정보통신대학원 GITG 312: Network Security
Fall 2015

Exercise

1. Describe the 'Cipher Block Chaining'.
2. List some popular hash functions used for message authentication.
3. Determine the private key when p = 5, q = 7, and public key is (35, 11) assuming that RSA algorithm is being used.
4. Describe the desirable properties of the cryptographic hash functions.
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. *Briefly* describe the man-in-the-middle attack.
7. List some common symmetric ciphers or encryption algorithms used in the SSL.
8. Explain the role of the sequence number embedded in the SSL record.
9. Describe the truncation attack in SSL
10. Describe the key differences briefly between TLS and DTLS.
11. Describe the information maintained/required by an IPsec security association (SA).