BugkuCTF—Crypto加密 writeup

原创

Senimo_ 于 2019-08-02 19:53:18 发布 2704 收藏 8

分类专栏： BugCTF writeup 文章标签： Bugku CTF writeup crypto

本文链接：https://blog.csdn.net/weixin_44037296/article/details/98230720

BugkuCTF—Crypto加密 writeup

- 滴答～滴
- 聪明的小羊
- ok
- 这不是摩斯密码
- easy_crypto
- 简单加密
- 散乱的密文
- 凯撒部长的奖励
- 一段Base64
- .!?
- +[]-
- 奇怪的密码
- 托马斯.杰斐逊
- zip伪加密
- 告诉你个秘密（ISCCCTF）
- 这不是md5
- 贝斯家族
- 富强民主
- python（N1CTF）
- 进制转换
- affine
- Crack it
- rsa
- 来自宇宙的信号

BugkuCTF链接

滴答～滴

分值：20

-... -.- -.-. - ...-. – … … -.-.

“答案格式KEY{xxxxxxxxx}”

可以看出是**摩斯电码**，在线莫斯电码解码，添加正确格式即为**flag**：`KEY{bkctfmisc}`

聪明的小羊

分值：20

一只小羊翻过了2个栅栏

“KYsd3js2E{a2jda}”

提示为翻过2个栅栏，栅栏密码在线解密，每组字数为`2`，得到**flag**：KEY{sad23jjdsa2}。

ok

分值：30

Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.

……

Ook. Ook. Ook. Ook. Ook. Ook! Ook? Ook! Ook! Ook. Ook? Ook. Ook. Ook. Ook.

在线ook!解密，选择**Ook! to Text**，得到**flag**：`flag{ok-ctf-1234-admin}`.

这不是摩斯密码

分值：30

下载看看吧

```
+++++ +++++ [->++ +++++ +++<] >++.+ +++++ .<+++ [->-- -<]>- -.+++ +++.<
++++[ ->+++ +<]>+ +++.< +++[- >---< ]>--- .---- .<+++ ++++[ ->--- ----<
]>--- ----- ----- .<+++ ++++[ ->+++ ++++< ]>+++ ++.<+ +++++ +[->- -----
-<]>. <++++ ++++[ ->+++ +++++ <]>++ .<+++ [->-- -<]>- ----. <++++ +++[-
>---- ---<] >---- ----. +++++ +..++ +++.+ .<+++ [->-- -<]>- --.<+ +++++
+[->+ +++++ +<]>+ ++.++ +.+++ +++++ +.--- -.+++ ++.<+ ++[-> +++<] >++++
++.<
```

判断为**Brainfuck**加密，在线Brainfuck解密，选择**Brainfuck to Text**，得到**flag**：`flag{ok-c2tf-3389-admin}`

easy_crypto

分值：30

0010 0100 01 110 1111011 11 11111 010 000 0 001101 1010 111 100 0 001101 01111 000 001101 00 10 1 0 010 0 000 1 01111 10 11110 101011 1111101

简单加密

分值：60

e6Z9i$_{j8R}$U$_{QHE\{RnY\{QXg}}$QnQ{^{XVlRXlp}XI5Q6Q6SKY8jUAA

给出了一段密文，127次非字母内的循环移位，通过**python**脚本解码：

```
cas = 'e6Z9i~]8R~U~QHE{RnY{QXg~QnQ{^XVlRXlp^XI5Q6Q6SKY8jUAA'
for i in range(len(cas)):
    print("{}".format(chr(int(ord(cas[i]) - 4))), end='')
```

