

RSA 100分標準實作 [張家成]

A10615003 張家成 二資工四

RSA algorithm [Java]

- 建置環境

- MacOS Mojave 10.14.1
- Eclipse IDE for Java Developers [Version: Oxygen]
- Java SE 9.0.1

- 執行結果截圖

```
<RSA Encryption & Decryption>
Please input the plaintext:(eg.1123)
1123
decimal p = 100781237066647151305797658506909519407836788268874716284608726
decimal q = 113977769293907709375668724179258749213447466584791011345297246
n = 11486820587536929150344757183739523126332613634586577550299652627982781
φ(n) = 11486820587536929150344757183739523126332613634586577550299652627982
-----Encryption-----
e = 7
c = m^e mod n
Ciphertext: 2252466257338241800747
-----Decryption-----
d = 82048718482406636788176837026710879473804383104189839644997518771305581
m = c^d mod n
Plaintext: 1123
```

- 困難與心得

- 大數的操作不太熟悉，經過多次練習後熟悉了許多。