

分类 RE 下的题目

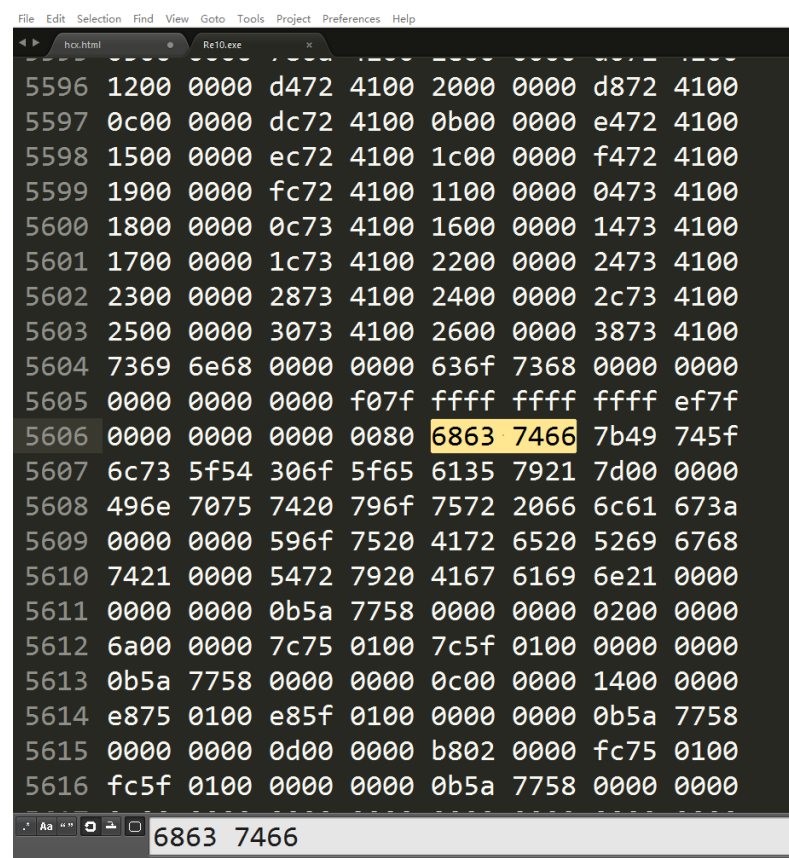
你看看，逆向多简单！ **POINT: 10**

题目 ID: 28

题目描述: 链接: <http://pan.baidu.com/s/1kVrzylx> 密码: bxmb

Hint: 这还要啥 Hint

打开链接，下载得一 exe 文件，尝试用 Sublime 打开，得到一堆 4 位一组 16 进制数据。尝试查找 hctf 的 ASCII 码



```
File Edit Selection Find View Goto Tools Project Preferences Help
hctf.html Re10.exe
5596 1200 0000 d472 4100 2000 0000 d872 4100
5597 0c00 0000 dc72 4100 0b00 0000 e472 4100
5598 1500 0000 ec72 4100 1c00 0000 f472 4100
5599 1900 0000 fc72 4100 1100 0000 0473 4100
5600 1800 0000 0c73 4100 1600 0000 1473 4100
5601 1700 0000 1c73 4100 2200 0000 2473 4100
5602 2300 0000 2873 4100 2400 0000 2c73 4100
5603 2500 0000 3073 4100 2600 0000 3873 4100
5604 7369 6e68 0000 0000 636f 7368 0000 0000
5605 0000 0000 0000 f07f ffff ffff ffff ef7f
5606 0000 0000 0000 0080 6863 7466 7b49 745f
5607 6c73 5f54 306f 5f65 6135 7921 7d00 0000
5608 496e 7075 7420 796f 7572 2066 6c61 673a
5609 0000 0000 596f 7520 4172 6520 5269 6768
5610 7421 0000 5472 7920 4167 6169 6e21 0000
5611 0000 0000 0b5a 7758 0000 0000 0200 0000
5612 6a00 0000 7c75 0100 7c5f 0100 0000 0000
5613 0b5a 7758 0000 0000 0c00 0000 1400 0000
5614 e875 0100 e85f 0100 0000 0000 0b5a 7758
5615 0000 0000 0d00 0000 b802 0000 fc75 0100
5616 fc5f 0100 0000 0000 0b5a 7758 0000 0000
Aa " 6863 7466
```

