**COMP90043: Cryptography and security**
**Week 6: Workshop Questions**

**Preparation:**

(1) Try at home before coming to workshop] Perform encryption and decryption using the RSA algorithm, as in Figure 9.5 (of teh textbook), for the following:
   (a) p = 3; q = 11, e = 7; M = 5
   (b) p = 5; q = 11, e = 3; M = 9
   (c) p = 7; q = 11, e = 17; M = 8
   (d) p = 11; q = 13, e = 11; M = 7
   (e) p = 17; q = 31, e = 7; M = 2

**Questions: Part A**

(1) State Fermat's and Euler's theorems. Using these two theorems simplify the following equations.
   (a) $4^{12} \pmod{21}$.
   (b) $2^{22} \pmod{23}$
   (c) $3^{17} \pmod{17}$
   (d) $5^{35} \pmod{17}$
   (e) $73^{10001} \pmod{101}$

(2) CRT Question. Solve for $x$ satisfying the following simultaneous congruences:

$$x \equiv 7 \pmod{11},$$
$$x \equiv 9 \pmod{13}.$$

(3) CRT Question. Solve for $x$ satisfying the following simultaneous congruences:

$$x \equiv 2 \pmod{3},$$
$$x \equiv 3 \pmod{5},$$
$$x \equiv 2 \pmod{7}.$$

(4) Assume that Alice chooses two primes 43 and 47 to construct her RSA key prime factors. Help her to set up public and private keys and demonstrate encryption and decryption with an example. Choose the smallest possible exponent for the public key.

(5) Demonstrate CCA attack on textbook RSA with an example.

(6) Suppose we have a set of blocks encoded with the RSA algorithm and we dont have the private key. Assume n = pq, e is the public key. Suppose also someone tells us they know one of the plaintext blocks has a common factor with n. Does this help us in any way?
(7) Explain how you can use RSA encryption function to construct a digital signature scheme.
(8) With RSA, discuss how the concept of Blinding can be implemented?