得到一段**Base64**编码：`a2V5ezY4NzQzMDAwNjUwMTczMjMwZTRhNThlZTE1M2M2OGU4fQ==`

在线Base64解码得到**flag**：`key{68743000650173230e4a58ee153c68e8}`

散乱的密文

分值：60

lf5{ag024c483549d7fd@@1}

一张纸条上凌乱的写着2 1 6 5 3 4

将给出的密文按顺序列出表：

2	1	6	5	3	4
l	f	5	{	a	g
0	2	4	c	4	8
3	5	4	9	d	7
f	d	@	@	1	}

将密文按顺序排列：

1	2	3	4	5	6
f	l	a	g	{	5
2	0	4	8	c	4
5	3	d	7	9	4
d	f	1	}	@	@

将两个占位符`@@`删除掉，得到**flag**：`flag{52048c453d794df1}`。

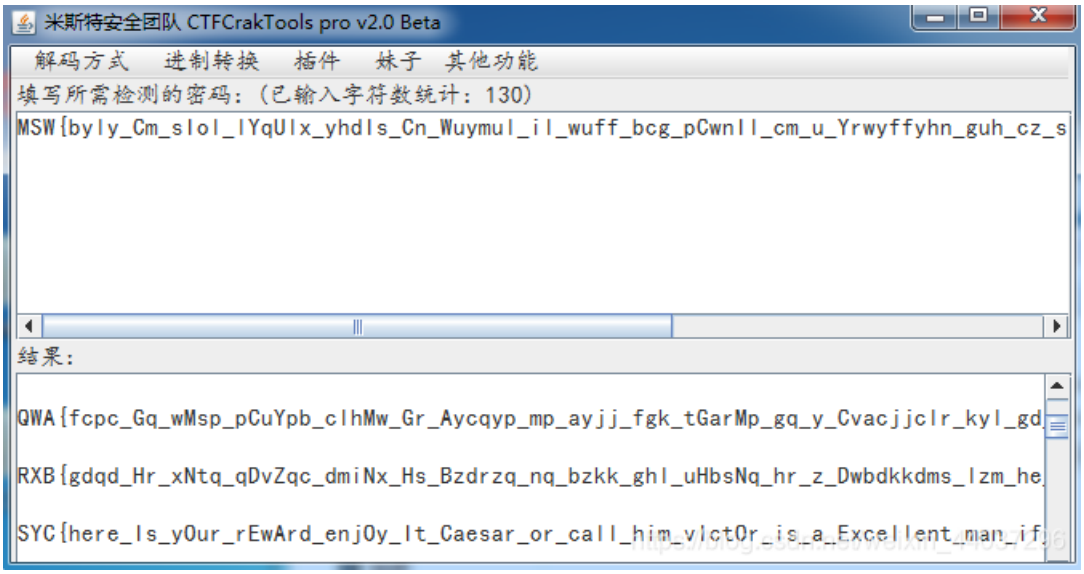
凯撒部长的奖励

分值：60

就在8月，超师傅出色地完成了上级的特遣任务，凯撒部长准备给超师傅一份特殊的奖励，兴高采烈的超师傅却只收到一长串莫名的密文，超师傅看到英语字串便满脸黑线，帮他拿到这份价值不菲的奖励吧。 密文：

MSW{byly_Cm_slol_lYqUlx_yhdls_Cn_Wuymul_il_wuff_bcg_pCwnll_cm_u_Yrwyffyhn_guh_cz_sio_quhn_ni_ayn_bcm_chzilguncihm_sio_wuh_dich_om}

题目来源：第七季极客大挑战



使用**CTFCrakTools pro**，在解码方式选择**凯撒密码>>解码**，找到格式为`SYC{}`的（题目未给出flag格式），即为**flag**：`SYC{here_Is_yOur_rEwArd_enjOy_It_Caesar_or_call_him_vIctOr_is_a_Excellent_man_if_you_want_to_get_his_informations_you_can_join_us}`。

一段Base64

分值：80

flag格式：flag{xxxxxxxxxxxxx}

XDEzNFwxN……w2M1w3MQ==

很长一段的**Base64编码**，使用**Converter**进行**Base64 toText**，获得一段`\134\170\65\143……\170\63\71`，再继续使用**Unescape**，获得一段`\x5c\x75\x30……\x30\x32\x39`，继续使用**Hex to Text**，得到`\u0053\u0074\u0072……\u0035\u0039\u002`再继续使用**Unescape**，获得一段`String.fromCharCode(38,35,……20,51,98,59\u002`，继续使用**Converter**进行**Dec to Text**，获得一段`#x26;#……8&#x3b`，**在线HTML解码**，得到`#x26;#102;……&#68&#x3b`，再进行一次**HTML解码**，得到`flag%7Bctf_tfc201717qwe%7D`，在线URL解码，得到**flag**：`flag{ctf_tfc201717qwe}`

.!?

