# FIT2093: Tutorial 7

## Public Key Cryptography

### Review

1. What are the essential ingredients of an asymmetric cipher?
2. List and define three uses of a public key cryptosystem.
3. What is the difference between a private key and a secret key?
4. How can public key encryption be used to distribute a secret key?
5. What is a public-key certificate?
6. Briefly explain Diffie-Hellman key exchange.
7. How many keys are required for two people to communicate via an asymmetric cipher? How many keys are required for n people to communicate with each other securely?

### Problems

1. Assume that Alice and Bob live in the 21st century and have access to encryption technology. What are Alice's options to securely send the recipe to Bob? Discuss the potential security threats for each of the options.
2. Perform encryption and decryption using RSA algorithm (where $n = p*q$; $C= M^e \bmod n$ ; $P = C^d \bmod n$; $e*d \bmod \phi(n) = 1$; plaintext M & Ciphertext C; e & d are public and private key.) for the following:
   a. $p=3$; $q=11$; $e = 7$; $M = 5$;
   b. $p =5$; $q = 11$; $e = 3$; $M = 9$;
3. In a public-key system using RSA, you intercept the ciphertext $C = 10$ sent to a user whose public key is $e = 5$, $n = 35$. What is the plaintext M?
4. Users A and B use the Diffie-Hellman key exchange technique with a common prime $p=11$, primitive root $g= 2$;
   a. $a = 6$ (A's private key), what is $A = g^a \bmod p$ (A's public key)?
   b. If $B = g^b \bmod p$ (B's public key) = 3, what is the shared secret session key?
   c. What is b, B's private key?