HGAME 2022 Week3 writeup by sasasas

HGAME 2022 Week3 writeup by sasasas
- CRYPTO
  - Block Cipher
  - Multi Prime RSA
  - RSA Attack 3

CRYPTO

Block Cipher

1.看一看py文件，发现是以8个字符为单位的异或加密

task.py

```python
from functools import reduce
from secret import flag


def pad(s):
    padding_length = (8 - len(s)) % 8
    return s + chr(padding_length) * padding_length


def xor(a, b):
    assert len(a) == len(b)
    return bytes(map(operator.xor, a, b))


def encrypt(s):
    iv = bytes(random.randint(0, 255) for _ in range(8))
    key = bytes(random.randint(0, 255) for _ in range(8))
    parts = list(map(str.encode, map(pad, re.findall(r'.{1,8}', s))))
    results = []
    for index, part in enumerate(parts):
        results.append(reduce(xor, [part, iv if index == 0 else results[-1], key]))
    return iv, key, results

iv, key, parts = encrypt(flag)
print(f"iv = {iv}")
print(f"key = {key}")
print(f"parts = {parts}")
```

2.把密钥，密文翻译成数字，写一个程序异或解密，得flag

output.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
iv = b'Up\x14\x98r\x14%\xb9'
key = b'\r\xe8\xb86\x9c33^'
parts = [b'0\xff\xcd\xc3\x8b\\T\x8b', b'RT\x1e\x89t&\x17\xbd', b'\x1a\xee\x8d\xd6\x9b>w\x8c', b'9CT\xb3^pF\xd0']
```

未命名1.cpp

```cpp
#include<stdio.h>
int main()
{
    int tmp[]={'U','p',20,152,'r',20,'%',185};
    int key[]={13,232,184,'6',156,'3','3','^'};
    int parts[]={'0',255,205,195,139,'\\','T',139,'R','T',30,13
    for(int i=0;i<32;i++)
    {
        printf("%c",tmp[i%8]^key[i%8]^parts[i]);
        tmp[i%8]=parts[i];
    }
}
```

Multi Prime RSA

1.与普通的RSA区别在，它的n不由两个大素数生成，而是多个素数的多次方相乘

task.py

```python
from Crypto.Util.number import getPrime
from libnum import s2n
from secret import flag

p = getPrime(256)
q = getPrime(256)
r = getPrime(256)
s = getPrime(256)
n = p ** 2 * q ** 3 * r ** 5 * s ** 7
e = 65537
c = pow(s2n(flag), e, n)
print(f"p = {p}")
print(f"q = {q}")
print(f"r = {r}")
print(f"s = {s}")
print(f"n = {n}")
print(f"e = {e}")
print(f"c = {c}")
```

2.先计算n的欧拉函数，再根据这个计算d

```python
def extendedGCD(a, b):
    if b == 0:
        return 1, 0, a
    else:
        x, y, q = extendedGCD(b, a % b)
        x, y = y, (x - (a // b) * y)
        return x, y, q

def computeD(fn, e):
    (x, y, r) = extendedGCD(fn, e)
    if y < 0:
        return fn + y
    return y

p = 617899321487194773840274583333805689780562861361378290929523173077119083534 77
q = 912079693533557636856332843788335063197947145070273329292907017487275341938 61
r = 105471299607375388622347272479207944509670502835651250945203397530010861809367
s = 831532387489037724481383075055797992771626521512444773914651305042671718814 37
N = (p ** 2 - p) * (q ** 3 - q ** 2) * (r ** 5 - r ** 4)* (s ** 7 - s ** 6)
n = 103934437216508710000106392059815181232415106468484184525097475852526514856770610378495842487 3
e = 65537
d=computeD(N,e)
f=open("1.txt","w")
print(f"d = {d}",file = f)
```

1.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
d = 47135806383402839291135727677523029992063136769401817789263273834456766018780014028741359046271333263 8
96785926584722167605153722923920471968987751723812070539733697446966512856272851376678902660263817876657 93
```

3.然后根据d,n在工具里解密c,得到flag

RSA Attack 3

1.RSA 大e 维纳攻击

```
n = 5074191700883449329907022569116947884084939687495276144216145686129441447648897172294440208136588933629
261167277014748183012844440603384989647664190074853086693408529737767147592432979469020671772152652865219 0
e = 7731019986744867778208157210934347278378113564171259764359712259144301122909153351675892523894975549139
344472122486488695145850478714420604126221642768947662383838946937593475909779263065810803906853606154077 6
c = 1652517299173945297931633443008489923940213374294747897118050416551168457224803016778171650532536550274
612728022444370874223001778580387635197325043524719396707713385963432915855227152371800527536048555551237 7
```

2.放工具跑一下，得flag