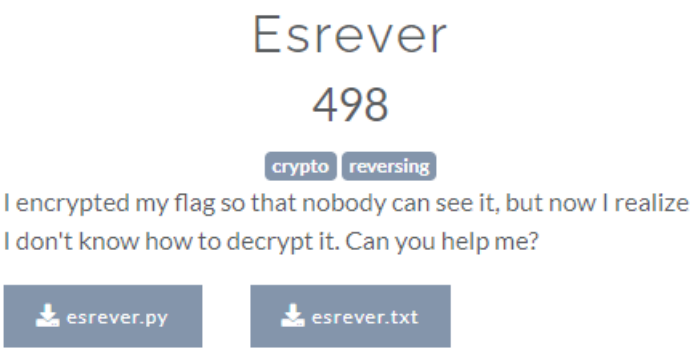
【CSICTF】Esrever WriteUp

原创

古月浪子 于 2020-07-23 16:08:46 发布 278 收藏

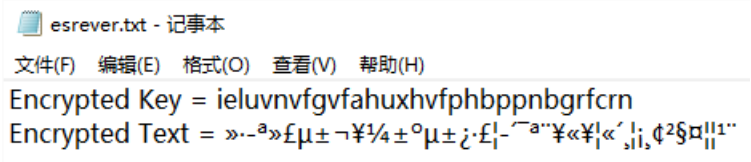
文章标签： CTF

本文链接：https://blog.csdn.net/tqydyqt/article/details/107479435



这道题看起来不像是逆向，更像是密码学 =_=

```python
import random

# TODO: Remember to remove real flag before deploying
flag = 'csictf{fake_flag}'

key = 'fake_key'

def enc1(text):
    r = random.randint(1,25)
    return bytes.fromhex(''.join([hex(((ord(i) - ord('a') - r) % 26) + ord('a'))[2:] for i in text])).decode('as
cii')

def enc2(text, key):
    k = [key[i % len(key)] for i in range(len(text))]
    return ''.join([chr(ord(text[i]) ^ ord(k[i]) + ord('a')) for i in range(len(text))])

def enc3(text):
    mapping = [28, 33, 6, 17, 7, 41, 27, 29, 31, 30, 39, 21, 34, 15, 3, 5, 13, 10, 19, 38, 40, 14, 26, 25, 32, 0
, 36, 8, 18, 4, 1, 11, 24, 2, 37, 20, 23, 35, 22, 12, 16, 9]

    temp = [None]*len(text)
    for i in range(len(text)):
        temp[mapping[i]] = text[i]

    return ''.join(temp)

def enc4(text):
    mapping = [23, 9, 5, 6, 22, 28, 25, 30, 15, 8, 16, 19, 24, 11, 10, 7, 2, 14, 18, 1, 29, 21, 12, 4, 20, 0, 26
, 13, 17, 3, 27]

    temp = [None]*len(text)
    for i in range(len(text)):
        temp[i] = text[mapping[i]]

    return ''.join(temp)

encryptedText = enc1(flag)
encryptedKey = enc1(key)
for i in range(random.randint(1,100)):
    encryptedText = enc1(encryptedText)
    encryptedKey = enc1(key)

print('Encrypted Key = ' + enc4(enc4(encryptedKey)))
print('Encrypted Text = ' + enc3(enc3(enc2(enc1(encryptedText), key))))
```

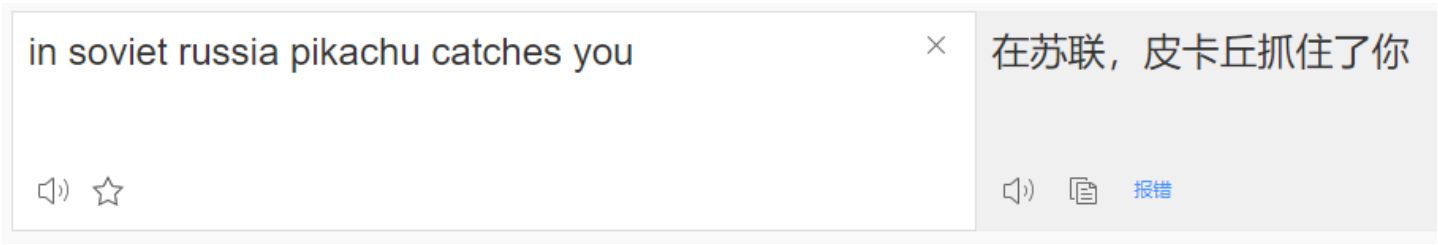


首先找key，enc4是对一个长度31的字符串进行变换每个字符的位置，逆函数非常好写，这里就不写了

求2次逆函数以后，得到了n次enc1加密后的key，enc1看起来不可逆，但是不管执行多少次，它的结果只会有26种：将每个字符移动0-25个位置，位置在a-z中循环，执行一次函数所有字符移动的位置是相同的，因此直接跑26次循环，能得到26种可能的结果

我们发现其中一个结果读得通，其他25个无意义

> insovietrussiapikachucatchesyou



那么暂定key就是这个，接下来求解flag

在我用WinHex提取二进制的时候，又出现了神秘的0xc2

esrever.txt

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
00000000	45	6E	63	72	79	70	74	65	64	20	4B	65	79	20	3D	20	Encrypted Key =
00000016	69	65	6C	75	76	6E	76	66	67	76	66	61	68	75	78	68	ieluvnvfgvfahuxh
00000032	76	66	70	68	62	70	70	6E	62	67	72	66	63	72	6E	0A	vfphbppnbgrfcrn
00000048	45	6E	63	72	79	70	74	65	64	20	54	65	78	74	20	3D	Encrypted Text =
00000064	20	C2	BB	C2	B7	C2	AD	C2	AA	C2	BB	C2	A3	C2	B5	C2	Â»Â·Â-Âª Â»Â£ÂµÂ
00000080	B1	C2	AC	C2	A5	C2	BC	C2	B1	C2	BA	C2	B5	C2	B1	C2	±Â¬Â¥Â¼Â±Âº ÂµÂ±Â
00000096	BF	C2	B7	C2	A3	C2	A6	C2	AD	C2	B4	C2	AF	C2	AA	C2	¿Â·Â£Â¦Â-Â´Â¯Âª Â
00000112	A8	C2	A5	C2	AB	C2	A5	C2	A6	C2	AB	C2	B4	C2	B8	C2	¨Â¥Â«Â¥Â¦Â«Â´Â¸Â
00000128	A6	C2	A1	C2	B8	C2	A2	C2	B2	C2	A7	C2	A4	C2	A6	C2	¦Â¡Â¸Â¢Â²Â§Â¤Â¦Â
00000144	A6	C2	B9	C2	A8	0A											¦Â¹Â¨

具体问题参考上一篇 pydis2ctf，这次索性放弃WinHex，直接从记事本复制到IDE，发现没问题，那么继续解题

首先是2次enc3函数，这个和enc4大同小异，然后求enc2的逆函数，可以看到就是简单的异或和加法

（这里有个坑，注意加号的优先级比异或的优先级高，写逆函数的时候别在这里翻车了，免得白白浪费几分钟。。。）

然后和上面一样，跑26次，发现了比较靠谱的字符串

csictfaesreverisjustreverseinreverserightc

可是明显flag格式不对，注意到题目名称是esrever，元音单词，所以csictf后面的a不是冠词，而right后面的c也莫名其妙，将a和c换成大括号，完美！

> csictf{esreverisjustreverseinreverseright}