安恒杯月赛之以赛战“疫”-- writeup解题思路

原创

Blus.King 于 2020-02-27 10:22:52 发布
文章标签： CTF 安恒月赛 以赛战疫 writeup

CRYPTO-古典密码1

iodj{36g9i2777

符号不变进行凯撒移位

flag{36d9f2777

-... ----. ..--- -... .- -.-. ...-- ----. .- .- ..---

摩斯解码

b92bac39aa2

a0dd}b6942c07

栅栏密码https://www.qqxiuzi.cn/bianma/zhalanmima.php

发现其他解法都不对，非得用这个网站解才对，奇怪:ab206cd90d47}

原因是4:3:3分割，然后竖着念

a0dd}

b694

2c07

最终得到

flag{36d9f2777b92bac39aa2ab206cd90d47}

简单的zip隐写

先解压，发现没有什么东西，于是用十六进制编辑器打开文件，发现遗传可疑的十六进制流。将其提取出来，单独保存成一个文件。发现是个ZIP压缩包。

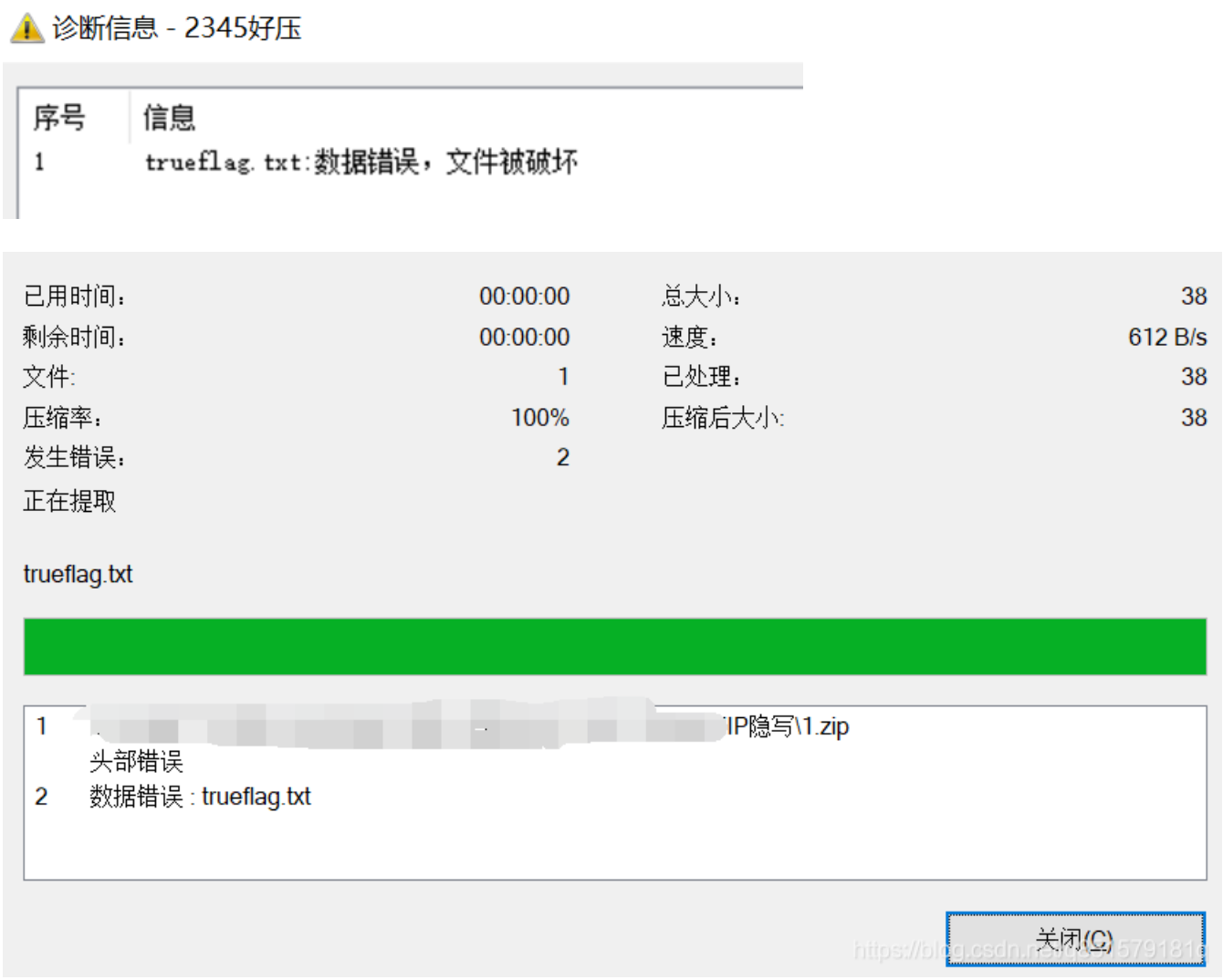
2002245e53422a799f3.rar 无标题1

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000240  82 E3 80 80 E3 80 80 20 E3 83 8E 20 E3 80 80 E3  ‚ã€€ã€€ ãƒŽ ã€€ã
00000250  80 80 E3 80 80 E3 83 BB E3 82 9C 2B 2E 0D 0A E3  €€ã€€ãƒ»ã‚œ+...ã
00000260  80 80 E3 81 97 E3 83 BC EF BC AA E3 80 80 E3 80  €€ã.—ãƒ¼ï¼ªã€€ã€
00000270  80 E3 80 80 C2 B0 E3 80 82 2B 20 2A C2 B4 C2 A8  €ã€€Â°ã€‚+ *Â´Â¨
00000280  29 0D 0A E3 80 80 E3 80 80 E3 80 80 20 20 20 20  )..ã€€ã€€ã€€
00000290  20 20 20 E3 80 80 E3 80 80 2E C2 B7 20 C2 B4 C2     ã€€ã€€.Â· Â´Â
000002A0  B8 2E C2 B7 2A C2 B4 C2 A8 29 20 C2 B8 2E C2 B7  ¸.Â·*Â´Â¨) Â¸.Â·
000002B0  2A C2 A8 29 0D 0A E3 80 80 E3 80 80 E3 80 80 E3  *Â¨)..ã€€ã€€ã€€ã
000002C0  80 80 E3 80 80 E3 80 80 E3 80 80 20 20 20 20 20  €€ã€€ã€€ã€€
000002D0  E3 80 80 28 C2 B8 2E C2 B7 C2 B4 20 28 C2 B8 2E  ã€€(Â¸.Â·Â´ (Â¸.
000002E0  C2 B7 E2 80 99 2A 0D 0A 0D 0A 0D 0A 35 30 34 42  Â·â€™*......504B
000002F0  30 33 30 34 31 34 30 30 30 30 30 30 30 31 30 30  0304140000000100
00000300  36 34 39 37 33 38 34 46 34 31 45 35 36 35 39 38  6497384F41E56598
00000310  32 36 30 30 30 30 30 30 32 36 30 30 30 30 30 30  2600000026000000
00000320  30 43 30 30 30 30 30 30 37 34 37 32 37 35 36 35  0C000000074727565
00000330  36 36 36 43 36 31 36 37 32 45 37 34 37 38 37 34  666C61672E747874
00000340  34 42 43 42 34 39 34 43 41 46 34 45 33 36 33 37  4BCB494CAF4E3637
00000350  34 44 34 43 33 33 33 31 33 32 33 35 34 43 33 35  4D4C333132354C35
00000360  34 38 34 43 34 42 34 39 33 35 34 41 34 42 33 36  484C4B49354A4B36
00000370  33 33 30 32 33 32 43 44 43 44 35 32 32 43 34 43  330232CDCD522C4C
00000380  43 44 43 43 43 44 34 44 36 41 30 31 35 30 34 42  CDCCCD4D6A01504B
00000390  30 31 30 32 31 46 30 30 31 34 30 30 30 30 30 30  01021F0014000000
000003A0  30 38 30 30 36 34 39 37 33 38 34 46 34 31 45 35  08006497384F41E5