分值：80

… … … … !!!. ?.. … … … .?.?! .?.. .!..
… … !.?.. … !!!. !!! !!?.? !.?!! !!!.. … … .!.?.
… …!? !!.?. … …?.? !.?.. … .!.?. … … !!!. !!!
!!! !?.?! .?!.? … …! ?!!.? … …?. ?!.?. … !.?.. …
!!!. !!! !!?.? !.?!! !!! !!!. … …!. ?.. …!? !!.?. …
?.?!. ?..!. ?.. … !!!. !!! ??? .?!.? !!! !!! !!!.? …
…!?! !.?.. …? .?!.? …! .!!!. !!! !!! !!! !!.?. … .!!!
.?.. …?. ?!.?. … !.!!! !!! !.?.. … …!?! !.?.. … .?.?!
.?.. … !.?.

使用在线Ook!解密，选择**Ook! to Text**，得到**flag**：`flag{bugku_jiami}`

+[]-

分值：80

++++++ ++++++ [->++ ++++++ +++<] >++.+ ++++++ .<+++ [->-- -<]>- -.+++ +++.<
++++[->+++ +<]>+ +++.< ++++++ [->-- —<] >.<++ ++[-> +++++<]>+++ .<+++
[->-- -<]>- ----. ++++. <+++[->+++ <]>+. <+++++ [->-- --<]> ----- -.<++
+[->+ ++<]> ++.-. ----- —.< +++[- >++++<]>+++ .---- .<+++ [->-- -<]>-
.<+++ +++[- >---- --<]> ----- ----. +.<++ ++++++ +[->+ ++++++ ++<]> ++++++
++++++ .<

使用在线Brainfuck解密，选择**Brainfuck to Text**，得到**flag**：`flag{bugku_jiami_23}`

奇怪的密码

分值：100

突然天上一道雷电

gndk€rlqhmtkwwp}z

字符	g	n	d	k	……
ASCII	103	110	100	107	……
字符	f	l	a	g	……
ASCII	102	108	97	103	……
差值	1	2	3	4	……

通过**Python**脚本实现字符串的转换：

```
lightning = 'gndk€rlqhmtkwwp}z'
result = ''
for i in range(len(lightning)):
    temp = ord(lightning[i])-(i+1)
    result += chr(temp)
print(result)
```

得到基本的**flag**格式：`flag%lei_ci_jiami`，修改为正确格式后提交。

托马斯.杰斐逊

分值：100

1： <ZWAXJGDLUBVIQHKYPNTCRMOSFE <

2： <KPBELNACZDTRXMJQOYHGVSFUWI <

3： <BDMAIZVRNSJUWFHTEQGYXPLOCK <

4： <RPLNDVHGFCUKTEBSXQYIZMJWAO <

5： <IHFRLABEUOTSGJVDKCPMNZQWXY <

6： <AMKGHIWPNYCJBFZDRUSLOQXVET <

7： <GWTHSPYBXIZULVKMRAFDCEONJQ <

8： <NOZUTWDCVRJLXKISEFAPMYGHBQ <

9： <QWATDSRFHENYVUBMCOIKZGJXPL <

10： <WABMCXPLTDSRJQZGOIKFHENYVU <

11： <XPLTDAOIKFZGHENYSRUBMCQWVJ <

12： <TDSWAYXPLVUBOIKZGJRFHENMCQ <

13： <BMCSRFHLTDENQWAOXPYVUIKZGJ <

14： <XPHKZGJTDSENYVUBMLAOIRFCQW <

密钥： 2,5,1,3,6,4,9,7,8,14,10,13,11,12

密文：HCBTSXWCRQGLES

flag格式 flag{你解密的内容}

经过查询发现是**托马斯.杰斐逊转轮加密**，加密由三部分字符串组成，第一部分为**加密表**，第二部分为**密钥**，第三部分为**密文**。

解密方式：先根据**密钥** `2` 给出的数字选出**加密表**中的内容：`2： <KPBELNACZDTRXMJQOYHGVSFUWI <`，将**密文**给出的字符：`H` 后面的内容放到开头，之前的字符串顺序不变接在后面：`2：<HGVSFUWIKPBELNACZDTRXMJQOY <`，以此解密：

