HGAME Week4 WriteUp

CRYPTO

居然狗住了，虽然又只写了一道题

2. ToyCipher_Linear

打开查看，再加上百度，发现这是一个费斯妥密码

```
def ToyCipher(block, mode='enc'):
    '''Feistel networks'''
```

然后在底下发现每次运行程序都会随机生成一个 key，那么我们要获取 flag 只能想办法通过这个 key？key 从哪里来，当然是从例子来，因为随机 key 是在主程序里的，一共只运行一次。这道题是把字符几次转换变成 bytes 之后，再四个一组进行加密。然后知道这些条件之后就按照程序倒着算了一下密钥，结果突然发现 key 跟密文那一块其实是无关的，只要把 f 函数那里的 key 删掉，然后处理一下再异或就是 key。

```
def f(x, roundkey):
    return rotL(x, 16, 7) ^ rotL(x, 16, 2)
```

完成脚本（https://paste.ubuntu.com/p/8J2cnndSW9/）运行获得 flag

```
lazyboy@ubuntu:~/Desktop/crypto$ python3 toy.py
b'\x91a\xb1o\xed_\xb2\x8c\x00\x1b\xdfp'
b'@\x91\xa6\xde\n\x85\xf5\xde0\x97\xa1\xab'
b'hgame{r0TAT!on_&&-x0r_4Re-b0tH~l1neaR_0pEr4t1On5}\x03\x03\x03'
lazyboy@ubuntu:~/Desktop/crypto$
```