Crypto

ECC

用 Sage 再做个逆运算再 n2s 就完事了。数据太大，不能直接复制粘贴，耗费了点时间。

```
p =
749970215594340659752724316266187207258384730917219366165603590006486518915 07
a =
617390437303328599782364690079486669975105442123623866290620320949253535196 57
b =
878217828184778176098825263164797214909198150136680967719923600024676578273 19
k =
936538742721761075844599820585270816040838711827978162047726445096232710612 31
E = EllipticCurve(GF(p), [a, b])
c1x =
144556136662118995760188351651324381020119882646071465119382497448719649460 84
c1y =
255065825705812897146126404932582998138031575617962473306937681467630357919 42
c2x =
375548711626194567091835091226739296364576222518801992350547345237824838699 31
c2y =
713920555406167365392679609893042870836292885303984745907823663848738144778 06
c1 = E([c1x,c1y])
c2 = E([c2x,c2y])
cipher_left =
682080624021626160092170390343311427862826781076502287617095844787799987347 10
cipher_right =
274539885450023845467069335904325850062404394433125710087918352036601528906 19

m = c1 - k * c2

flag_left = cipher_left / m[0]
flag_right = cipher_right / m[1]
print(flag_left)
print(flag_right)
```

Misc

摆烂

在 WinHex 里查看下载得到的压缩包，发现是一个png~~【并不】~~和一个压缩包，使用复制粘贴大法分离开。png 其实是一个 apng ~~surprise~~ ，找了个能分离 apng 的软件把两张图分离开。分开之后，是盲水印，借助 github 上的 BWM 解开，得到了压缩包密码。 解压缩之后得到了二维码碎片，按照定位点和白边拼好~~【不要旋转】~~，扫描二维码，得到了一段话，话里面有零宽字符，在 github 上有一个解密的项目~~【说实话真难找，好找的项目的用不了】~~，揭秘之后就得到了 flag 。