CRYPTO

白给的rsa

已知n，e，c。通过深入的学习rsa后，知道了c是密文，n和e组成了公钥，n和d组成了私钥。那么我们想要破解，就要知道d，要知道d就要知道phi，所以我们得先把n给分解了，通过网站http://www.factordb.com我们成功地在线分解n，那么一切都简单了。python能算大数，我们可以用gmpy2库中的invert函数算出d，最后通过算式pow(c，d，n)，当然，外面还得有一个大括号，括号外的函数可以是libnum.n2s也可以是to_bytes，后者更复杂一些，一发入魂，拿到了flag。可惜本周只做了一道题，感觉竞争好激烈啊。