정보통신대학원 GITG 312: Crypto Basics and Network Security

Exercise Fal 2020

1. One of the desirable properties of the cryptographic hash functions is ‘ireversibilty’. Describe ‘ireversibilty”.

2. Describe how ‘server authentication’ is performed in the SL/TLS system.

3. IPsec and SA

a) Briefly describe the Security Asociation in the IPsec protocol.

b) Describe the (state) information maintained by the sending/receiving entiy of a security

asociation.

4. Describe briefly the DTLS protocol.

5. Describe the role of nonce used to combat he replay atack. Include in your answer the description on

explaining how the nonce works to do its role.

6. Describe the man-in-the-midle atack.

7. List some common symmetric ciphers or encryption algorithms used in the SL/TLS. 8. Explain the role of the sequence number embeded in the SL/TLS record.

9. Describe the truncation atack in SL/TLS

10. Describe the works achieved over the handshake phase of the SL/TLS protocol.