# SENG2250/6250 System and Network Security
# Self-Quiz Week 3, Semester 2, 2020

**True/False Questions**.

1. Key management is just a mechanism to store the secret keys.
   False. Key management is a complex system that offers services including key generation, registration, distribution, storage, updating, deletion, recovery, and archiving.

2. Key establishment is a mechanism to create a secret key that shares between users.
   True.

3. Key agreement protocol runs between two users and a trusted third party who exchange secret information between users.
   False. Key agreement/exchange allows users cooperatively agree on a shared secret as a result of the protocol. An (online) trusted third party is not required.

4. Diffie-Hellman kay agreement protocol is secure against man-in-the-middle attacks.
   False. Refer to lecture slides L3-S28 and the short video.

5. Symmetric-key based key agreement protocols (e.g., NS protocol) cannot provide perfect forward secrecy.
   True.

6. Public key infrastructure is a set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke public key certificates.
   True.

7. Cross-certification is a mutual authentication between users who have different certificates.
   False. Cross-certification allows two certificate authorities (CA) to certify each other. This facilitates the X.509 Hierarchy that users subscribed from different CAs can be verified.

8. Self-signed certificate should never be used because it is not secure against man-in-the-middle attacks.
   False. A self-signed certificate is typically used by a root CA which has to certify itself before providing services. But this is a special case, and we should not use a self-signed certificate in most security applications.

**Short-Answer Questions**

9. Explain two ways to prevent replay attacks.
   - Timestamp. We can add a timestamp in an (authenticated) message that can indicate the time of generation. It requires time synchronisation prior to use.

- Challenge-response mechanism. Use a nonce as a challenge of a session, and the response must be about the “fresh” nonce. It does not require time synchronisation.

10. Find a solution to man-in-the-middle (MITM) attacks of Diffie-Hellman key agreement. (Hint: use public key certificate)
    The reason for MITM attacks is the lack of key/message authentication. A solution is to use certified public keys. Along with the exchanged public key keys, a valid certificate should be sent as well. Then, the recipient should verify the public key before the shared key computation. Therefore, the adversary cannot impersonate other users before he does not have the correct public (and private) key.