[ACTF新生赛2020]crypto-aes

原创

前方是否可导？ 于 2020-07-25 19:54:08 发布 619 收藏 4

分类专栏： AES

版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/weixin_44110537/article/details/107583819

版权

AES 专栏收录该内容

2 篇文章 0 订阅

订阅专栏

encrypt

```
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()
```

decrypt

key是两个字节不断重复得到的，因此结合输出的与iv向量的异或值很容易的到key和iv

```
'''
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()
'''
key_iv=91144196586662942563895769614300232343026691029427747065707381728622849079757
flag_encrypt=b'\x8c-\xcd\xde\xa7\xe9\x7f.b\x8aKs\xf1\xba\xc75\xc4d\x13\x07\xac\xa4&\xd6\x91\xfe\xf3\x14\x10|\xf8
p'
#print(hex(key_iv))
key=hex(key_iv)[2:6]*16
iv=key_iv^eval('0x'+key)
import Crypto.Util.number
iv=Crypto.Util.number.long_to_bytes(iv)
key=Crypto.Util.number.long_to_bytes(eval('0x'+key))
import Crypto.Cipher.AES
decrypt=Crypto.Cipher.AES.new(key,Crypto.Cipher.AES.MODE_CBC,iv)
print(decrypt.decrypt(flag_encrypt))
```

创作打卡挑战赛 〉
赢取流量/现金/CSDN周边激励大奖