000003B0  36 35 39 38 32 36 30 30 30 30 30 30 32 36 30 30  6598260000002600
000003C0  30 30 30 30 30 43 30 30 32 34 30 30 30 30 30 30  00000C0024000000
000003D0  30 30 30 30 30 30 30 30 32 30 30 30 30 30 30 30  0000000020000000
000003E0  30 30 30 30 30 30 30 30 37 34 37 32 37 35 36 35  0000000074727565
000003F0  36 36 36 43 36 31 36 37 32 45 37 34 37 38 37 34  666C61672E747874
00000400  30 41 30 30 32 30 30 30 30 30 30 30 30 30 30 30  0A00200000000000
00000410  30 31 30 30 31 38 30 30 41 34 41 42 39 34 31 37  01001800A4AB9417
00000420  43 37 37 32 44 35 30 31 41 34 41 42 39 34 31 37  C772D501A4AB9417
00000430  43 37 37 32 44 35 30 31 46 30 41 38 45 43 46 32  C772D501F0A8ECF2
00000440  43 36 37 32 44 35 30 31 35 30 34 42 30 35 30 36  C672D501504B0506
00000450  30 30 30 30 30 30 30 30 30 31 30 30 30 31 30 30  0000000001000100
00000460  35 45 30 30 30 30 30 30 35 30 30 30 30 30 30 30  5E00000050000000
00000470  30 30 30 30 00 F1 9C 5C EB 29 02 03 0B 90 00 04  0000.ñœ\ë).....
00000480  90 00 20 07 80 4F 77 80 00 00 0D 77 72 6F 6E 67  .. .€Ow€...wrong
00000490  66 6C 61 67 2E 74 78 74 0A 03 02 B2 40 BF E2 C6  flag.txt...²@¿âÆ
000004A0  72 D5 01 66 6C 61 67 E5 9C A8 E5 93 AA E9 87 8C  rÕ.flagåœ¨å“ªé‡Œ
000004B0  EF BC 9F 1D 77 56 51 03 05 04 00                 ï¼Ÿ.wVQ....
```


2002245e53422a799f3.rar 无标题1

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000  50 4B 03 04 14 00 00 00 01 00 64 97 38 4F 41 E5  PK........d—8OAå
00000010  65 98 26 00 00 00 26 00 00 00 0C 00 00 00 74 72  e˜&...&.......tr
00000020  75 65 66 6C 61 67 2E 74 78 74 4B CB 49 4C AF 4E  ueflag.txtKËIL¯N
00000030  36 37 4D 4C 33 31 32 35 4C 35 48 4C 4B 49 35 4A  67ML3125L5HLKI5J
00000040  4B 36 33 02 32 CD CD 52 2C 4C CD CC CD 4D 6A 01  K63.2ÍÍR,LÍÌÍMj.
00000050  50 4B 01 02 1F 00 14 00 00 00 08 00 64 97 38 4F  PK..........d—8O
00000060  41 E5 65 98 26 00 00 00 26 00 00 00 0C 00 24 00  Aåe˜&...&.....$.
00000070  00 00 00 00 00 00 20 00 00 00 00 00 00 00 74 72  ...... .......tr
00000080  75 65 66 6C 61 67 2E 74 78 74 0A 00 20 00 00 00  ueflag.txt.. ...
00000090  00 00 01 00 18 00 A4 AB 94 17 C7 72 D5 01 A4 AB  ......¤«”.ÇrÕ.¤«
000000A0  94 17 C7 72 D5 01 F0 A8 EC F2 C6 72 D5 01 50 4B  ”.ÇrÕ.ð¨ìòÆrÕ.PK
000000B0  05 06 00 00 00 00 01 00 01 00 5E 00 00 00 50 00  ..........^...P.
000000C0  00 00 00 00                                      ....
```

