

# 2017陕西省网络空间安全技术大赛\_Crypto\_crypt1\_Writeup

原创

 Flying Fatty 于 2017-04-19 15:29:43 发布  1950  收藏

分类专栏: [Crypto CTF之旅](#)

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/kevin66654/article/details/70240167>

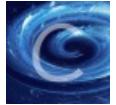
版权



[Crypto 同时被 2 个专栏收录](#)

28 篇文章 1 订阅

订阅专栏



[CTF之旅](#)

84 篇文章 2 订阅

订阅专栏

[题目地址](#)

中间人相遇攻击

题目给了一份这样的RC2加密的代码

```

# -*- coding: utf-8 -*-
from Crypto import Random
from Crypto.Cipher import ARC2

def encrypt_data(data, key):
    iv = 'k\xbb\xf4B\x18\xe9U\xd0'
    cipher = ARC2.new(key, ARC2.MODE_CFB, iv)
    msg = cipher.encrypt(data)
    return msg

def decrypt_data(data, key):
    iv = 'k\xbb\xf4B\x18\xe9U\xd0'
    cipher = ARC2.new(key, ARC2.MODE_CFB, iv)
    msg = cipher.decrypt(data)
    return msg

def encrypt(data, key1, key2):
    encrypted = encrypt_data(data, key1)
    encrypted = encrypt_data(encrypted, key2)
    return encrypted

def decrypt(data, key1, key2):
    decrypted = decrypt_data(data, key2)
    decrypted = decrypt_data(decrypted, key1)
    return decrypted

if __name__ == '__main__':
    plain_text = 'flag{*****}'
    cipher_text1 = "|\\xd6-\\x14?\\xb9\\xa1\\x86\\x81\\xa4\\xdc\\x950\\x941'V'\\xaf"

```

没几行，一眼可以看到重要信息：decrypt\_data和encrypt\_data中的iv是一样的，要得到flag，我们需要知道的东西是key1和key2

根据hint，我们需要知道中间人攻击是个啥，然后采取破解手段

因为我们已知明文的一部分是flag{，先用key1加密，得到一个中间字符串

最后的密文知道，用key2解密，得到一个中间字符串

如果某两个key的情况下，这两个中间字符串相等，那么这两个key就是我们所要的

这里有个暴力的技巧：在构造字符串表格的时候，使用内容少的来存储（减小大量空间，方便查询）

根据百度百科，密钥的长度在目前的实现是8字节，每个字节是256种可能，所以可能情况是256的8次方，key1的枚举量应该是2的64次方（不清楚writeup为啥直接写的 $2^{24}$ ）

python的字典可能存不了这么大的，所以估计只能一个一个跑，先猜测是20，20没有结果再21，再22吧……

还有为啥是prime也没搞懂……（因为是RSA的开发者开发的，喜欢素数？）

思路：

先把flag{字符串加密，存入字典中，字符对是加密后的结果与key1的值

然后，暴力key2，对密文进行解密，如果前几个字节在字典中出现（说明撞库了），而且key2是素数（不明白为啥）

那么，key1和key2就是我们需要的，再按照题意传参进去解密得到flag

```
# -*- coding: utf-8 -*-
import RC2

plain_text = 'flag{'
cipher_text1 = "|\\xd6-\\x14?\\xb9\\xa1\\x86\\x81\\xa4\\xdc\\x950\\x941'V'\\xaf"
def isprime(n):
    if n <= 1:
        return False
    if n == 2:
        return True
    if n % 2 == 0:
        return False
    for i in range(3,int(n**0.5)+1,2):
        if n % i == 0:
            return False
    return True

data = dict()
for key1 in xrange(0,2**24):
    data[RC2.encrypt_data(plain_text,str(key1))] = key1
for i in xrange(0,2**24):
    try:
        a = RC2.decrypt_data(cipher_text1,str(i))
        if isprime(data[a[:5]]) == True and isprime(i) == True:
            print (data[a[:5]],i)
    except:
        pass

key1 = 13433911
key2 = 38593
data = RC2.decrypt_data(cipher_text1,str(key1))
print RC2.decrypt_data(data,str(key2))
```

这个RC2的可以得到flag也觉得很奇怪，都没有原来程序的iv，是怎么跑出来的.....

或者把key1和key2放到题目给的py中运行，得到flag{!TianGe-&-Hu!}

```
key1 = 38593
key2 = 13433911
print decrypt(cipher_text1,str(key1),str(key2))
```

学到了暴力姿势~