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.

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

3. Key agreement protocol runs between two users and a trusted third party who exchange secret information between users.

4. Diffie-Hellman kay agreement protocol is secure against man-in-the-middle attacks.

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

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.

7. Cross-certification is a mutual authentication between users who have different certificates.

8. Self-signed certificate should never be used because it is not secure against man-in-the-middle attacks.

Short-Answer Questions

9. Explain two ways to prevent replay attacks.

10. Find a solution to man-in-the-middle (MITM) attacks of Diffie-Hellman key agreement. (Hint: use public key certificate)