2： <HGVSFUWIKPBELNACZDTRXMJQOY <

5： <CPMNZQWXYIHFRLABEUOTSGJVDK <

1： <BVIQHKYPNTCRMOSFEZWAXJGDLU <

3： <TEQGYXPLOCKBDMAIZVRNSJUWFH <

6： <SLOQXVETAMKGHIWPNYCJ**B**FZDRU <

4： <XQYIZMJWAORPLNDVHGFC**U**KTEBS <

9： <WATDSRFHENYVUBMCOIKZ**G**JXPLQ <

7： <CEONJQGWTHSPYBXIZULV**K**MRAFD <

8： <RJLXKISEFAPMYGHBQNOZ**U**TWDCV <

14：<QWXPHKZGJTDSENYVUBMLAOIRFC <

10：<GOIKFHENYVUWABMCXPLTDSRJQZ <

13：<LTDENQWAOXPYVUIKZGJBMCSRFH <

11：<ENYSRUBMCQWVJXPLTDAOIKFZGH <

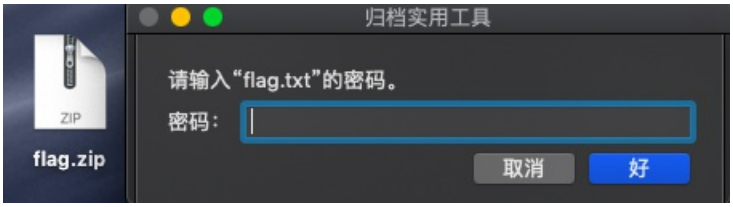
12：<SWAYXPLVUBOIKZGJRFHENMCQTD <

解密后发现倒数第6列有 `BUGKU` 字样，猜测为**flag**内容：`XSXSBUGKUADMIN`，即**flag**为：`flag{xsxsbugkuadmin}`。

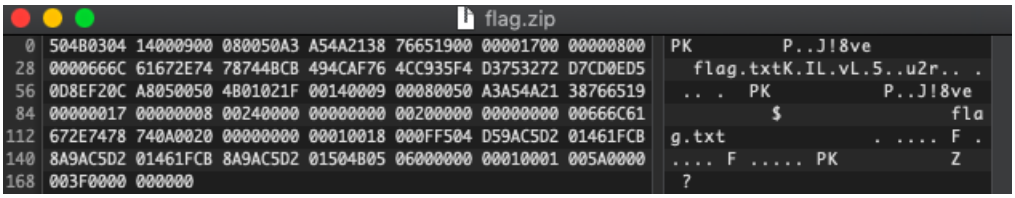
zip伪加密

分值：100

flag.zip



下载**flag.zip**，里面包含文件：`flag.txt`，但需要输入密码解压，根据题目为**zip伪加密**，修改了**zip**文件的全局方式位标记后，打开显示需要密码，实际没有密码。
使用**HEX Fiend**打开`flag.zip`：



将第一行的`140009000`修改为`14000000`，保存重新打开后即可解压得到`flag.txt`，打开即获得**flag**：`flag{Adm1N-B2G-kU-SZIP}`

告诉你个秘密（ISCCCTF）

分值：100

636A56355279427363446C4A49454A7154534230526D6843
56445A31614342354E326C4B4946467A5769426961453067

根据判断为**十六进制**（十六进制数的16个符号：0 1 2 3 4 5 6 7 8 9 A B C D E F），通过**Python**脚本将其转换为**ASCII码**：

```
word = '636A56355279427363446C4A49454A7154534230526D684356445A31614342354E326C4B4946467A5769426961453067'
word = word.lower()
result = ''
for i in range(0, len(word), 2):
    temp = int('0x'+word[i]+word[i+1], 16)
    result += chr(temp)
print(result)
```

得到一串**Base64**编码，在线Base64解码得到`r5yG lp9I BjM tFhBT6uh y7iJ QsZ bhM`通过字符间被包含的字符所构成的字符串即为**flag**：`TONGYUAN`

这不是md5

分值：100

666c61677b6165373335383762613536626166566357d

发现是**十六进制**，在线十六进制转字符，得到**flag**：`flag{ae73587ba56baef5}`

贝斯家族

分值：100

@iH<,{bdR2H;i6*Tm,Wx2izpx2!

Base91在线解码，解码即获得**flag**：`flag{554a5058c9021c76}`

富强民主

分值：100

公正公正公正诚信文明公正民主公正法治法治友善平等和谐敬业和谐富强和谐富强和谐文明和谐平等公正公正和谐法治公正公正公正文明和谐民主和谐敬业和谐平等和谐敬业和谐敬业和谐和谐和谐公正法治友善法治