尝试对zip进行解压，发现格式错误。



找到zip的格式说明，同时自己找一个正常的zip做对比

压缩源文件数据区

50 4B 03 04：这是头文件标记（0x04034b50）

14 00：解压文件所需 pkware 版本

00 00：全局方式位标记（有无加密）

08 00：压缩方式

5A 7E：最后修改文件时间

F7 46：最后修改文件日期


```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000   50 4B 03 04 14 00 00 00 01 00 64 97 38 4F 41 E5  PK........d—8OAå
00000010   65 98 26 00 00 00 26 00 00 00 0C 00 00 00 74 72  e˜&...&.......tr
00000020   75 65 66 6C 61 67 2E 74 78 74 4B CB 49 4C AF 4E  ueflag.txtKËIL¯N
00000030   36 37 4D 4C 33 31 32 35 4C 35 48 4C 4B 49 35 4A  67ML3125L5HLKI5J
00000040   4B 36 33 02 32 CD CD 52 2C 4C CD CC CD 4D 6A 01  K63.2ÍÍR,LÍÌÍMj.
00000050   50 4B 01 02 1F 00 14 00 00 00 08 00 64 97 38 4F  PK..........d—8O
00000060   41 E5 65 98 26 00 00 00 26 00 00 00 0C 00 24 00  Aåe˜&...&.....$.
00000070   00 00 00 00 00 00 20 00 00 00 00 00 00 00 74 72  ...... .......tr
00000080   75 65 66 6C 61 67 2E 74 78 74 0A 00 20 00 00 00  ueflag.txt.. ...
00000090   00 00 01 00 18 00 A4 AB 94 17 C7 72 D5 01 A4 AB  ......¤«”.ÇrÕ.¤«
000000A0   94 17 C7 72 D5 01 F0 A8 EC F2 C6 72 D5 01 50 4B  ”.ÇrÕ.ð¨ìòÆrÕ.PK
000000B0   05 06 00 00 00 00 01 00 01 00 5E 00 00 00 50 00  ..........^...P.
000000C0   00 00 00 00                                      ....
```


