i春秋第二届春秋欢乐赛 over the hill writeup

原创

bingge15 于 2019-10-06 21:36:41 发布 569 收藏

分类专栏： CTF 文章标签： CTF hill

本文链接：https://blog.csdn.net/hanjinrui15/article/details/102254551

版权

CTF 专栏收录该内容

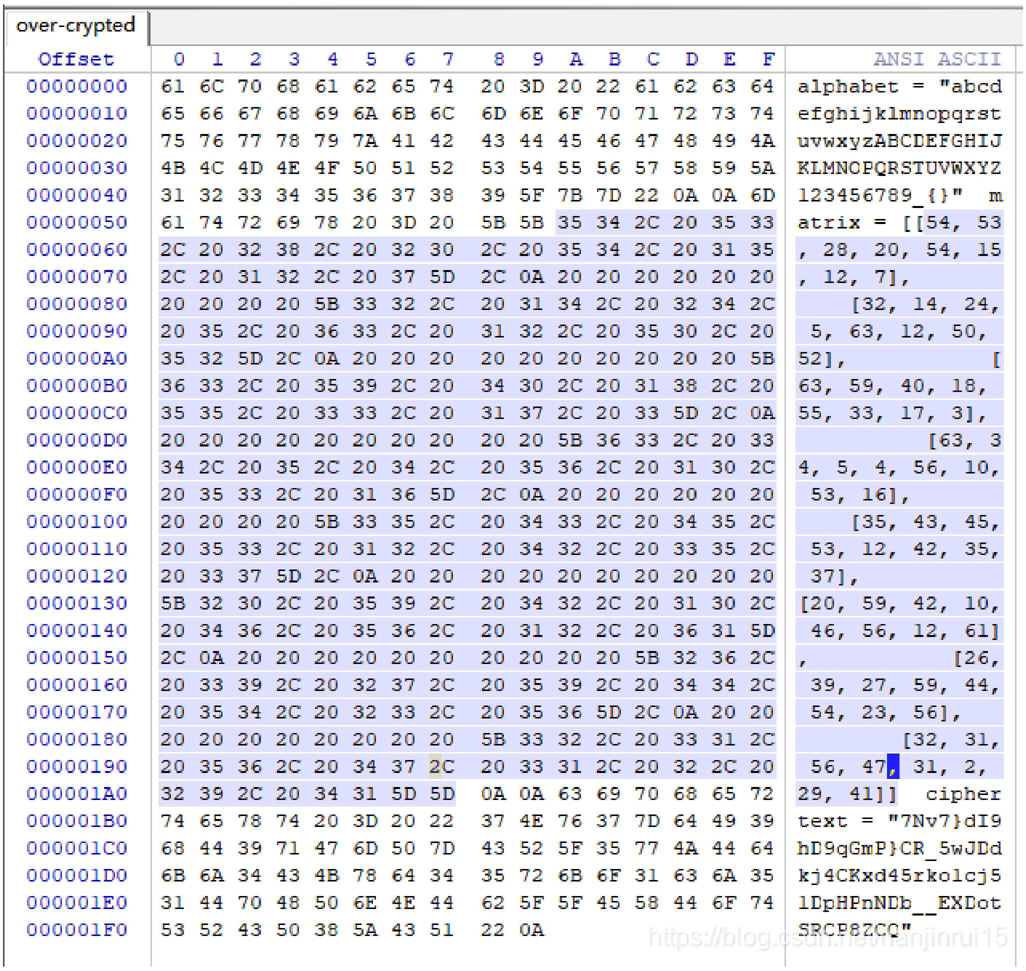
17 篇文章 1 订阅

订阅专栏

i春秋第二届春秋欢乐赛 over the hill writeup

希尔密码

这道题是希尔密码，我们先用winhex查看一下给出的file：



```
over-crypted
  Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F      ANSI ASCII
 00000000   61 6C 70 68 61 62 65 74  20 3D 20 22 61 62 63 64   alphabet = "abcd
 00000010   65 66 67 68 69 6A 6B 6C  6D 6E 6F 70 71 72 73 74   efghijklmnopqrst
 00000020   75 76 77 78 79 7A 41 42  43 44 45 46 47 48 49 4A   uvwxyzABCDEFGHIJ
 00000030   4B 4C 4D 4E 4F 50 51 52  53 54 55 56 57 58 59 5A   KLMNOPQRSTUVWXYZ
 00000040   31 32 33 34 35 36 37 38  39 5F 7B 7D 22 0A 0A 6D   123456789_{}"  m
 00000050   61 74 72 69 78 20 3D 20  5B 5B 35 34 2C 20 35 33   atrix = [[54, 53
 00000060   2C 20 32 38 2C 20 32 30  2C 20 35 34 2C 20 31 35   , 28, 20, 54, 15
 00000070   2C 20 31 32 2C 20 37 5D  2C 0A 20 20 20 20 20 20   , 12, 7],
 00000080   20 20 20 20 5B 33 32 2C  20 31 34 2C 20 32 34 2C       [32, 14, 24,
 00000090   20 35 2C 20 36 33 2C 20  31 32 2C 20 35 30 2C 20    5, 63, 12, 50,
 000000A0   35 32 5D 2C 0A 20 20 20  20 20 20 20 20 20 20 5B   52],           [
 000000B0   36 33 2C 20 35 39 2C 20  34 30 2C 20 31 38 2C 20   63, 59, 40, 18,
 000000C0   35 35 2C 20 33 33 2C 20  31 37 2C 20 33 5D 2C 0A   55, 33, 17, 3],
 000000D0   20 20 20 20 20 20 20 20  20 20 5B 36 33 2C 20 33             [63, 3
 000000E0   34 2C 20 35 2C 20 34 2C  20 35 36 2C 20 31 30 2C   4, 5, 4, 56, 10,
 000000F0   20 35 33 2C 20 31 36 5D  2C 0A 20 20 20 20 20 20    53, 16],
 00000100   20 20 20 20 5B 33 35 2C  20 34 33 2C 20 34 35 2C       [35, 43, 45,
 00000110   20 35 33 2C 20 31 32 2C  20 34 32 2C 20 33 35 2C    53, 12, 42, 35,
 00000120   20 33 37 5D 2C 0A 20 20  20 20 20 20 20 20 20 20    37],
 00000130   5B 32 30 2C 20 35 39 2C  20 34 32 2C 20 31 30 2C   [20, 59, 42, 10,