在线核心价值观解码获得**flag**：`flag{90025f7fb1959936}`。

python（N1CTF）

进制转换

分值：100

二进制、八进制、十进制、十六进制，你能分的清吗？

来源：第七届大学生网络安全技能大赛

text.txt

使用**Python**脚本进行进制之间的转换，具体代码如下：

```
word = 'd87 x65 x6c x63 o157 d109 o145 b100000 d116 b1101111 o40 x6b b1100101 b1101100 o141 d105 x62 d101 b11010
01 d46 o40 d71 x69 d118 x65 x20 b1111001 o157 b1110101 d32 o141 d32 d102 o154 x61 x67 b100000 o141 d115 b100000
b1100001 d32 x67 o151 x66 d116 b101110 b100000 d32 d102 d108 d97 o147 d123 x31 b1100101 b110100 d98 d102 b111000
 d49 b1100001 d54 b110011 x39 o64 o144 o145 d53 x61 b1100010 b1100011 o60 d48 o65 b1100001 x63 b110110 d101 o63
b111001 d97 d51 o70 d55 b1100010 d125 x20 b101110 x20 b1001000 d97 d118 o145 x20 d97 o40 d103 d111 d111 x64 d32
o164 b1101001 x6d o145 x7e'
temp = ''
result = ''
password = ''
for i in range(len(word)):
    temp += word[i]
    if word[i] == ' ':
        temp = '0'+temp
        if '0d' in temp:
            temp = temp[2:]
            result = chr(int(temp))
        if '0x' in temp:
            result = chr(int(temp, 16))
        if '0o' in temp:
            result = chr(int(temp, 8))
        if '0b' in temp:
            result = chr(int(temp, 2))
        temp = ''
        password += result
print(password)
```

运行**Python**脚本得到**flag**：

```
Welcome to kelaibei. Give you a flag as a gift.
flag{1e4bf81a6394de5abc005ac6e39a387b} . Have a good time
```

affine

分值：100

y = 17x-8 flag{szzyfimhyzd}

答案格式：flag{*}

来源：第七届山东省大学生网络安全技能大赛

根据题目**仿射**，推断为仿射密码：

乘法逆元：

1	3	5	7	9	11	15	17	19	21	23	25
1	9	21	15	3	19	7	23	11	5	17	25

解密：**y=ax-8**，根据**乘法逆元**推断`a=23`，通过**Python**脚本，具体代码如下：

```
word = 'szzyfimhyzd'
result = ''
for i in range(len(word)):
    temp = 23 * (ord(word[i]) - ord('a') + 8)
    temp = temp % 26
    result += chr(temp + ord('a'))
print(result)
```

运行脚本得出**flag**内容：`affineshift`

Crack it

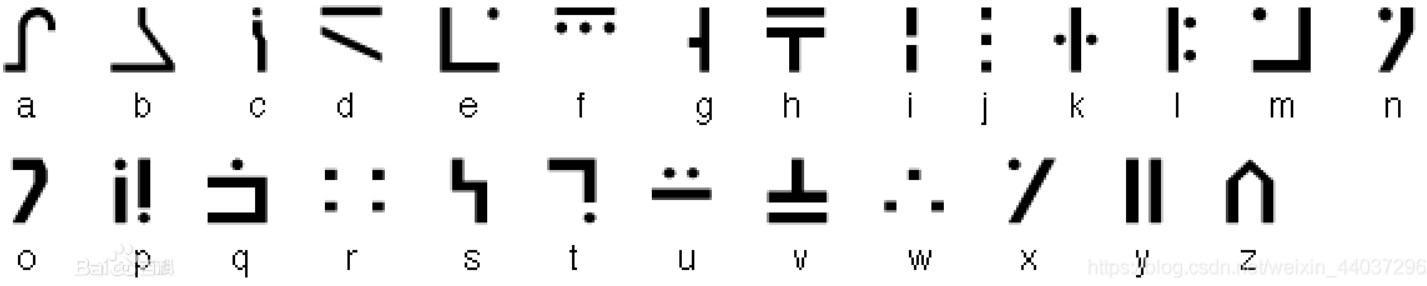
分值：100
破解该文件，获得密码，flag格式为：flag{*}
来源：第七届山东省大学生网络安全技能大赛
root:6HRMJoyGA$26Flgg6CU0bGUOfqFB0Qo9AE2LRZxG8N3H.3BK8t49wGlYbkFbxVFtGOZqVlq3qQ6k0oetDbn2aVzdhuVQ6US.:17770:0:99999:7:::

rsa

来自宇宙的信号

分值：110
银河战队出击
flag格式 flag{字母小写}

给出了7个奇怪的符号，根据题目**来自宇宙的信号**，搜索`银河语言`得到一张`标准银河字母图册`：



通过与图册比对得到**flag**：`flag{nopqrst}`