b06705001 資管 3 楊力行 b06705001

0x0a

看到要解的是 RSA 加密 ， 且題目可以把解密後的結果的後四位元 leak 出來，就猜到是要用 lsb oracle 來解，因此我先把 leak 出的 4 位元再取最後一 bit 像課堂上教的一樣去解，但發現他有限制次數，因此只能 4 位元一起處理，把課堂教的改成 16 去進行次方，以使後 4 位清零，接著再把 N 取出他的後四位，在每次都把 16 減掉(n 的後四位乘上 0 – 15 再 mod 16)mod 16 去和得到的 m 比較，一樣就假設 m 在這一段中，不斷做，直到找到，再用 long_to_bytes 就解出來，但是我的程式不知為何要跑好多次才能正確一次(猜測與 MOD16 碰撞有關)，並且最後一位因為浮點數的關係永遠無法正確解出}。