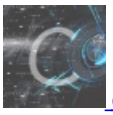
ctf--crypto(持续更新)

原创

小健健健 于 2020-10-09 13:26:46 发布

分类专栏： ctf 文章标签： 安全

本文链接：https://blog.csdn.net/superprintf/article/details/108974336



持续更新

基础视频

链接: https://pan.baidu.com/s/1eX42AbnJoLdXpbCbz9PV8A

密码: w2ic

链接: https://pan.baidu.com/s/18xtAME2ZTuXP31lSqMfiNA

密码: hq3w

工具

离线

CTFCrackTools

burpsuite

在线

ctf在线工具

ctfhub

密码学基础

密码学发展史

古典密码

1.凯撒加密

2.rot13加密(特殊凯撒加密key=13)

2.playfair加密

3.维吉尼亚加密(古典唯一需要密钥)

4.栅栏加密

6.培根加密(全都是由a,b组成)

7.猪圈加密(特殊图形组成)

8.卡尔达诺兰格码

现代密码

一.对称加密
DES
3DES (DES加密3次)
Blowfish
AES (取代DES算法)
IDEA
RC4
RC5
RC6

二.非对称加密
1.rsa
rsa数学基础
rsa加密
ctf中rsa的套路

编码

1.ascii
2.base64
3.url
4.html
5.unicode
6.utf-8
7.摩斯电码 (.和-组成)
8.二维码
9.jother (由[]{}()+!组成,浏览器console解码)
10.jsfuck (由()[]+!组成)

摘要

md5
sha1

其他

键盘加密(按照给定字符序列在键盘上顺序连接组成图形)

数学基础

威尔逊定理
欧拉定理

例题应用

1.(吉林大学ctf社团2020比赛)

```python
#baby math
from math import factorial
from badmonkey import flag
p = 67548091959834168893715184384042304643187712583625279732873340332656672001190994591841806466801694748478240191972568298261492222410900988459785704126597797
def my_wilson(x,p):
    return factorial(x)%p
res = my_wilson(p-2333,p)
mid = md5(str(res).encode()).hexdigest()
assert mid == "a3fe2bd4fb7c2f3642d57d67967c649b"
print("Spirit{{{}}}".format(res%(2**100)))
```

2.(吉林大学ctf社团2020比赛)

```python
# python3
from badmonkey import flag
message = bytes_to_long(flag)
enc = message ^ message>>23
print("enc = ",enc)
# enc = 696190889020604856890193198853561201348825165171326836202150445122902404137656377702109518236445
```

3.(吉林大学ctf社团2020比赛)

```python
from Crypto.Util.number import *
from badmonkey import flag
m = bytes_to_long(flag)
BITS = m.bit_length()
a,b,c,d = 15,27,19,23
mask1 = 369841549385560419960145110748416342072064655166160664909380673704115440043194206034053169640 1
mask2 = 346094936228413605327149191295215681128668637596516289923378317819143497614337880436441605691 0
def encrypt(y):
    y = y ^ y >> a
    y = y ^ y << b & mask1
    y = y ^ y << c & mask2
    y = y ^ y >> d
    return y&((2<<BITS)-1)
enc = encrypt(m)
print("enc = ",enc)
# enc = 105020280028875659488820786291928408604429365491842563619229179743634124315729301154059404979 8
```

4.lcg-5(lcg系列)

```python
from Crypto.Util.number import *
flag = b'Spirit{************************************}'

plaintext = bytes_to_long(flag)
length = plaintext.bit_length()

a = getPrime(length)
b = getPrime(length)
n = getPrime(length)

seed = plaintext
output = []
for i in range(10):
    seed = (a*seed+b)%n
    output.append(seed)

print("output = ",output)
# output =  [99972979862725109477663449594989753231360120757871207214243257750038403415526735894871348302984279976762380392141084943092972488023184271739094993470430272327679424224016751930100362045115374960494124801675393555642497051610643836, 67746128942473196452725786247650638758766438494159039738725366626480516682408824056405694482291885967976367955024718527852523623055558453351555018880878435253212386957166871512567178155189586705950539510840515712615136943375677027346821049033296095071476608523371102901038444464314877549948107134114941301290458464611872942706, 11755491858586722647182265446253701221615594136571038555321378377363341368427070357031882725576677912630050307145062, 77520702709056734908043447575890806532343756796575684280255998721553876434763065756131476813302275627124908054923457754745340793606649602871190615837661809359377788072256203797817090151599031273142680590748, 28024400819186045905025961461136700942626009520206871846596053076951511205898169430513225030943635789167734140046625627226318035765837286789021891141596394835871645925685252241680021740265826179768429792645576780380635014113687982]
```

所有题的答案