ctf-夏令营-crypto

原创

逃课的小学生 于 2018-09-02 16:24:33 发布
分类专栏： ctf crypto 文章标签： ctf crypto

1.通过nc端口可以获得一个加密算法的五个参数n,e,d,c2,r。几次nc发现参数n,e,d不发生变化，而c2和r在不断的变化，所以猜测这是一个RSA加密，而c2和r都是密文，进行尝试，发现c2解出的明文与r^-1相乘可以获得一段有意义的明文，即为答案

```
import gmpy2
def shuchu(mingwenstr):
    if mingwenstr[len(mingwenstr)-1]=='L':
        mingwenstr=mingwenstr[2:len(mingwenstr)-1]
    else:
        mingwenstr=mingwenstr[2:len(mingwenstr)]
    if not len(mingwenstr)%2==0:
            mingwenstr='0'+mingwenstr
    i=len(mingwenstr)
    mingwen=""
    while i>=1:
        str1=mingwenstr[i-2:i]
        mingwen=chr(int(str1,16))+mingwen
        i=i-2
    return mingwen

e=3
d=58070556439793090526057208709744281266699522732880809417222160656726252113813697356285226658626010881834 4
n=87105834659689635789085813064616421900049284099321214125833240985089378170720546034427839987939016322751 6
c2=30132543736268406128006366464667229771073658466016673121647580163529342379328161036460170843634938824748
r=40362150765525455398305794281797305490609797222633763924968255583201392938971882099474127231258279012753 6
p3=pow(c2,d,n)
rinv=gmpy2.invert(r,n)
p4=(p3*rinv)%n
p4=hex(p4)
print shuchu(p4)
```

2.题目为x=chr（random.randint（0,0xff））+chr（random.randint（0,0xff）+chr（random.randint（0,0x1f）+chr（random.randint（0,0x1f）） hashlib.sha256（x）.hexdigest（）[0:8]==‘ caade32b ‘，尝试直接按题目代码进行暴力破解，发现无法得到结果，仔细思考明白在ascii码中只有32-128对应字符可以键入，其余字母是无法作为flag键入的，于是修改程序暴力破解，获得答案

```
import random
import hashlib
for a in xrange(32,128):
    for b in xrange(32,128):
        for c in xrange(32,128):
            for d in xrange(32,128):
                x=chr(a)+chr(b)+chr(c)+chr(d)
                if hashlib.sha256(x).hexdigest()[0:8]=='caade32b':
                    print x
```

3.题目为Alice与Bob正在通信，Alice发给Bob两段密文如下：
Li4tLS0gLi4tLS0g4oCmLS0gLi4tLS0g4oCmLS0gLi0tLS0gLi4tLS0gLi4tLS0g4oCmLS0g4oCmLS0g4oCmLS0gLusphcakdacvayunmtnqhp Eve截获了这两段密文，请你帮助他将密文破译出来。我们在题目中发现两端密文“Li4tLS0gLi4tLS0g4oCmLS0gLi4tLS0g4oCmLS0gLi0tLS0gLi4tLS0gLi4tLS0g4oCmLS0g4oCmLS0g4oCmLS(
很明显第一段明文使用base64加密，在线解密可得“..--- ..--- …-- ..--- …-- .---- ..--- ..--- …-- …-- …-- .---- ..--- ..---….- .---- …-- …--“，这是一段摩斯密码，解密可得“223231223331224133”，使用手机键盘即可发现其对应的是bedbfdbgf，这时一个密文时3*3，一个密文是3*7，猜测这里进行了hill加密，直接使用hill解密无果，尝试对第二段密文进行修改，将‘usphcakdacvayunmtnqhp’编程3*7的矩阵[usphcak,dacvayu,nmtnqhp]，在对第一三行做反转，可得[kcahpsu,dacvayu,phqntmn]，逆向栅栏可得字符串ppdkhaaqccnvhtapmysnuu，在对其使用hill密码解密可得gotothemoviethisnight。

4.题目为Eve窃听了Alice和Bob的通信，得到了Alice和Bob通信的公钥是（4846403,97）。以及下列一系列数据，请帮助Eve解密出这些数据的明文？ 1668222、313433、3647056、2851410、21188、3766877、3904324、1869820、3632941、2414731，可知这只是一个简单RSA解密，解密获得答案即可：

```
import gmpy2
n=4846403
e=97
c=[1668222,313433,3647056,2851410,21188,3766877,3904324,1869820,3632941,2414731]
p=2153
q=2251
d=int(gmpy2.invert(e,(p-1)*(q-1)))
m=[]
for i in c:
    mingwen=pow(i,d,n)
    m.append(mingwen)

print m
```

5.题目：
Alice与Bob正在进行加密通话。Eve从中进行了窃听，截获了Bob发给Alice的口令明文：Alice：d*@*68707600*K。Eve尝试用该用户和口令去登录Bob的服务器，发现该口令不正确。于是Eve入侵了Bob的电脑，在Bob的服务器上找到了Alice对应的口令的摘要，下载打开后如下所示：
4*de5f*d23l9fbdbll9fl3*8797**de75d7**94*。Eve尝试破译该口令时，发现该摘要和口令存在很多问题。你能帮助Eve破译出Alice的口令吗？有口令可以猜到这里大概是hash加密，而密文有四十位可以让我们想到这里应该是sha-1加密，这时暴力破解即可：

```
import hashlib
import re
s="4.de5f.d2319fbdb119f13.8797..de75d7..94."
for i in xrange(32,128):
    for j in xrange(32,128):
        for k in xrange(32,128):
            mingwen="d"+chr(i)+"@"+chr(j)+"68707600"+chr(k)+"K"
            temp=hashlib.sha1(mingwen).hexdigest()
            if re.match(s,temp):
                print mingwen
```