HW4 of Introduction to Information Security 2018

Deadline: 12/13 23:55

實作出 RSA 加解密(bit 指的是 n 的長度)

70 分標準：

1. 小數字的 RSA 加解密（part1 slide p.38, e 請在所有符合條件的值中選一個使用）

Ex. p=71, q=83, Plaintext=2018 => Ciphertext=2221

100 分標準(第一項 12 分，其餘每項 6 分)：

1. 1024 bit 的 RSA 加解密
2. 產生大質數 (part 2 slide p.15)
3. Square & multiply
4. Chinese Remainder Theorem (speed up!)

plaintext 不可寫死

Note:

1. 本次作業是個人作業
2. 上傳到 moodle 需附上說明文件（規格和前幾次作業同），請壓縮成一個檔案，檔名格式為 HW4_學號
3. 上方的測資為範例，實際測試時會有其他測資，因此即使只寫了 70 分的內容，也不可以將值寫死