BUUCTF Crypto部分题总结

原创

qiushuo29 于 2021-08-10 20:26:58 发布 141 收藏
分类专栏： CTF密码学

1.Quoted-printable

首先看到题目所给的密码并非常见的密码，搜索一下题目Quoted-printable，查看一下相关信息

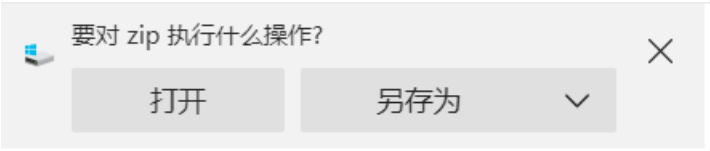
quoted-printable 就是说用一些可**打印常用字符**，表示一个字节（8位）中所有非打印字符方法！. Quoted-printable编码方法. 任何一个8位的字节值可编码为3个字符：一个等号”=”后跟随两个十六进制数字 (0–9或A–F)表示该字节的数值.例如，ASCII码换页符（十进制值为12）可以表示为”=0C”，等号”=”（十进制值为61）必须表示为”=3D”. 除了可打印ASCII字符与换行符以外，所有字符必须表示为这种格式.

了解了相关信息后，搜索相关工具

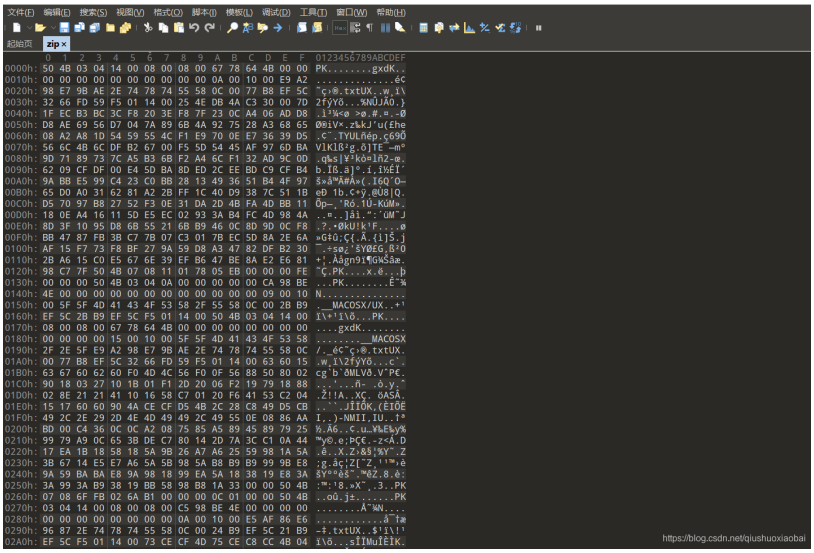
解码后发现flag“那你也很棒哦”