将压缩标志位改为正常的08,即可解压得到flag

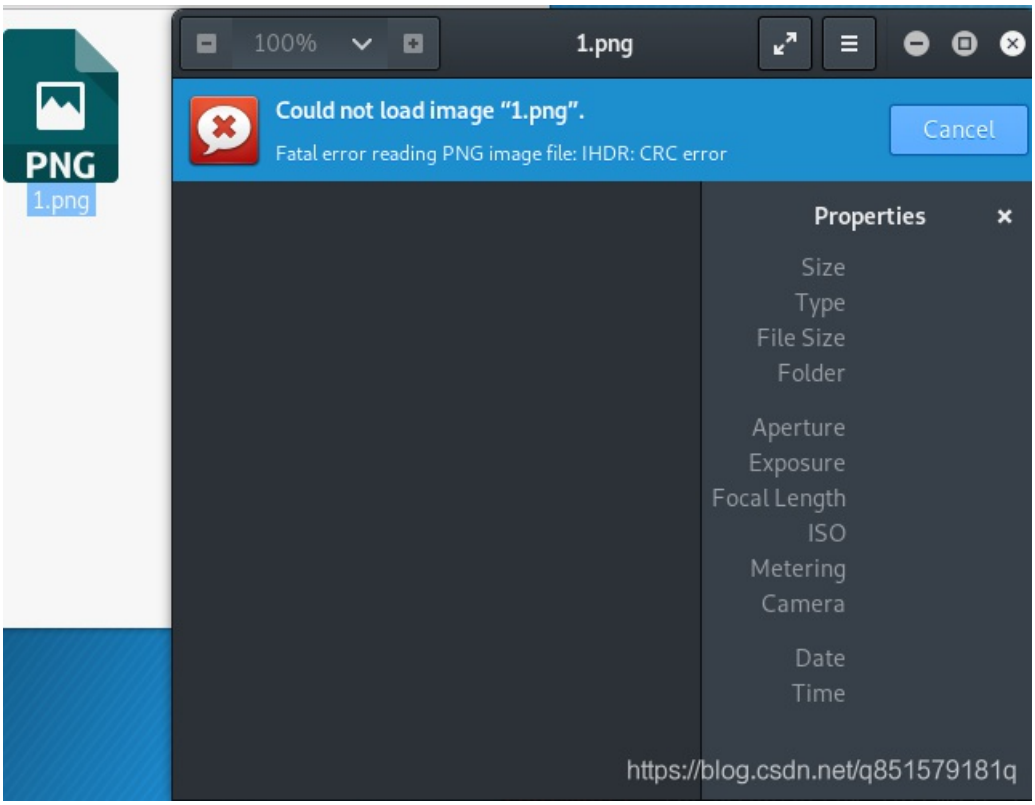
简单的RSA1

加密过程中使用相同的n，不同的e对同一组明文数据进行加密，很显然是 **共模攻击。**

编写简洁脚本，7行代码解决问题

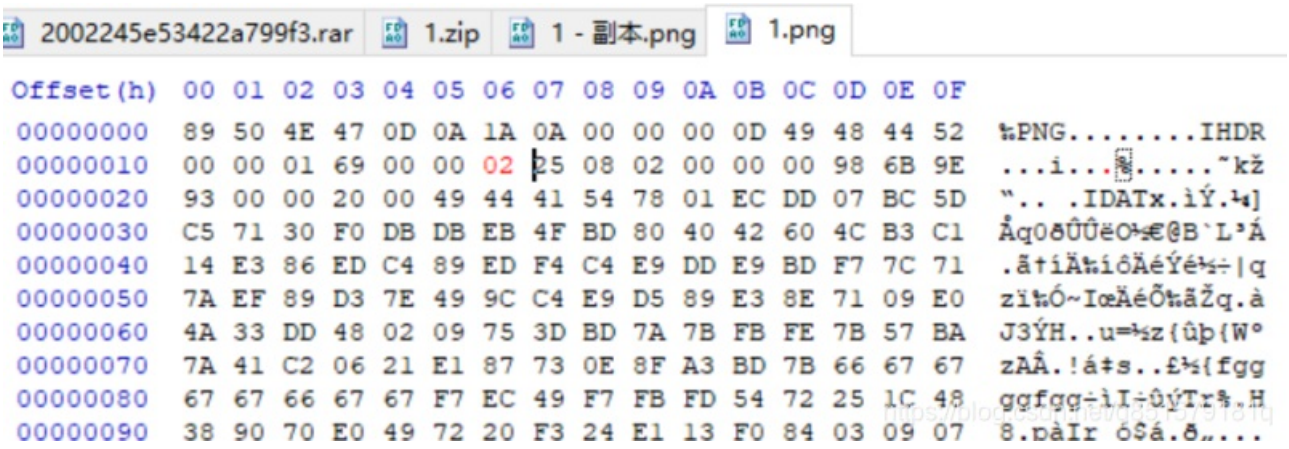
```
import gmpy2

e1 = 65537

e2 = 11187289

n=21550279102644053137401794357450944302610731390301294678793250727396089358072700658571

c1=33984983819123958191909724891724628656199784124264610066378531323944213585544440855509

c2=34667339213058046381059472027611637474726186024459952452537713845532165694740052117746

s0, s1, s2 = gmpy2.gcdext(e1, e2)

m = pow(c1, s1, n)*pow(c2, s2, n) % n

print hex(m)[2:].decode("hex")
```

柠檬精- lemonEssence



