CTF CRYPTO

原创

C__搬砖人 于 2021-07-13 15:53:08 发布 72 收藏

分类专栏： CTF 文章标签： 密码学 信息安全

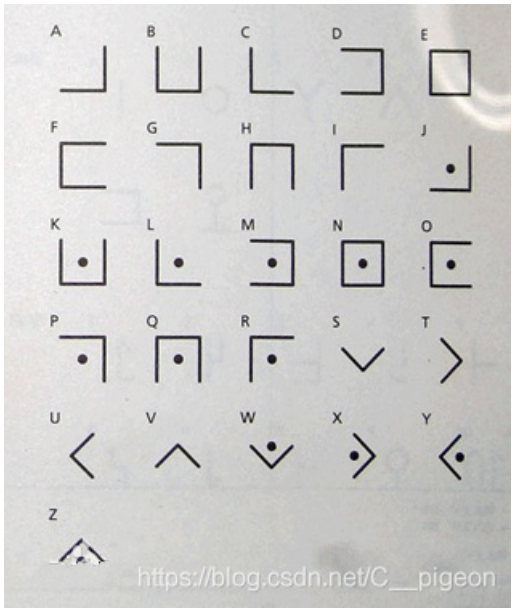
本文链接：https://blog.csdn.net/C__pigeon/article/details/118702184

CTF CRYPTO

萌萌哒的八戒

题目：

解答：猪圈密码



FLAG：

```
flag{whenthepigwanttoeat}
```

old-fashion /世上无难事

题目：

```
Os drnuzearyuwn, y jtkjzoztzoes douwlr oj y ilzwex eq lsdexosa kn pwodw tsozj eq ufyoszlbz yrl rlufydlx pozw douwlrzlbz, ydderxosa ze y rlatfyr jnjzli; mjy gfbmw vla xy wbfnsy symmyew (mjy vrwm qrvvrf), hlbew rd symmyew, mebhsymw rd symmyew, vbomgeyw rd mjy lxrzy, lfk wr dremj. Mjy eyqybzye kyqbhjyew mjy myom xa hyedrevbfn lf bfzyewywgxwmbmgmbrf. Wr mjy dsln bw f1_2jyf-k3_jg1-vb-vl_l
```

```
VIZZB IFIUOJBWO NVXAP OBC XZZ UKHVN IFIUOJBWO HB XVIXW XAW VXFI X QIXN VBD KQ IFIUOJBWO WBKAH NBWXO VBD XJBCN NKG QLKEIU DI XUI VIUI DKNV QNCWIANQ XN DXPIMKIZW VKHV QEVBBZ KA XUZKAHNBA FKUHKAKX XAW DI VXFI HBN QNCWIANQ NCAKAH KA MUBG XZZ XEUBQQ XGIUKEX MUBG PKAWIUHXUNIA NVUBCHV 12NV HUXWI XAW DI XUI SCQN QB HZXW NVXN XZZ EBCZW SBKA CQ NBWXO XAW DI DXAN NB NVXAP DXPIMKIZW MBU JIKAH QCEV XA BCNQNXAWKAH VBQN HKFI OBCUQIZFIQ X JKH UBCAW BM XLLZXCQI XAW NVI PIO KQ 640I11012805M211J0XJ24MM02X1IW09
```

解答：词频分析https://quipqiup.com/

FLAG:

```
flag{n1_2hen-d3_hu1-mi-ma_a}
flag{640e11012805f211b0ab24ff02a1ed09}
```

权限获得第一步

题目：

```
Administrator:500:806EDC27AA52E314AAD3B435B51404EE:F4AD50F57683D4260DFD48AA351A17A8:::
```

解答：

同前面的Windows系统密码，都是经过MD5处理的解密

```
F4AD50F57683D4260DFD48AA351A17A8
```

即可得到flag

FLAG:

```
flag{3617656}
```

RSA3

题目：

```
c1=223220352756632370416468937704519335093247019134843033380762106035426127589562628696408224864701211494244855713610074212936755163388221952803137949911360481409188424712198402635363388862504926827394364100134366511617207258554848666900847887213495556620198790815011132229961233055330093259643777988927031615218528059568112195638833128963301562986216746843539195475581279209257068428089147621990110549558165349776752673950095753478203870734839284250665363614827748923709695207403042874565555089333727823275065690107725374975417643114290522162911989320926177926452539014789108015928782035648611189120454649598325660513 61
n=227080788158850114624620490643391858987124392772268310734578884031293785473502924202670165518190524307790047558466490440010241414852832864831307026160572746984736111495087988697063475019315831176327107007872280164801276773936499295304165986860273542164225659344590151619276136079028315428579778596125962823536793277733037270044072621972315863245991819835726224045903540845417880622621645101406058681224103880901744201477524085541297897609023008980462739090078528184740307706996476473630151021189567376739413542176926960449696953085064365731425655734875835070373569448480398643823392162666706735674888715089253111548 01
e1=11187289
c2=187020100451870155565486916423949828356692621472302127313099386752264585552104259724294184492734105353879859310367118542656239050668056657518032691068807467690034789007910995902395139254497488140759040174715855728484735564905654500626647064491284158347879619472662597897859629222387011340797204142284140661930714953046123410529874556159300235368238014992697733571860874527475008406404193650115544211830375056534612867327409837027408226711480456194976671845861236572856040618756539095678223289140653377977334446403515187754876498199782623636172657979828431796308887294072384966509877204287082171152579890078673316983 97
e2=9647291
```

