攻防世界crypto 新手区攻略

原创

ZSL13213636450 于 2020-03-22 18:13:07 发布 2023 收藏 6

文章标签： 密码学

本文链接：https://blog.csdn.net/weixin_46329549/article/details/105031888

文章目录

前言：

crypto主要是针对密码学的题，要想把crypto做好，就必须要对各种密码学进行研究。

1.base64

第一关较为简单，直接使用base64进行解密即可。
cyberpeace{Welcome_to_new_World!}

2.Caesar

第二关用到了凯撒码，

直接使用凯撒密码解密即可

3.Morse

已经提示，使用摩斯码解密即可。(摩斯码相关内容可以百度）
1变为 - ，0变为 .
题目上也给出了flag的格式，变换即可。

4.混合编码

这道题混合编码，主要用到了base64与unicode
使用unicode编码转换

注意flag的格式。

5.Railfence

根据题目提示是栅栏密码，题目上面提示到了5，所以是分为5行，使用解密工具，flag直接就出来了。

6.不仅仅是Morse

这道题对文本进行了变换，题目也提示不简单的是morse密码，经过观察，发现可以将 / 换为空格，转化为标准的morse码，然后进行morse解密，得到一串类似培根加密后的密文，对培根码解密即可得到flag。

7.幂数加密

打开文件进行分析是云影密码，（云影密码就是用0作为间隔，然后把所得数字相加，再对应相应的26个字母，即可得到flag）。

884210122048022440401422420248012 2
88421 122 48 2244 4 142242 248 122
23 5 12 12 4 15 14 5
w e l l d o n e
根据题目要求修改flag。

8.easy_RSA

这道题是RSA算法。
直接给出代码
import gmpy2
p = 473398607161
q = 4511491
e = 17
s = (p-1)*(q-1)
d = gmpy2.invert(e,s)
print(‘flag is :’,d)
得到flag：cyberpeace{125631357777427553} 。

9.easychallenge

这道题是将python的py程序编译成的中间式文件，需要我们将其反编译成我们可读的python代码，可以利用在线反编译工具直接反编译代码。
代码出来之后，还要利用base64进行解密。
解密之后，得到flag。

10.Normal RSA

这道题暂时没有思路，以后进行补充。

11.转轮机加密

这道题是转轮机加密，首先要明白转轮机工作：原理转轮密码机由多个转轮构成，每个转轮旋转的速度都不一样，比如有3个转轮，分别标号为1,2,3，其中1号转轮转动26个字母后，2号转轮就转动一个字母，当2号转轮转动26个字母后，3号转轮就转动1个字母。因此，当转轮密码机转动26X26X26次后，所有转轮恢复到初始状态，即3个转轮密码机的一个周期长度为26X26X26（17576）的多表代换密码。

这道题自己做会非常复杂，直接找出大佬的代码

```python
#!/usr/bin/env python3
# -*- coding:utf-8 -*-

import re

sss = '1: < ZWAXJGDLUBVIQHKYPNTCRMOSFE < 2: < KPBELNACZDTRXMJQOYHGVSFUWI < 3: < BDMAIZVRNSJU
m = 'NFQKSEVOQOFNP'
# 将sss转化为列表形式
content=re.findall(r'< (.*?) <',sss,re.S)
# re.S:DOTALL，此模式下，"."的匹配不受限制，可匹配任何字符，包括换行符
iv=[2,3,7,5,13,12,9,1,8,10,4,11,6]
print(content)
vvv=[]
for i in range(13):
    index=content[iv[i]-1].index(m[i])
    vvv.append(index)
print(vvv)

for i in range(0,26):
    flag=""
    for j in range(13):
        flag += content[iv[j]-1][(vvv[j]+i)%26]
    print(flag.lower())
```


12.ease ECC

这道题是ECC 椭圆曲线加密

暂时不会。