

This_is_not_a_standard_AES256

发表于 2021-01-16 分类于 [Challenge](#) , [2019](#) , [安洵杯](#) , [Crypto](#)
[Challenge](#) | [2019](#) | [安洵杯](#) | [Crypto](#) | [This_is_not_a_standard_AES256](#)

[点击此处](#) 获得更好的阅读体验

WriteUp来源

<https://xz.aliyun.com/t/6912>

题目考点

解题思路

先nc获取信息

```
1 PS C:\Users\HiragaAya> nc 49.233.64.38 22333
2 This is you Sbox(tuple)
3 126, 143, 160, 15, 180, 170, 84, 152, 109, 20, 40, 136, 49, 179, 125, 165, 53, 251, 215, 87, 167, 41, 241, 178, 253, 239, 233, 193, 60, 110, 14, 246, 89, 228, 31, 42, 72,
4 -----
5 This is you key(str)
6 letrvogspwoxjknzfylteavqbimszrwhk
7 -----
8 This is you cipher(list)
9 93, 78, 25, 81, 18, 232, 250, 12, 94, 128, 81, 128, 88, 156, 180, 110, 151, 87, 197, 247, 8, 228, 51, 71, 102, 38, 146, 218, 40, 70, 6, 16
10 -----
11 Enjoy it!
12 PS C:\Users\HiragaAya>
```

然后使用exp.py

```
1 import AES256,sbox
2 send = (126, 143, 160, 15, 180, 170, 84, 152, 109, 20, 40, 136, 49, 179, 125, 165, 53, 251, 215, 87, 167, 41, 241, 178, 253, 239, 233, 193, 60, 110, 14, 246, 89, 228, 31,
3 invsbox = sbox.InvSbox(send)
4 print (invsbox)
5 cipher = [93, 78, 25, 81, 18, 232, 250, 12, 94, 128, 81, 128, 88, 156, 180, 110, 151, 87, 197, 247, 8, 228, 51, 71, 102, 38, 146, 218, 40, 70, 6, 16]
6 key = "letrvogspwoxjknzfylteavqbimszrwhk"
7 plain = AES256.decrypt(cipher,key,"ECB","")
8
9 AES256.plain_to_ascii(plain)
```

运行得到逆S盒

```
1 161, 101, 167, 60, 171, 44, 206, 86, 131, 108, 76, 255, 138, 61, 30, 3, 253, 64, 77, 92, 9, 165, 38, 225, 226, 93, 245, 148, 42, 173, 152, 34, 88, 125, 150, 205, 48, 189,
2 243, 73, 65, 39, 176, 147, 112, 103, 201, 114, 8, 29, 40, 94, 224, 159, 222, 211, 160, 106, 81, 209, 143, 202, 178, 247, 14, 0, 70, 133, 129, 56, 83, 227, 55, 117, 135, 11,
```

填入AES256.py的前面

```
1 (161, 101, 167, 60, 171, 44, 206, 86, 131, 108, 76, 255, 138, 61, 30, 3, 253, 64, 77, 92, 9, 165, 38, 225, 226, 93, 245, 148, 42, 173, 152, 34, 88, 125, 150, 205, 48, 189,
2 243, 73, 65, 39, 176, 147, 112, 103, 201, 114, 8, 29, 40, 94, 224, 159, 222, 211, 160, 106, 81, 209, 143, 202, 178, 247, 14, 0, 70, 133, 129, 56, 83, 227, 55, 117, 135, 11,
3 flag{sbox_to_invsbox}
4 PS C:\Users\HiragaAya>
```

Flag

```
1 flag{sbox_to_invsbox}
```

- 本文作者: CTFHub
- 本文链接: <https://writeup.ctfhub.com/Challenge/2019/安洵杯/Crypto/w6UVUTuVciHE4ADdriLJE5.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 # 2019 # Crypto # 安洵杯

[funny_php](#)

[crackWithFreq](#)