解答：共模攻击

```
from gmpy2 import invert
import binascii
def gongmogongji(n, c1, c2, e1, e2):
    def egcd(a, b):
        if b == 0:
            return a, 0
        else:
            x, y = egcd(b, a % b)
            return y, x - (a // b) * y
    s = egcd(e1, e2)
    s1 = s[0]
    s2 = s[1]

    if s1 < 0:
        s1 = - s1
        c1 = invert(c1, n)
    elif s2 < 0:
        s2 = - s2
        c2 = invert(c2, n)
    m = pow(c1, s1, n) * pow(c2, s2, n) % n
    return m
#n相同
n1=22708078815885011462462049064339185898712439277226831073457888403129378547350292420267016551819052430779004755846649044001024141485283286483130702616057274698473611149508798869706347501931583117632710700787228016480127677393649929530416598686027354216422565934459015161927613607902831542857977859612596282353679327773303727004407262197231586324599181983572622404590354084541788062262164510140605868122410388090174420147752408554129789760902300898046273090078528184740307706996476473630151021189567376739413542176926960449696953085064365731425655734875835070373569448480398643823392162666706735674888715089253111548014e1=11187289
e2=9647291
message1=22322035275663237041646893770451933509324701913484303338076210603542612758956262869640822486470121144944855713610074212936755163388221952803137949911360481409188424712198402635363388862504926827394364100134366511617207258554848666900847887213495556620198790815011132229961233055330093259643777988927031615218528059568112195638833128963301562986216746843539195475581279209257068428089147621990110549558165349776752673950095753478203870734839284250665363614827748923709695207403042874565555089333727823275065690107725374975417643114290522162911989320926177926452539014789108015928782035648611189120454649598325660513611
message2=18702010045187015556548691642394982835669262147230212731309938675226458555210425972429418449273410535387985931036711854265623905066805665751803269106880746769003478900791099590239513925449748814075904017471585572848473556490565450062664706449128415834787961947266259789785962922238701134079720414228414066193071495304612341052987455615930023536823801499269773357186087452747500840640419365011554421183037505653461286732740983702740822671148045619497667184586123657285604061875653909567822328914065337797733444640351518775487649819978262363617265797982843179630888729407238496650987720428708217115257989007867331698397

m=gongmogongji(n1,message1,message2,e1,e2)
m=format(m,hex(m))
print( m)
#输出为16进制需用工具转为字符串
```

FLAG:

```
flag{49d91077a1abcb14f1a9d546c80be9ef}
```

RSA2

题目:

```
e = 65537
n = 248254007851526241177721526698901802985832766176221609612258877371620580060433101538328030305219918697643619814200930679612109885533801335348445023751670478437073055544724280684733298051599167660303645183146161497485358633681492129668802402065797789905550489547645118787266601929429724133167768465309665906113
dp = 905074498052346904643025132879518330691925174573054004621877253318682675055421970943552016695528560364834446303196939207056642927148093290374440210503657

c = 140423670976252696807533673586209400575664282100684119784203527124521188996403826597436883766041879067494280957410201958935737360380801845453829293997433414188838725751796261702622028587211560353362847191060306578510511380965162133472698713063592621028959167072781482562673683090590521214218071160287665180751
```

解答：dp攻击

```
from gmpy2 import*
from libnum import*

e = 65537
n = 248254007851526241177721526698901802985832766176221609612258877371620580060433101538328030305219918697643619814200930679612109885533801335348445023751670478437073055544724280684733298051599167660303645183146161497485358633681492129668802402065797789905550489547645118787266601929429724133167768465309665906113
dp = 905074498052346904643025132879518330691925174573054004621877253318682675055421970943552016695528560364834446303196939207056642927148093290374440210503657
c = 140423670976252696807533673586209400575664282100684119784203527124521188996403826597436883766041879067494280957410201958935737360380801845453829293997433414188838725751796261702622028587211560353362847191060306578510511380965162133472698713063592621028959167072781482562673683090590521214218071160287665180751

for i in range(1,e):                   #在范围(1,e)之间进行遍历
    if(dp*e-1)%i == 0:
        if n%(((dp*e-1)//i)+1) == 0:   #存在p，使得n能被p整除
            p=((dp*e-1)//i)+1
            q=n//(((dp*e-1)//i)+1)
            phi=(q-1)*(p-1)            #欧拉定理
            d=invert(e,phi)         #求模逆
            m=pow(c,d,n)               #快速求幂取模运算
print(hex(m))       #16进制转文本
```

