

[点击此处](#)获得更好的阅读体验

WriteUp来源

来自M01N战队

题目描述

某安全机构截获了一段密文，并通过社工的方式获取了该密文对应的加密方式。现请你帮助他们对该密文进行解密。
4441774e565535504f535a4e524870556446414f5a45496b6152634f41424e49483355774e5339414d44553d

题目考点

- 算法分析

解题思路

根据题意编写解密算法，得到flag

```
1 import struct
2 import base64
3 import binascii
4 flag = 'xxxxxxxxxxxxxxxxxxxxxx'
5 key = 0x326c3567
6
7 def crypto(data):
8     #print(data,data>>16)
9     return data ^ data >> 16
10
11 def encode(data_content, key):
12     cyphertext = []
13     data_content_length = len(data_content)
14     cyphertext += [crypto(data_content[0] ^ key)]
15
16     for i in range(1, data_content_length):
17         cyphertext += [crypto(cyphertext[i-1] ^ data_content[i])]
18
19     crypted_result = ''
20     for c in cyphertext:
21         crypted_result += struct.pack("I", c)
22
23     return base64.b64encode(crypted_result)
24 def decode(p_en_content,key):
25
26     p_en_content=base64.b64decode(p_en_content)
27     en_content = struct.unpack("I" * (len(p_en_content) / 4), p_en_content)
28     print(en_content)
29     plain_text=[]
30     en_len= len(en_content)
31     plain_text+= [crypto(en_content[0])^key]
32     for i in range(1, en_len):
33         plain_text += [crypto(en_content[i])^en_content[i-1] ]
34     decrypted_result = ''
35     for c in plain_text:
36         decrypted_result += struct.pack("I", c)
37
38     return decrypted_result
39
40 padding = 4 - len(flag) % 4
41 if padding != 0:
42     flag = flag + "\x00" * padding
43
44 data_content = struct.unpack("I" * (len(flag) / 4), flag)
45 en_data=encode(data_content, key)
46 print(decode(en_data,key))
47 #data_content = struct.unpack("I" * (len(flag) / 4), flag)
48 en_flag=binascii.a2b_hex('4441774e565535504f535a4e524870556446414f5a45496b6152634f41424e49483355774e5339414d44553d')
49 print(decode(en_flag,key))
50 print('%x'%crypto(crypto(0x45678922)))
```

Flag

```
1 flag{e4sy_Cr7pt0_cgs_lz_!@#}
```

- 本文作者: CTFHub
- 本文链接: <https://writeup.ctfhub.com/Challenge/2021/工业信息安全技能大赛/巡回赛-兰州站/by1MKTduiZHfth7z9wrtWa.html>
- 版权声明: 本博客所有文章除特别声明外, 均采用 [BY-NC-SA](#) 许可协议。转载请注明出处!

[#Challenge #2021](#) [#工业信息安全技能大赛](#) [#巡回赛-兰州站](#)

[1](#)

[7](#)