H0W

Author : wayneOuO | 吳崇維 | B06902058

Problem Description

提供了一個pyc檔，以及一個so檔案。python的行為是接受一個檔案，並經過類似加密的過程後輸出。題目給了一個輸出後的檔案，求原始檔案。

Solution

首先要先觀察so檔案裡面的行為，他一共有6個function (nini1 ~ nini6) 以及4種加密方法。

首先要先了解6種function的行為以及加密方式。

加密：

- 一之型：xor 0xfaceb00c
- 二之型：add 0x12385
- 三之型：可以用下列函式表示

```
def thr(x):
  a = x & 0x5555555555
  b = x & 0xaaaaaaaaaa
  a = (a // 16) + (a % 16) * 2 ** 28
  b = (b % (2 ** 30)) * 4 + ( (b - (b % (2 ** 30))) // (2**30) )
  return a|b
```

- 四之型: 就是依序用1, 2, 3加密

可以發現上面四個都是可以一對一reverse的，其中三之型比較複雜，去觀察每一個bit的轉換後一一對應。

不過python的檔案會先以 `srand((time(NULL)))` 來設定種子，設定之後random的選用加密方法。不過最後會將當時設定的日期append在檔案後面。

所以reverse過程就是：將要reverse的檔案的日期確定 (注意格式：例如month的範圍是0~11，日期是以星期幾表示，因此有多種可能)，設定種子之後用相對應的解密方法解回去，會得到一個檔案，嘗試過後發現有一次嘗試的檔案開頭是png的magic number，確定flag就在裡面！