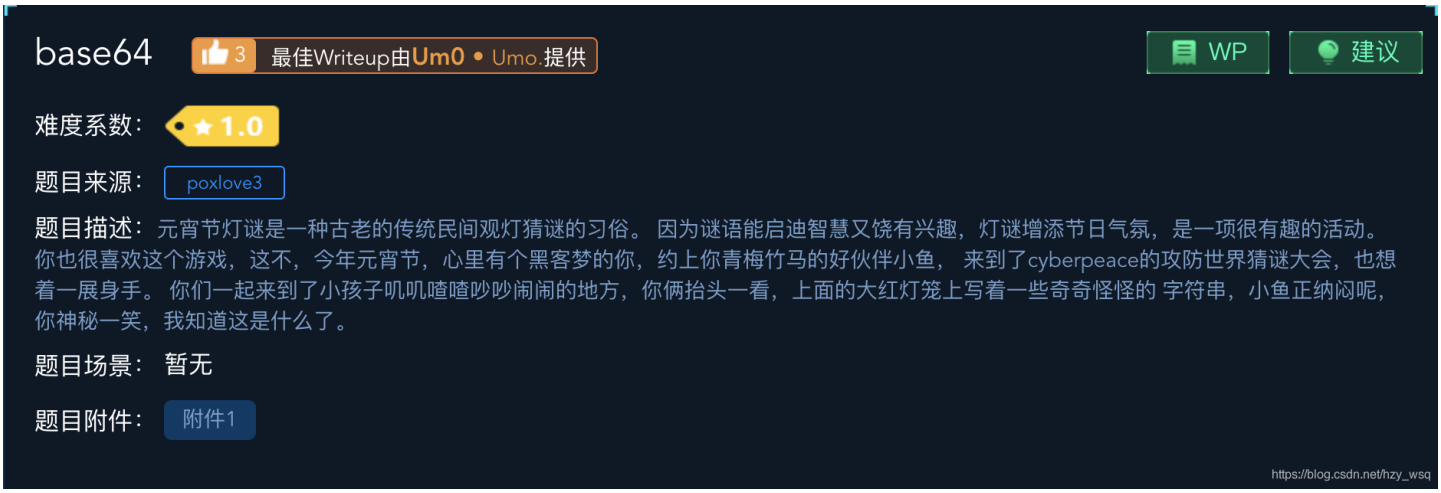
密码学一般可分为 **古典密码学** 和**现代密码学**。CTF中脑洞密码题(非现代加密方式)一般都是各种古典密码的变形。

1.常见线索

一般情况下，题目中会给出一些线索。比如**题目名称，题目描述**等。

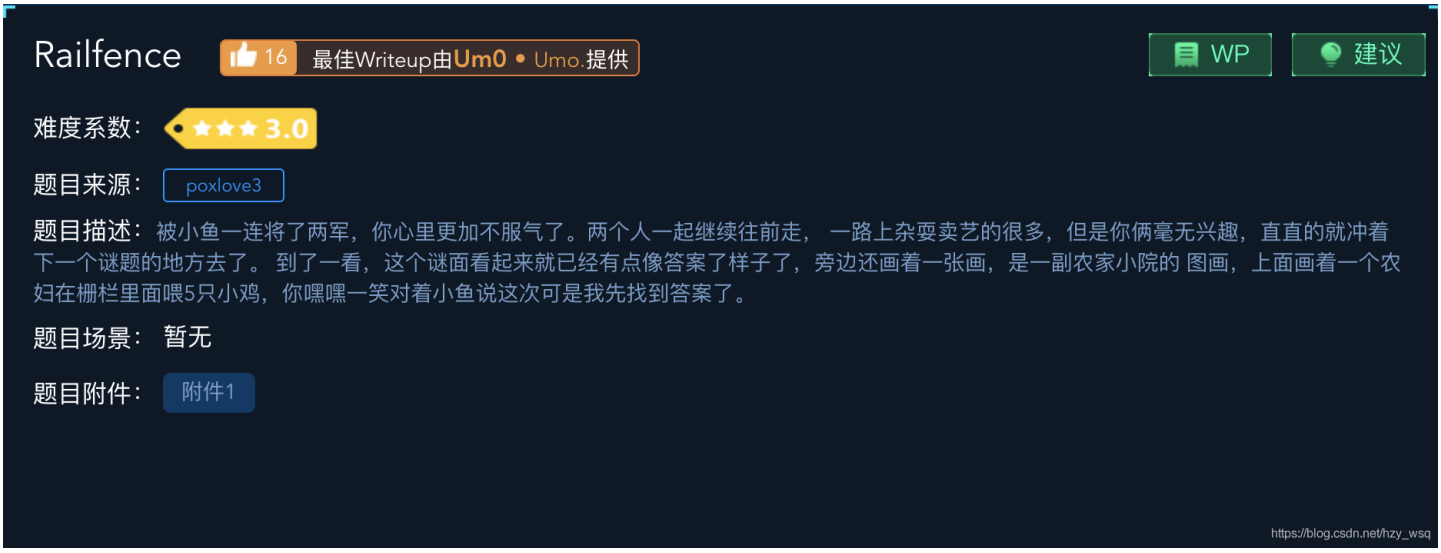
举例：题目名称为base64

题目链接



举例：题目描述中写了“上面画着一个农妇在栅栏里面喂5只小鸡”...