 00000140   20 34 36 2C 20 35 36 2C  20 31 32 2C 20 36 31 5D    46, 56, 12, 61]
 00000150   2C 0A 20 20 20 20 20 20  20 20 20 20 5B 32 36 2C   ,           [26,
 00000160   20 33 39 2C 20 32 37 2C  20 35 39 2C 20 34 34 2C    39, 27, 59, 44,
 00000170   20 35 34 2C 20 32 33 2C  20 35 36 5D 2C 0A 20 20    54, 23, 56],
 00000180   20 20 20 20 20 20 20 20  5B 33 32 2C 20 33 31 2C           [32, 31,
 00000190   20 35 36 2C 20 34 37 2C  20 33 31 2C 20 32 2C 20    56, 47, 31, 2,
 000001A0   32 39 2C 20 34 31 5D 5D  0A 0A 63 69 70 68 65 72   29, 41]]  cipher
 000001B0   74 65 78 74 20 3D 20 22  37 4E 76 37 7D 64 49 39   text = "7Nv7}dI9
 000001C0   68 44 39 71 47 6D 50 7D  43 52 5F 35 77 4A 44 64   hD9qGmP}CR_5wJDd
 000001D0   6B 6A 34 43 4B 78 64 34  35 72 6B 6F 31 63 6A 35   kj4CKxd45rkolcj5
 000001E0   31 44 70 48 50 6E 4E 44  62 5F 5F 45 58 44 6F 74   1DpHPnNDb__EXDot
 000001F0   53 52 43 50 38 5A 43 51  22 0A                     SRCP8ZCQ"
```

计算

```
import numpy

from sage.all import *

alphabet = ("abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ123456789_{}")

n = len(alphabet)

Zn = IntegerModRing(n)

secret  = [[54, 53, 28, 20, 54, 15, 12, 7],

          [32, 14, 24, 5, 63, 12, 50, 52],

          [63, 59, 40, 18, 55, 33, 17, 3],

          [63, 34, 5, 4, 56, 10, 53, 16],

          [35, 43, 45, 53, 12, 42, 35, 37],

          [20, 59, 42, 10, 46, 56, 12, 61],

          [26, 39, 27, 59, 44, 54, 23, 56],

          [32, 31, 56, 47, 31, 2, 29, 41]]

secret = matrix(Zn, secret).inverse()

ciphertext = "7Nv7}dI9hD9qGmP}CR_5wJDdkj4CKxd45rko1cj51DpHPnNDb__EXDotSRCP8ZCQ"

blocks = [ciphertext[i : i + secret.ncols()] for i in range(0, len(ciphertext), secret.ncols())]

plaintext = ''

for block in blocks:

    decrypted_block = secret * matrix(Zn, [alphabet.find(c) for c in block]).transpose()

    plaintext +=  ''.join(alphabet[int(i[0])] for i in decrypted_block)


print plaintext
```

在在线运行程序网站上泡一下：https://sagecell.sagemath.org/
得到结果：

```
IceCTF{linear_algebra_plus_led_zeppelin_are_a_beautiful_m1xture}
```