easyaes

发表于 2021-01-15 分类于 Challenge， 2020， 安洵杯， Crypto
Challenge | 2020 | 安洵杯 | Crypto | easyaes

点击此处获得更好的阅读体验

WriteUp来源

https://xz.aliyun.com/t/8581

题目考点

- *AES加密*

解题思路

hint和key长度不等,且hint为四个字符的重复

即输出的密文中有部分hint的字符,可以首先恢复hint再逐步次求出key

已知密文、明文、私钥可以根据aes的cbc模式原理求出位移

```
#!/usr/bin/python
from Crypto.Util.number import long_to_bytes
import binascii, sys
from Crypto.Util.strxor import strxor
from Crypto.Cipher import AES

# -----------get key---------
tmp = 566312332923254122055287547981339707836332169363020498931302204611391606827777
hint = int(str(hex(tmp))[2:10] * 8,16)
key = long_to_bytes(tmp ^ hint)

# ----------get iv-----------
msg = b'Welcome to this competition, I hope you can have fun today!!!!!!'
msgs = [msg[ii:(ii+16)] for ii in range(0,len(msg),16)]
msgs.reverse()
IV = binascii.unhexlify('3c976c92aff4095a23e885b195077b66')

def decry(key,IV,ms):
    aes=AES.new(key,AES.MODE_ECB)
    return strxor(aes.decrypt(IV),ms)

for ms in msgs:
    IV=decry(key,IV,ms)
print(b'd0g3{' + IV+ b'}')
```

Flag

```
d0g3{aEs_1s_SO0o_e4sY}
```

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2020/安洵杯/Crypto/rkNXFQUaTyA73LwqMobWhA.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 # Crypto # 安洵杯
密码学?爆破就行了
easyrsa