RSA 鑰匙配對驗證

驗證推演結果

- 公開鑰匙：$K_U = \{e, n\} = \{5, 119\}$ 、私有鑰匙：$K_R = \{d, n\} = \{77, 119\}$
- 驗證結果：假設明文 M = 19 ， e=5、d=77
  - 加密編碼：**$C \equiv M^e \bmod n \equiv 19^5 \bmod 119 \equiv 66 \bmod 119$**，則密文為 **66**。

    演算過程如下：

$$19^2 = 361 \equiv 4 \bmod 119$$

$$19^4 \equiv 4 \times 4 = 16 \equiv 16 \bmod 119$$

$$19^5 = 19^4 \times 19^1 = 16 \times 19 = 304 = 66 \bmod 119$$

  解密編碼：$M \equiv C^d \bmod n \equiv 66^{77} \bmod 119 \equiv 19 \bmod 119$，則明文為 19。

演算過程如下：

$$66^2 = 72 \bmod 119$$

$$66^4 = 72 \times 72 = 5184 = 67 \bmod 119$$

$$66^8 = 67 \times 67 = 4489 = 86 \bmod 119$$

$$66^{16} = 86 \times 86 = 7396 = 18 \bmod 119$$

$$66^{32} = 18 \times 18 = 324 = 86 \bmod 119$$

$$66^{64} = 86 \times 86 = 7396 = 18 \bmod 119$$

$$66^{77} = 66^{64} \times 66^8 \times 66^4 \times 66 = 6845256 = 19 \bmod 119$$