Crypto_[ACTF新生赛2020]crypto-aes

原创

M3ng@L 于 2021-11-16 13:27:27 发布 181 收藏

文章标签： 密码学 python

本文链接：https://blog.csdn.net/qq_51999772/article/details/121353885

[ACTF新生赛2020]crypto-aes

题目描述：

```
from Cryptodome.Cipher import AES
import os
import gmpy2
from flag import FLAG
from Cryptodome.Util.number import *

def main():
    key=os.urandom(2)*16
    iv=os.urandom(16)
    print(bytes_to_long(key)^bytes_to_long(iv))
    aes=AES.new(key,AES.MODE_CBC,iv)
    enc_flag = aes.encrypt(FLAG)
    print(enc_flag)
if __name__=="__main__":
    main()
```

注意这个`os.urandom(n)`函数返回的是随机n个字节

而形如`os.urandom(n)*k`是返回k个n随机字节

比如

> >>>os.urandom(3)*3
> b'j\x12\x00j\x12\x00j\x12\x00'

所以这里的key是两个不断重复的字节组成

然后key是32字节，iv（偏移量）是16字节

当二者进行异或之后，只有低位16位实际进行了异或所以高位16位依然是key的高16位，而key又是重复的字节组成，所以可以推出key的全部字节

> 这里有一点是字节的高位在字节流的左侧，而不是像十进制中的数字高位在右侧的惯性思维，print一下对比看看

key已知后再对iv和key异或的结果进行异或就可以得到iv（这里的iv需要是异或之后的结果的低16位，使用切片操作切一下就行）

得到key和iv，再import AES继续求解（mode是CBC）

代码实现：

```
from Crypto.Util.number import *
from Crypto.Cipher import AES
from pwn import xor
iv_key = 91144196586662942563895769614300232343026691029427747065707381728622849079757
enc_flag = b'\x8c-\xcd\xde\xa7\xe9\x7f.b\x8aKs\xf1\xba\xc75\xc4d\x13\x07\xac\xa4&\xd6\x91\xfe\xf3\x14\x10|\xf8p'

iv_key = long_to_bytes(iv_key)
iv_key_high = iv_key[2:4]
key = iv_key_high * 16
iv = xor(iv_key,key)[16:]
aes = AES.new(key,AES.MODE_CBC,iv)
flag = aes.decrypt(enc_flag)
print(flag)
```

思路来源：[(51条消息) ACTF新生赛2020]crypto-aes（考点：AES）_MikeCoke的博客-CSDN博客

AES讲解：AES — PyCryptodome 3.11.0 documentation