小结：遇到英文字母和数字两两混合且用“=”连接，要想起Quoted-printable编码。

2.大帝的密码武器

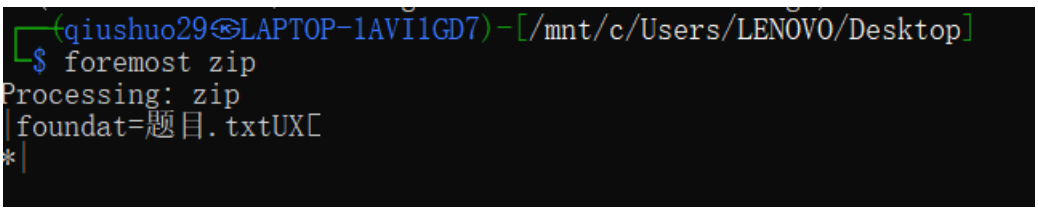


下载题目，得到zip文件无法打开，使用010editor

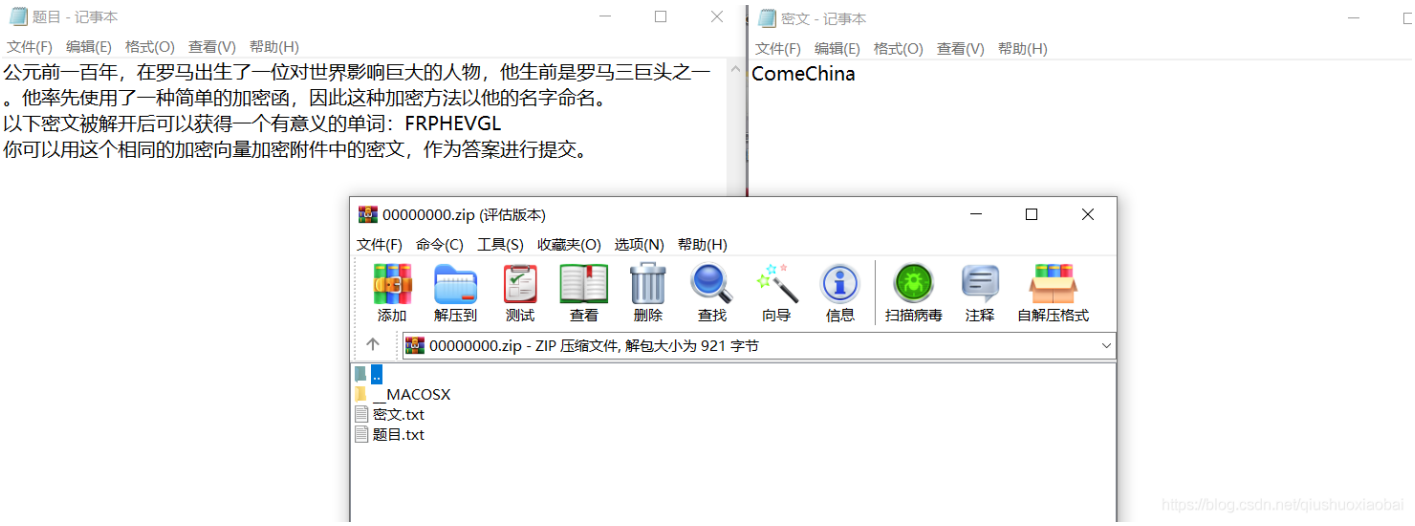


查看文件头为 50 4B 为zip文件的文件头，无法得到压缩包

尝试使用kali Linux的foremost功能分离文件



可分离出 题目.txt 在output文件夹中



得到flag：ComeChina

小结：根据提示的zip文件，无法得到更多的题目信息，可以尝试使用foremost分离，得到更多信息。

3.信息化时代的步伐

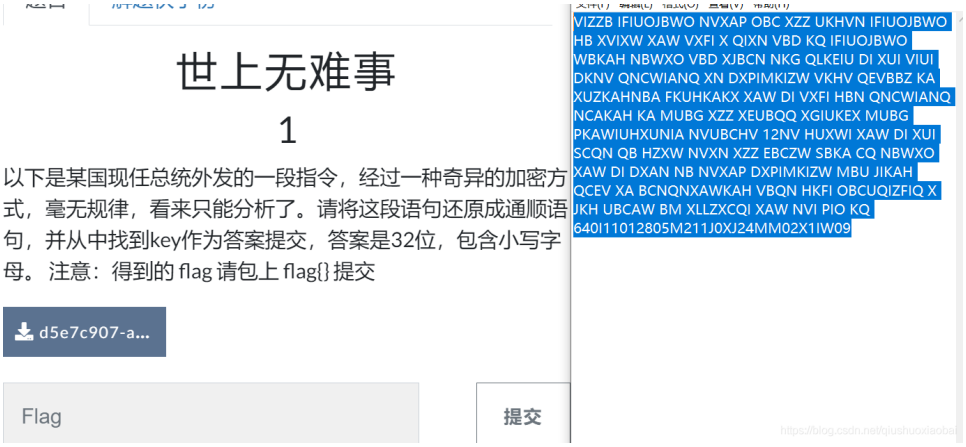
题目中提示答案为 一串中文，所给的密码是一串数字，着手数字转化为中文，此时作者第一时间想到的是九键输入，观察其中多有0，00等应无法得出较好的中文的信息，转换思路

附件是清政府拒绝的数十年后，年代较早，想起了中文电码一说，查找中文电码工具，

使用工具转化后，得到flag：计算机要从娃娃抓起

小结：中文与数字间的转换，要记得中文电码。

4.世上无难事



观察密码发现，此密码不同于base密码，观察其中英文字母间有间隔，像是用凯撒加密过的英文语段，使用凯撒(Caesar)加密/解密 - Bugku CTF工具枚举后