题目链接



2.常见编码

base64/32/16编码

加密解密网站链接

原理：Base64是用于传输8Bit字节码的编码方式之一，基于64个可打印字符来表示二进制数据的表示方法。由于2的6次方等于64，所以每6个比特为一个单元，对应某个可打印字符。三个字节有24个比特，对应4个base64单元，即3个字节可表示4个可打印字符。它可用来作为电子邮件的传输编码。在base64中的可打印字符包括字母A-Z、a-z、数字0-9，共有62个字符。

base32中只有大写字母（A-Z）和数字234567。

base16中只有数字0-9以及大写字母ABCDEF。

当看到==或=号的加密方式时，可以考虑base64。

ASCII编码

ASCII对照表

举例：突然天上一道雷电gndk€rlqhmtkwwp}z

比较一下"gndk"与"flag"的ASCII码，

gndk的10进制的ASCII码分别是：103 110 100 107

flag的10进制的ASCII码分别是 ：102 108 97 103

发现ASCII以此减少 1 2 3 4，所以以此类推解密得flag{lei_ci_jiami}

Morse莫斯密码

通过不同的排列顺序来表达不同的英文字母、数字和标点符号。

莫斯密码翻译器

莫斯密码包括5中状态

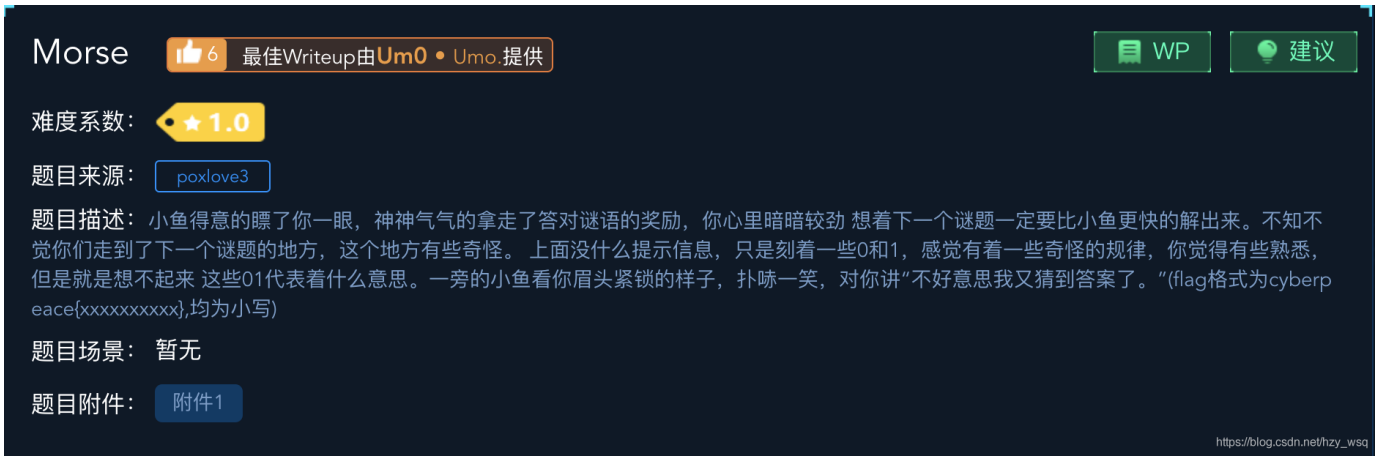
1.点（.）

2.划（-）

3.每个字符间短的停顿（在点和划之间的停顿）

4.每个词之间中等的停顿

5.以及句子之间长的停顿



11 111 010 000 0 1010 111 100 0 00 000 000 111 00 10 1 0 010 0 000 1 00 10 110

（这里只用 0和1，所以应该是用01代替.、-。 那么到底是用1代表.还是用0代表.呢？ 都试一下）

Unicode编码

Unicode在线编码解码链接

原文本：You had me at hello

编码

后：\u0059\u006f\u0075\u0020\u0068\u0061\u0064\u0020\u006d\u0065\u0020\u0061\u0074\u0020\u0068\u0065\u006c\u006c\u006f