FLAG：

```
flag{wow_leaking_dp_breaks_rsa?_98924743502}
```

异性相吸

题目：

```
key：asadsasdasdasdasdasdasdasdasdasdqwesqf
密文：ã哂■ 塔屋鞜卖到腡堂ؖ䉒嘅均✚瓤
```

解答：一开始以为是新佛曰密码解密无答案http://hi.pcmoe.net/buddha.html

用101Editor打开发现key和密文长度一致，看writeup 采用二进制异或得到结果后16进制转字符串

```
key = '011000010111001101100001011001000111001101100001011100110110010001100001011100110110010001100001011100110
1100100011000010111001101100100011000010111001101100100011000010111001101100100011000010111001101100100011000010
111001101100100011000010111001101100100011100010111011101100101011100110111000101100110'
cip = '00000111000111110000000000000000110000100000000010000010010010101010000000110001000000101010001011000010010110
1011100010110000100101001010110010100110100010001010010000000110100010000000001001011000010001100000001100101010000
1000111000000101010101100100011101010111010001000001001001011101010010100001010000011011'
flag = ''
for i in range(0,len(key)):
    if(key[i] == cip[i]):
        flag += '0'
    else:
        flag += '1'
flag = hex(int(flag,2))
print(flag)
```

FLAG:

```
flag{ea1bc0988992276b7f95b54a7435e89e}
```

RSA

题目：

```
两个文件pub.key和flag.enc
用101Editor打开pub.key得到：
-----BEGIN PUBLIC KEY-----
MDwwDQYJKoZIhvcNAQEBBQADKwAwKAIhAMAzLFxkrkcYL2wch21CM2kQVFpY9+7+
/AvKr1rzQczdAgMBAAE=
-----END PUBLIC KEY-----
```

在线网站**http://tool.chacuo.net/cryptrsakeyparse**进行分解

```
密钥类型RSA
密钥强度256
PN(e)65537
PN(n)
86934482296048119190666062003494800588905656017203025617216654058378322103517
DER格式
303c300d06092a864886f70d0101010500032b003028022100c0332c5c64ae47182f6c1c876d42336910545a58f7eefefc0bcaaf5af341ccdd0203010001
```

yafu大整数分解：操作步骤：C:\Users\Lenovo>E:\个人CTFTools\编码与密码\密码\RSA\RSA大整数分解\yafu-1.34\yafu-x64（文件所在地址）factor(86934482296048119190666062003494800588905656017203025617216654058378322103517)

得到

```
p = 285960468890451637935629440372639283459
q = 304008741604601924494328155975272418463
```

脚本解密：

```
import rsa
import gmpy2
e = 65537
n = 869344822960481191906660620034948005889056560172030256172166540583783221035 17
p = 285960468890451637935629440372639283459
q = 304008741604601924494328155975272418463
fn = (p-1)*(q-1)
d = int(gmpy2.invert(e,fn))
key = rsa.PrivateKey(n,e,d,q,p)          #在pkcs标准中,pkcs#1规定,私钥包含(n,e,d,p,q)
with open("flag.enc","rb") as f:
    f = f.read()
    print(rsa.decrypt(f,key))
```

注意：**flag.enc**必须放在该脚本所在文件夹且脚本名不能和**rsa**库重名

Unencode编码

UUencode编码

编码实例：

明文：Be slow to promise and quick to perform.

编码后：H0F4@小于VQO=R!T;R!P小于F]M:7-E(&%N9"!Q=6EC:R!T;R!P97)F;W)M+@``

https://www.qqxiuzi.cn/bianma/uuencode.php

题目：

```
89FQA9WMD<V1A<V1S83DY.#<W3$Q,2TM]
```

FLAG:

```
flag{dsdasdsa99877LLLKK}
```

RSAROLL

题目：data.txt

```
{920139713,19}

704796792
752211152
274704164
18414022
368270835
483295235
263072905
459788476
483295235
459788476
663551792
475206804
459788476
428313374
475206804
459788476
425392137
704796792
458265677
341524652
483295235
534149509
425392137
428313374
425392137
341524652
458265677
263072905
483295235
828509797
341524652
425392137
475206804
428313374
483295235
475206804
459788476
306220148
```

解答：

```
大数分解：得到p=18443，q=49891将p,q,e,c带入求m
```

```
import gmpy2
n = 920139713
e = 19
p = 18443
q = 49891
phi = (p-1) * (q-1)
d = gmpy2.invert(e,phi)
f = open('E:\文件\data.txt','r')
flag = ''
for lines in f.readlines():
    tmp = pow(int(lines),d,n)
    flag += chr(tmp)
print(flag)
f.close()
```

FLAG:

```
flag{13212je2ue28fy71w8u87y31r78eu1e2}
```

[AFCTF2018]Morse

题目：

```
-....\.----\-....\-....\-....\...--\-....\....-\-....\-....\-....\-...\...--\.----\-....\...--\..---\-....\-....
\....-\.....\..-.\-....\...--\...--\-----\.....\..-.\...--\...--\...--\....-\...--\.....\-....\----.\-....\-..
```

解答：在线解密http://www.txttool.com/t/?id=Mzg1得61666374667b317327745f73305f333435797d（666是不是很熟悉）

16进制转asii得flag

FLAG

```
afctf{1s't_s0_345y}
flag{1s't_s0_345y}
```