CTF-CRYPTO-Feistel

原创

大熊何在 于 2020-11-30 17:32:13 发布 217 收藏 2

分类专栏： CRYPTO

本文链接：https://blog.csdn.net/zippo1234/article/details/110392831

CTF-CRYPTO-Feistel

每天一题，只能多不能少

Feistel

题目分析

1. 类似feistel
2. 密钥碰撞

开始

1.题目

给出feistel.py和feistel.log

feistel.py

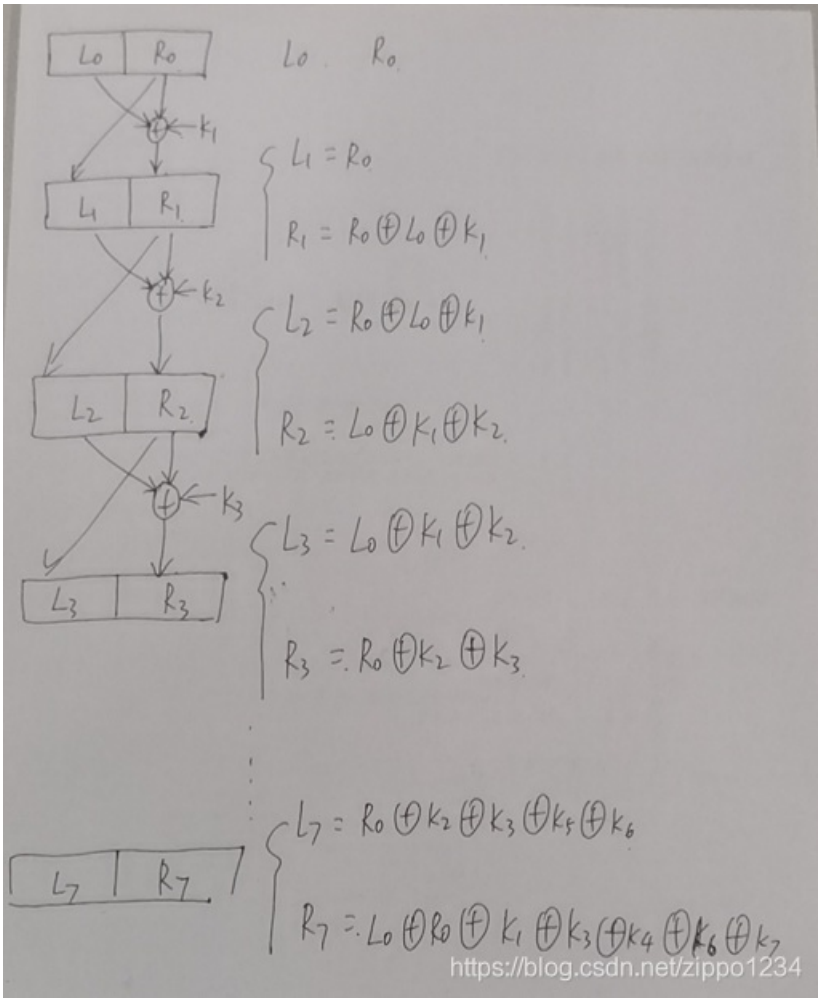
```
#!/usr/bin/python
#encoding=utf-8
import os
def strxor(a,b):
    assert len(a) == len(b)
    c = ''
    for i in range(len(a)):
        c += chr(ord(a[i])^ord(b[i]))
    return c

def round(M, K):
    L = M[0:27]
    R = M[27:54]
    new_l = R
    new_r = strxor(strxor(R, L), K)
    return new_l+new_r

def fez(m,K):
    for i in K:
        m = round(m, i)
    return m

K = []
for i in range(7):
    K.append(os.urandom(27))

m = open("flag.txt","rb").read()
assert len(m)<54
m += os.urandom(54-len(m))

test = os.urandom(54)
print 'test = '+test.encode("hex")
print 'fez(test,K) = '+fez(test,K).encode("hex")
print 'fez(m,K) = '+fez(m,K).encode("hex")
```

feistel.log

```
test = 1a8b7027a3766821a072a779c0879f3d6bf06dbea48e2d52a390f3b68386d48f7f45cc15388d65aca04500d17e4c105b2911625e8bc6
fez(test,K) = e704fb0de86487c7ceee1d95555cef945b5b2fee4c5454b36a8f84bebed7cd63bb86cec33f4de2aea3f5ca4f6e859d679854d8b3a6d5
fez(m,K) = 39e62fbd1a3b8b05da0eafd5471774f650079a99942d5d5153577b1cbb123d49d4d14445d96bb7235d85e77aa1290b725d2f06199a86
```

2.分析

就是2018年护网杯的fez。。。。。只是改了下加密的内容而已。
加密过程类似DES的feistel。



也就是

$$L = R \oplus K \oplus K \oplus K \oplus K \cdots K \oplus K$$

3.脚本

直接抄袭WP即可。。。

```
def xor(a,b):
    assert len(a)==len(b)
    c=""
    for i in range(len(a)):
        c+=chr(ord(a[i])^ord(b[i]))
    return c

test='1a8b7027a3766821a072a779c0879f3d6bf06dbea48e2d52a390f3b68386d48f7f45cc15388d65aca04500d17e4c105b2911625e8bc6'.decode('hex')
test_K='e704fb0de86487c7ceee1d95555cef945b5b2fee4c5454b36a8f84bebed7cd63bb86cec33f4de2aea3f5ca4f6e859d679854d8b3a6d5'.decode('hex')
K_M='39e62fbd1a3b8b05da0eafd5471774f650079a99942d5d5153577b1cbb123d49d4d14445d96bb7235d85e77aa1290b725d2f06199a86'.decode('hex');

Lt=test[0:27]
Rt=test[27:54]

#Kl=K2^K3^K5^K6  Kr=K1^K3^K4^K6^K7
Kl=xor(test_K[0:27],Rt)
Kr=xor(Lt,xor(test_K[27:54],Rt))

Mr=xor(Kl,K_M[0:27])
Ml=xor(Mr,xor(Kr,K_M[27:54]))

print Ml,Mr
```

4.get flag

```
flag{F3i2t3l_2trUct_i2_n0t_haRd}
```

结语

其实认真计算推演一下是能够自己做出来的。。或许能把。