

Weak 1

- ## 1. Misc 签到题

Base64 解密后进行摩斯电码解密即可。

- ## 2. Crypto infantRSA

通过查询后用 python 计算私钥后 根据 RSA 解密原理直接可由
密文, 私钥, 模数得出明文
后 m.to_bytes() 直接转化出 flag

The screenshot displays a PyCharm IDE with a Python script named `666.py` open. The script implements the RSA algorithm, including functions for calculating the greatest common divisor (gcd) and the modular inverse (modinv). The main execution block calculates the product of two primes (p and q), the totient (phi), the private key (d), and the message (m). It then prints the result of the modular inversion and the encrypted message.

```

1 def egcd(a, b):
2     if a == 0:
3         return (b, 0, 1)
4     else:
5         g, y, x = egcd(b % a, a)
6         return (g, x - (b // a) * y, y)
7
8 def modinv(a, m):
9     g, x, y = egcd(a, m)
10    if g != 1:
11        raise Exception('modular inverse does not exist')
12    else:
13        return x % m
14
15 e=13
16 p = 681782737458022065655472455411
17 q = 675274897132088253519831953441
18 d=modinv(e,(p-1)*(q-1))
19 print(d)
20 m=pow(2756984650823610745173688411496311542172902608559859019841,141658607814768364339375366617699419709389378231351875726277,460390767897997184102969941508880171690097589571068900519251)
21 print(m.to_bytes(22,'byteorder='big'))

```

The output console shows the execution path and the final encrypted message:

```

Run: TicTacToe
C:\Program Files\Python37\python.exe C:\Users\29679\Desktop\TicTacToe\TicTacToe\666.py
141658607814768364339375366617699419709389378231351875726277
390621104726693889143894280064807335236334831991333245
b'hgame(t3Xt600K_RSA!!!!)'
Process finished with exit code 0

```

- ### 3. Web Cosmos 的博客

通过查找资料与提示发现 为 git 源码泄露 后进入 github 得到 flag

