WriteUp（2020.7.14-2020.7.21）

原创

BIAUTUMN 于 2020-07-22 09:57:13 发布 178 收藏

文章标签： 密码学 信息安全 加密解密

本文链接：https://blog.csdn.net/BIAUTUMN/article/details/107505615

buuctf 刮开有奖

暑假第一道毫无思路的逆向题目

https://www.cnblogs.com/Mayfly-nymph/p/11488817.html#cTrX4ddK

大佬说的非常详细

反编译后两次解密

在运用脚本即可

buuctf findit

apkide打开，

找到一组16进制数组，字符串转换

接着凯撒密码解密

flag{c164675262033b4c49bdf7f9cda28a75}

（这是逆向题？）

buuctf java逆向解密

这个是第二道毫无头绪的题目

https://www.cnblogs.com/Mayfly-nymph/p/12571863.html

jd-gui这个工具第一次使用

buuctf 8086

是16位的dos程序

```
 type: Pure data
       segment para stack 'DATA' use16
       assume cs:dseg
5jzZWz db ']U[du~|t@{z@wj.}.~q@gjz{z@wzqW~/b;',0
       align 10h
       ends

; ---------------------------------------------------------------------------

nt type: Pure code
       segment byte public 'CODE' use16
       assume cs:seg001
       assume es:nothing, ss:nothing, ds:dseg, fs:nothing, gs:nothing

; ========== S U B R O U T I N E =======================================

outes: noreturn

30     proc near               ; CODE XREF: sub_10030↓j
                               ; start+5↓p
       jmp     short sub_10030
30     endp

; ---------------------------------------------------------------------------
       db 0B9h, 22h, 0, 8Dh, 1Eh, 2 dup(0), 8Bh, 0F9h, 4Fh, 80h
       db 31h, 1Fh, 0E2h, 0F8h, 8Dh, 16h, 2 dup(0), 0B4h, 9, 0CDh
       db 21h, 0C3h
       assume ss:dseg, ds:nothing

; ========== S U B R O U T I N E =======================================

outes: noreturn
```


直接IDA：

看到一个字符串，这肯定是flag经过异或了的

下面有一些字节，按C转换成代码：

```
                               ; start+5↓p
       jmp     short sub_10030
       endp

; ---------------------------------------------------------------------------
       mov     cx, 22h ; '"'
       lea     bx, aUDuTZWjQGjzZWz ; "]U[du~|t@{z@wj.}.~q@gjz{z@wzqW~/b;"

                               ; CODE XREF: seg001:000F↓j
       mov     di, cx
       dec     di
       xor     byte ptr [bx+di], 1Fh
       loop    loc_10039
       lea     dx, aUDuTZWjQGjzZWz ; "]U[du~|t@{z@wj.}.~q@gjz{z@wzqW~/b;"
       mov     ah, 9
       int     21h             ; DOS - PRINT STRING
                               ; DS:DX -> string terminated by "$"
       retn
       assume ss:dseg, ds:nothing

; ========== S U B R O U T I N E =======================================
```


就是逐字节异或1F，即可得到flag：

```
In [1]: a = ']U[du~|t@{z@wj.}.~q@gjz{z@wzqW~/b;'

In [2]: b=''

In [3]: for i in a:
   ...:     b+=chr(ord(i)^0x1f)
   ...:

In [4]: print b
BJD{jack_de_hu1b1an_xuede_henHa0}$

In [5]:
```