并未发现结果，尝试使用quipqiup工具爆破quipqiup - cryptoquip and cryptogram solver

将密文输入

```
0   -1.534  HELLO EVERYBODY THANK YOU ALL RIGHT EVERYBODY GO AHEAD AND HAVE A SEAT HOW IS EVERYBODY DOING TODAY HOW ABOUT TIM SPICER WE ARE HERE WITH STUDENTS AT WAKEFIELD HIGH
            SCHOOL IN ARLINGTON VIRGINIA AND WE HAVE GOT STUDENTS TUNING IN FROM ALL ACROSS AMERICA FROM KINDERGARTEN THROUGH 12TH GRADE AND WE ARE JUST SO GLAD THAT ALL COULD
            JOIN US TODAY AND WE WANT TO THANK WAKEFIELD FOR BEING SUCH AN OUTSTANDING HOST GIVE YOURSELVES A BIG ROUND OF APPLAUSE AND THE KEY IS
            640E11012805F211B0AB24FF02A1ED09

1   -4.126  MILLO ITIKYBODY EMANC YOR ALL KUGME ITIKYBODY GO AMIAD AND MATI A SIAE MOP US ITIKYBODY DOUNG EODAY MOP ABORE EUV SZUWIK PI AKI MIKI PUEM SERDINES AE PACIJUILD MUGM
            SWMOOL UN AKLUNGEON TUKGUNUA AND PI MATI GOE SERDINES ERNUNG UN JKOV ALL AWKOSS AVIKUWA JKOV CUNDIKGAKEIN EMKORGM 12EM GKADI AND PI AKI FRSE SO GLAD EMAE ALL WORLD
            FOUN RS EODAY AND PI PANE EO EMANC PACIJUILD JOK BIUNG SRWM AN ORESEANDUNG MOSE GUTI YORKSILTIS A BUG KORND OJ AZZLARSI AND EMI CIY US
            640I11012805J211B0AB24JJ02A1ID09

2   -4.157  HILLO IMITERODE SHANX EOW ALL TUGHS IMITERODE GO AHIAD AND HAMI A KIAS HOP UK IMITERODE DOUNG SODAE HOP AROWS SUV KYUCIT PI ATI HITI PUSH KSWDINSK AS PAXIFUILD HUGH
            KCHOOL UN ATLUNGSON MUTGUNUA AND PI HAMI GOS KSWDINSK SWNUNG UN FTOV ALL ACTOKK AVITUCA FTOV XUNDITGATSIN SHTOWGH 12SH GTADI AND PI ATI BWKS KO GLAD SHAS ALL COWLD
            BOUN WK SODAE AND PI PANS SO SHANX PAXIFUILD FOT RIUNG KWCH AN OWSKSANDUNG HOKS GUMI EOWTKILMIK A RUG TOWND OF AYYLAWKI AND SHI XIE UK
            640I11012805F211R0AR24FF02A1ID09

3   -4.162  MOLLU OKORYBUDY EMANC YUX ALL RIGME OKORYBUDY GU AMOAD AND MAKO A SOAE MUT IS OKORYBUDY DUING EUDAY MUT ABUXE EIZ SFIHOR TO ARO MORO TIEM SEXDONES AE TACOPIOLD MIGM
            SHMUUL IN ARLINGEUN KIRGINIA AND TO MAKO GUE SEXDONES EXNING IN PRUZ ALL AHRUSS AZORIHA PRUZ CINDORGAREON EMRUXGM 12EM GRADO AND TO ARO QXSE SU GLAD EMAE ALL HUXLD
            QUIN XS EUDAY AND TO TANE EU EMANC TACOPIOLD PUR BOING SXHM AN UXESEANDING MUSE GIKO YUXRSOLKOS A BIG RUXND UP AFFLAXSO AND EMO COY IS
            640O11012805P211B0AB24PP02A1OD09

4   -4.178  HECCA EVERYZAKY THING YAP ICC ROSHT EVERYZAKY SA IHEIK INK HIVE I LEIT HAD OL EVERYZAKY KAONS TAKIY HAD IZAPT TOM LJOUER DE IRE HERE DOTH LTPKENTL IT DIGEBOECK HOSH
            LUHAAC ON IRCONSTAN VORSONOI INK DE HIVE SAT LTPKENTL TPNONS ON BRAM ICC IURALL IMEROUI BRAM GONKERSIRTEN THRAPSH 12TH SRIKE INK DE IRE WPLT LA SCIK THIT ICC UAPCK
            WAON PL TAKIY INK DE DINT TA THING DIGEBOECK BAR ZEONS LPUH IN APTLTINKONS HALT SOVE YAPRLECVEL I ZOS RAPNK AB IJJCIPLE INK THE GEY OL
            640E11012805B211Z0IZ24BB02I1EK09
```


得到文段，THE KEY IS 640E11012805F211B0AB24FF02A1ED09

即可得到flag

小结：对特殊加密的英文语段，可以使用quipqiup工具进行爆破，观察是否可以得出结果。