dis

发表于 2021-01-25 更新于 2021-02-16 分类于 Challenge， 2020， 工业信息安全技能大赛， 哈尔滨站
Challenge | 2020 | 工业信息安全技能大赛 | 哈尔滨站 | dis

点击此处获得更好的阅读体验

WriteUp来源

来自MO1N战队

题目描述

> *某程序上残留下的一个程序字节码，请您帮助分析。flag格式为：flag{}。*

题目考点

- *pyc逆向*

解题思路

逐条还原python语句

```
1  a = raw_input("Input Your Password:")
2  a = '0x'+a.encode('hex')
3  a = int(a,16)
4  b = 65537
5  c = 10853984726857399027523402435467243724652508507660551696032000572274158989864 1
6  a=a%c
7  ans=1
8  while b!=0:
9      if b&1:
10         ans=(ans*a)%c
11     b>>=1
12     a=(a*a)%c
13 if ans == 19768389376732605541278069478730687959201475928791774076030532997986175692691:
14     print 'correct'
15 else :
16     print 'error'
```

分析后发现就是个RSA加密的过程

其中n可以被很容易的分解

解密一下就可以了

```
1  import gmpy2
2  p = 32559318041180174235672726412725375893 9
3  q = 33336032140260317826387959596800416921 9
4  e = 65537
5  c = 19768389376732605541278069478730687959201475928791774076030532997986175692691
6  fi = (p-1)*(q-1)
7  n = p*q
8  d = gmpy2.invert(e,fi)
9  m = pow(c,d,n)
10 print hex(m)[2:].decode('hex')
```

Flag

```
1 flag{RSA_i5_Safe}
```

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2020/工业信息安全技能大赛/哈尔滨站/tXudnSjivQFbTPSju4cPGM.html*

 # Challenge # 2020 # 工业信息安全技能大赛 # 哈尔滨站
justplay
Modbus协议分析