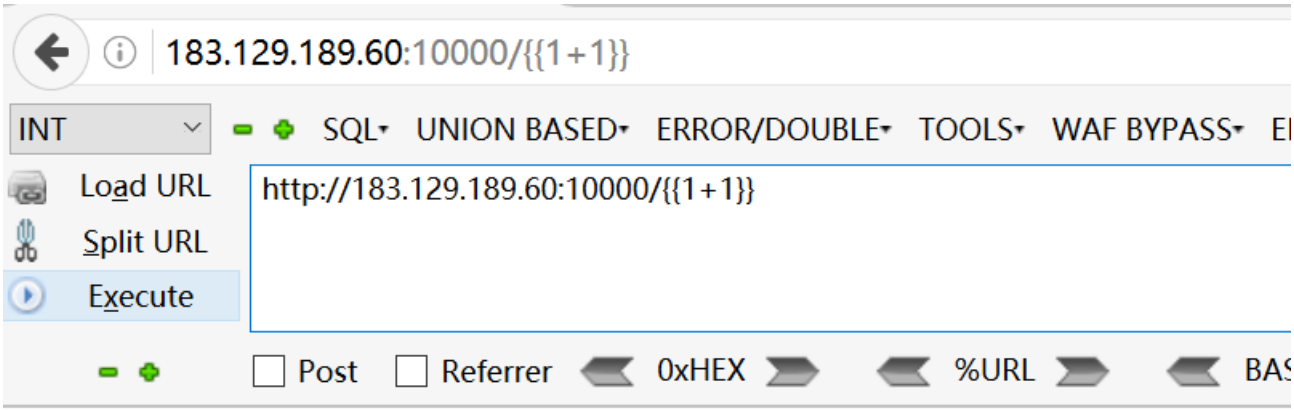
kali下打开报错，说明做了高度隐写，致使其CRC循环校验失败

修改高度，看看隐藏了什么



easyflask1

显然是模板注入



Oops! That page doesn't exist.

/2

之后测试发现有过滤.....

然后就没有然后了.....

easy-py

pyc反编译-https://tool.lu/pyc/还原

我的 所有 开发类 站长类 极客类

请选择pyc文件进行解密。支持所有Python版本

选择文件 未选择任何文件

```python
import base64
import string

def caser(flag):
    enc1 = ''
    for i in flag:
        enc1 += chr(ord(i) - 5)

    return enc1


def rail(flag):
    p1 = ''
    p2 = ''
    p3 = ''
    enc2 = ''
    for i in range(len(flag)):
        j = i % 3
        if j == 0:
            p1 += flag[i]
            continue
        if j == 1:
```

美化(Beautify) 下载(Download)

然后就没有然后了.....