Esrever

发表于 2021-01-09 分类于 Challenge， 2020， CSICTF， Reverse
Challenge | 2020 | CSICTF | Reverse | Esrever

点击此处获得更好的阅读体验

WriteUp来源

https://dunsp4rce.github.io/csictf-2020/reversing/2020/07/21/Esrever.html

by `anishbadhri`

题目描述

> *I encrypted my flag so that nobody can see it, but now I realize I don't know how to decrypt it. Can you help me?*

题目考点

解题思路

`esrever.py` *contains 4 functions* `enc1`, `enc2`, `enc3` *and* `enc4`. *The first step would be to determine how to reverse each of these functions*

- `enc4` *can be reversed by using the same mapping array but assigning in reverse.*
- `enc3`, *similar to* `enc4` *can be reversed using the same mapping aray and assiging in reverse.*
- `enc2` *is an xor function and hence is its own reverse.*
- `enc1` *is a caesar shift of a random value and hence needs to be iterated for the range of the random value*

The `encryptedText` *and* `encryptedKey` *being encrypted with* `enc1` *a hundred times does not matter as the caesar shift can be tested on all values of 0 to 26.*

The flag is obtained on reversing each function from the end.

Solution Script:

```
def enc4rev(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[mapping[i]] = text[i]
  return ''.join(temp)
def enc3rev(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, 
    temp = [None]*len(text)
    for i in range(len(text)):
        temp[i] = text[mapping[i]]
    return ''.join(temp)
def enc2rev(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))])
encryptedkey = enc4rev(enc4rev('ieluvnvfgvfahuxhvfphbppnbgrfcrn'))
encryptedtext = enc3rev(enc3rev('»·ª»£µ±¬¥¼±°µ±¿·£¦´¯ª¨¥«¥¦«´¸¦¸¢²§¤¦¦¹¨'))
finalres = set()
for j in range(1,26):
  normalkey = bytes.fromhex(''.join([hex(((ord(i) - ord('a') + j) % 26) + ord('a'))[2:] for i in encryptedkey])).decode('ascii')
  tex = enc2rev(encryptedtext, normalkey)
  for k in range(0, 26):
    normaltex = bytes.fromhex(''.join([hex(((ord(i) - ord('a') + k) % 26) + ord('a'))[2:] for i in tex])).decode('ascii')
    finalres.add(normaltex)
for i in finalres:
  if i[0:6] == "csictf":
    print(i)
```

Flag

```
csictf{esreverisjustreverseinreverseright}
```

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2020/CSICTF/Reverse/gn8cdffZy22z5KUNmoAoKY.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 # 2020 # Reverse # CSICTF
Blaise
Shaken