Public Key Encryption: Part 1

IMPORTANT NOTES: Study lecture materials at least 1 hour and prepare Question 1-3 prior to the tutorial session. Prepared questions will be discussed in the tutorial session.

1. What are the essential ingredients of an asymmetric / public-key cipher?
2. What is the difference between the public key and the private (secret) key? Why the public-key cryptosystem is still secure even after giving the public key to the attacker?
3. Write the following composite numbers as a multiplication of their prime factors.
   (a) 12
   (b) 78
   (c) 99
   (d) 128
4. Complete the following modular arithmetic operations and determine the result:
   (a) $(12 + 8) \bmod 6$
   (b) $(2 \times 12) \bmod 6$
   (c) $(20 + 125) \bmod 5$
   (d) $(20 - 35) \bmod 5$
   (e) $10^4 \bmod 3$
   (f) $10^{-1} \bmod 31$
   (g) $13^{-1} \bmod 19$
5. Using the "Square and Multiply" modular exponentiation algorithm calculate the following:
   (a) $71^{56} \bmod 11$
   (b) $58^{66} \bmod 31$