M. E. (ICE) 2nd Semester Examination, 2013

Information & System Security (ICE 1003)

Time: 3 hours
Full Marks: 70

Answer any five questions

1. Define different security services. Compare active and passive security attacks. What is poly-alphabetic cipher? How is it different from Caesar cipher? Are all stream ciphers mono-alphabetic? Explain.

   4+3+2+2+3

2. Why modern block ciphers are designed as substitution ciphers instead of transposition ciphers? Explain linear cryptanalysis attack. Perform brute-force attack on transposition cipher. Use a brute-force attack to decipher the following message: 'xpalasxy'. Assume that you know it is an affine cipher and the plaintext 'ab' is enciphered to 'gl'.

   3+4+3+4

3. Show the set of permutation tables for a 3-bit block transposition cipher where the block size is 3 bits. What is the difference between diffusion and confusion? How is it achieved in DES? What is the need of hierarchical KDC? Explain the mechanism of symmetric key distribution (without KDC) such that confidentiality and authentication is maintained.

   3+4+3+4

4. Show that in DES the first 24 bits of each subkey come from the same subset of 28 bits of the initial key and second 24 bits of each subkey come from a disjoint subset of 28 bits of the initial key. Describe meet-in-the-middle attack on double DES. Why AES is considered as byte-oriented technique? Briefly explain the mix columns operation in AES.

   4+4+2+4

5. How the subkey for each round of IDEA algorithm is generated? Where can we use ECB mode of operation? Explain the ciphertext stealing technique in CBC mode during encryption and decryption. Compare CTR mode to OFB and ECB mode.

   4+2+4+4

6. What is trapdoor one way function? Explain ElGamal cryptosystem and show the correctness of this cryptosystem. Perform chosen ciphertext attack on RSA. How can we prevent timing attack of RSA?

2+5+4+3

7. How symmetric encryption is used to produce message authentication? What are the difference between encryption and MAC function? Consider the messages are in the form of a sequence of decimal numbers, M=(a_1, a_2,.... a_n). The hash value is calculated as $\Sigma\ a_i$ for some predefined value n. Does this hash function satisfy the requirements of hash function? What are the possible attacks on MD-5?

5+2+4+3

8. Why is base-64 encoding useful in e-mail application? Also explain base-64 encoding. Describe the alert protocol in SSL. List the design goals of firewall. What are the attacks on packet filter? How can we overcome those attacks?

4+3+2+5