M. E. (ICE) 2nd Semester Examination, 2012

Information & System Security (ICE 1003)

Time: 3 hours
Full Marks: 70

Answer any five questions

1. Why is confidentiality an important principle of security? Explain the principle of symmetric key cryptography. Why there is no need to keep the symmetric encryption algorithms secret? What are the advantages and disadvantages of Caesar cipher? What are the disadvantages of substitution cipher? Explain why both substitution and transposition cipher can be thought of as permutations.

2+3+2+3+2+2

2. Describe the different types of cryptanalytic attacks based on what is known to the attacker. Are all stream ciphers monoalphabatic? Explain. What is the difference between monoalphabatic and polyalphabatic cipher? How many possible keys does a playfair cipher have? Express your answer as an approximate power of 2.

6+2+3+3

3. Define P-box and its three variations. Describe differential cryptanalysis attack. Let M' be the bitwise complement of M. prove that if the complement of plaintext block is taken and the complement of an encryption key is taken,then result of encryption with these values is the complement of the original cipher text. That is ,

   If $Y=DES_K(X)$
   Then $Y'=DES_{K'}(X')$.

5+5+4

4. Explain the known-plaintext attack on triple DES with two keys. How key expansion is performed in AES. Why do we have only one S-box in AES, but several in DES? State the characteristics of Blowfish.

4+5+3+2

5. Why modes of operation are needed if modern block ciphers are to be used for encipherment? Why do some block cipher modes of operation use encryption function while others use both encryption and decryption? What are the advantages and disadvantages of ECB mode of operation? Show why CFB mode creates a non-synchronous stream cipher, but OFB mode create a synchronous one. What is the difference between link and end-to-end encryption?

2+3+3+3+3

6. Describe four general schemes for distribution of public key. In Diffie-Hellman algorithm sender and receiver choose two random number x and y. consider that x and y are same number, do the session keys calculated by sender and receiver have same value? Give an example to prove your claims. What is the difference between session key and master key. What are the disadvantages of symmetric key cryptography?

5+4+3+2

7. Explain how public key cryptography is used for authentication and secrecy. Describe the possible attacks on RSA algorithm. Compare MD-5 with SHA-1. What are the different approaches of message authentication.

4+5+3+2

8. Describe the brute-force attack on message authentication code. Explain the handshake protocol in SSL. How is screened host firewall, dual-homed bastion different from screened host firewall, single homed bastion? Give the limitation of firewall.

4+5+3+2