又知 “{”、“}”ASCII 码为 7b、7d，则中间即为 flag

分类 CRYPTO 下的题目

密码学教室入门（二）

题目 ID: 19

题目描述: 凯撒加密是一种古老的对称加密算法

学习文档: https://en.wikipedia.org/wiki/Caesar_cipher

mlfrj{Hfjxfw_hnumjw_8x_ozxy_ktw_kzs}

Hint: 这都不会可以退出密码学了

移位密码，根据开头 5 位可知是 hgame（虽然后来也说了），然后得 hgame{Caesar_cipher_8s_just_for_fun}，对于数字符号处理，查找了许久也没弄出来，然后疯狂试 flag，试出数字为 1，则得 hgame{Caesar_cipher_1s_just_for_fun}

题目 ID: 20

题目描述：维吉尼亚密码是最常见的分组密码。将明文对应的书名中的空格换成下划线，在并且加上 hgame{}后作为 flag

https://en.wikipedia.org/wiki/Vigenère_cipher

ET. PESFVWI, AJGZII BU D LISQ ISW IKV MRQTLWTOOHRY JP WLJ CCVXNMNH, XJTVLJNFU RR
IBTQED'T DHLFMH DX MJU WVNBN. GEWOCB MX SGOIFTGG, SSMA WS GF CUVJTVHH FHCLR
QBVHV YICW HFZ. C QIB UTLEQ CGJMST QQ XMF HRPQPYLRL ECB, YSEGU RJX KEWHGV
FWPWJLY CA WLJ EGEWHGV ESE C WLNSF LRIJXLHZN ZLT JU VSTO THZJBNHH FT FU. QFOGWXJ.
IG KEI XTLXYFP DR FDERYSU QI LNT KPTWJURRRFPW EY UJH LFOFV SK ECURFZ'U IEYIGU ESE
JLHIFP LX NO JLW HFNO; HJGCUKJ GQXRI JV ZLNMG VIFSEKMSH VKI HFNO HZSKQK YIG VXTSOLRL
PH WLJ CCVXNMNH.

Hint: 确认维吉尼亚分组长度，然后做字频分析，over...标点和空格不计入分组长度当中

先是写了个小程序，从 2 组开始到 5 组，做字频分析，长时间未果，后得知字符空格也要算，重做改后题目，仍未果_(: 3 」 ∠)_ 尝试从符号入手，‘T’, ‘U’ 应为 ‘S’, ‘S’，然后在此网站上疯狂试 flag (<http://planetcalc.com/2468/>)，终得一段，扔进百度得 A Tale of Two Cities 即为 hgame{ A Tale of Two Cities }

Intel Artificial Intelligence

AI is the Next Big Wave in Computing. See How Intel is Preparing for the Future. Go to intel.com

Vigenère cipher

Alphabet: English

Tabula recta starts with:
☒ ROT0 ("a" transforms to "a")
☐ ROT1 ("a" transforms to "b")

Text:

ECURFZ'U IEYIGU ESE JLHIFP LX NO
JLW HFNO; HJGCUKJ GQXRI JV
ZLNMG VIFSEKMSH VKI HFNO
HZSKQK YIG VXTSOLRL PH WLJ
CCVXNMNH.

Key: BCDEF

Transformation:
☐ Encrypt
☒ Decrypt

PLANETCALC

Calculate

Transformed text:
dr. manette, viewed as a hero for his imprisonment in the bastille, testifies on darnay's behalf at his trial. darnay is released, only to be arrested again later that day. a new trial begins on the following day, under new charges brought by the defarges and a third individual who is soon revealed as dr. manette. he had written an account of his imprisonment at the hands of darnay's father and hidden it in his cell; defarge found it while searching the cell during the storming of the bastille.

其它好些题目查了半天，试了半天未果，还是 too young,好想有大佬带_(: 3 」 ∠)_