정보통신대학원 GITG 312: Crypto Basics and Network Security
Exercise
Spring 2020

1. One of the desirable properties of the cryptographic hash functions is ‘irreversibility’. Describe ‘irreversibility”.
2. Describe how ‘server authentication’ is performed in the SSL/TLS system.
3. IPsec and SA
   a) Briefly describe the Security Association in the IPsec protocol.
   b) Describe the (state) information maintained by the sending/receiving entity of a security association.
4. Describe briefly the DTLS protocol.
5. Describe the role of nonce used to combat the replay attack. Include in your answer the description on explaining how the nonce works to do its role.
6. Describe the man-in-the-middle attack.
7. List some common symmetric ciphers or encryption algorithms used in the SSL/TLS.
8. Explain the role of the sequence number embedded in the SSL/TLS record.
9. Describe the truncation attack in SSL/TLS
10. Describe the works achieved over the handshake phase of the SSL/TLS protocol.