XXencode编码

XXencode在线编码解码

原理：原理：XXencode将输入文本以每三个字节为单位进行编码。如果最后剩下的资料少于三个字节，不够的部分用零补齐。这三个字节共有24个bit，以6bit为单位分为4个组，每个组以十进制来表示所出现的数值只会落在0-63之间。以所对应值的位置字符代替。它所选择的可打印字符是：

±0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz，一共64个字符。跟base64打印字符相比，就是uuencode多一个‘-’字符，少一个‘/’字符。但是，它里面字符顺序与base64完全不一样。

（原文链接：https://blog.csdn.net/pdsu161530247/article/details/75667218）

原文本：The quick brown fox jumps over the lazy dog

编码后：hJ4VZ653pOKBf647mPrRi64NjS0-eRKpkQm-jRaJm65FcNG-gMLdt64FjNkc+

UUencode编码；

UUencode在线编码解码

原文本：You had me at hello

编码后：366]U(&AA9"!M92!A="!H96QL;P``

Quoted-printable编码解码

编码解码链接

原理：在邮件处理的各式编码中，很多编码的目的都是使七位字符的邮件协议体系可以传送八位的二进制文件、双字节语言等等。Quoted-Printable也是这样的编码，它的目的是帮助非ASCII编码的信件传输通过SMTP协议。

Quoted-Printable编码是字符对应的编码，每个末编码的二进制字符被编码成三个字符，即一个等号和一个十六进制的数字，如"=AB"

子，如"=AB"。

URL编码

url在线编码解码链接

原理：URL地址（常说网址）规定了常用地数字，字母可以直接使用，另外一批作为特殊用户字符也可以直接用（/,:@等），剩下的其它所有字符必须通过%xx编码处理。

注意：在CTF WEB题目中经常会用到URL编码，比如在url链接的后面补充一些字段以获取数据库中的信息。

原链接：http://www.mzf.com/?login=123

编码后：http%3a%2f%2fwww.mzf.com%2f%3flogin%3d123

Escape/Unescape编码

Escape/Unescape在线编码解码链接

Escape/Unescape加密解码/编码解码,又叫%u编码。Escape编码/加密,就是字符对应UTF-16 ,16进制表示方式前面加%u。Unescape解码/解密，就是去掉"%u"后，将16进制字符还原。

原文本：你好

编码后：%u4f60%u597d

HTML实体编码

HTML在线编码解码链接

HTML ISO-8859-1 参考手册

敲击码

原理：敲击码(Tap code)是一种以非常简单的方式对文本信息进行编码的方法。因该编码对信息通过使用一系列的点击声音来编码而命名，敲击码是基于5×5方格波利比奥斯方阵来实现的，其中，K字母被整合到C中。

敲击码表：

	1	2	3	4	5
1	A	B	C/K	D	E
2	F	G	H	I	J
3	L	M	N	O	P

4 Q R S T U
5 V W X Y Z

源文本	F	O	X
位置	2,1	3,4	5,3
敲击码	.. .	... .	....

md5加密解密

MD5加密解密

密文类型	举例格式	说明
md5	e10adc3949ba59abbe56e057f20f883e 49ba59abbe56e057	标准md5，32位或16位
md5(md5($pass))	b80c9c5f86de74f0090fc1a88b27ef34	第一次加密后，结果转换成小写，对结果再加密一次
md5(md5(md5($pass)))	e57941ff9000aedb44eb2fa13f6e3e3c	第一次加密后，结果转换成小写，对结果再加密一次,结果转换成小写，对结果再加密一次
MD5(MD5($pass))	bb7ff6177ee612ef9dc6acd3a9ea7ea9	第一次加密后，结果转换成大写，对结果再加密一次
MD5(MD5(MD5($pass)))	36d627bd562e83ab995fb1fdf59c95d9	第一次加密后，结果转换成大写，对结果再加密一次,结果转换成大写，对结果再加密一次
sha1	f03e8a370aa8dc80f63a6d67401a692ae72fa530	密文长度必须为40位
md4	c0a27f801162b8b862cd5f5a1a66e85a	32位
mysql	29596332026fd206	老MYSQL数据库用的，16位，且第1位和第7位必须为0-8
mysql5	b34c662f720236babfc1b3f75203a80e1009844a	新版本MySql数据库用的
md5($pass.$salt)	9393dc56f0c683b7bba9b3751d0f6a46:OTD6v4c8l3Zid2AL	在密码后附加一个字符串再加密
md5($salt.$pass)	5610604c157ef1d0fb33911542e5b06f:zg	在密码前附加一个字符串再加密