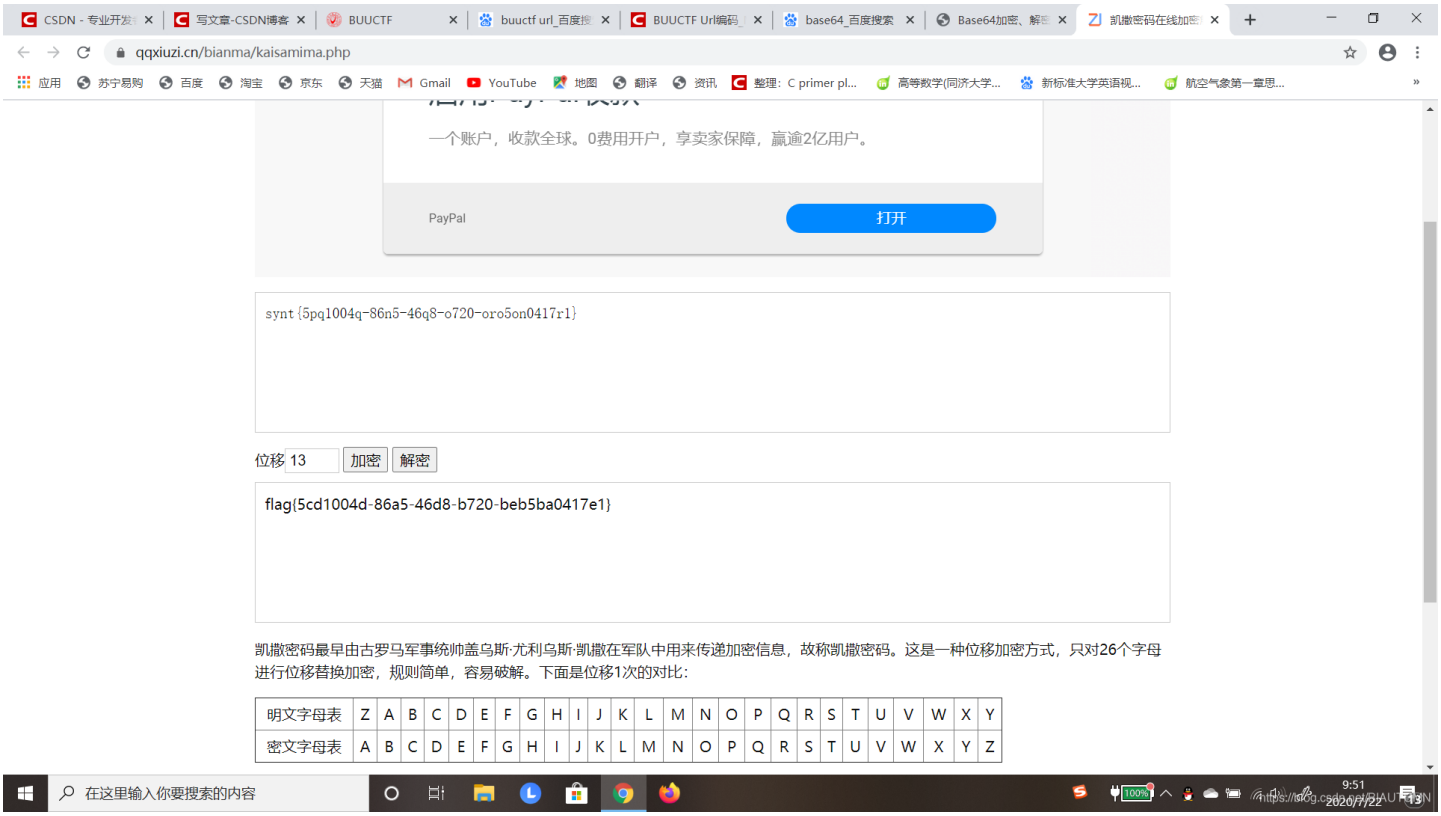

（似乎在哪里见过类似的题目，也是对数组进行异或）

最近逆向刷的有些上头，刷几道密码和杂项换换胃口

buuctf url编码

得到数据后直接解密即可

buuctf 看我回旋踢



很明显拿到密文无论是从密文结构还是题目暗示（回旋）

都可以看出是凯撒密码

解密即可

buuctf 一眼就解密

看到一个等号就知道是base64

确实一眼就解密

[创作打卡挑战赛](#)

[赢取流量/现金/CSDN周边激励大奖](#)