

--	--	--	--	--	--	--	--	--	--

Third Semester M.Tech. Degree Examination, June 2012
Information Security

Time: 3 hrs.

Max. Marks: 100

Note: Answer any FIVE full questions.

- 1 a. What is information security? Define the seven critical characteristics of information. (08 Marks)
b. With a neat diagram, explain the various phases of Sec SDLC. (12 Marks)
- 2 a. List the major process steps in the Plan-Do-Check-Act cycle of information security management system. (10 Marks)
b. Name the different categories of firewalls based on processing mode. Discuss the three subsets of the packet filtering firewall. (10 Marks)
- 3 a. Define the following:
(i) Host based IDPS (ii) Network based IDPS
(iii) Honey-Pot (iv) Padded cell
(v) Active vulnerability scanner. (10 Marks)
b. List the five areas addressed by the Network management model. Indicate the objects of each of the five domains of the maintenance model. (10 Marks)
- 4 a. Differentiate between passive and active security attacks. (06 Marks)
b. What is cryptanalysis? What are the various types of cryptanalytic attacks? (06 Marks)
c. Compare DES, 3DES and AES. (08 Marks)
- 5 a. What requirements must be met by a hash function? (06 Marks)
b. Describe the RSA public key encryption algorithm. (08 Marks)
c. Perform encryption and decryption using RSA for : $p = 3$, $q = 11$, $e = 7$, $M = 5$. (06 Marks)
- 6 a. What are the technical deficiencies of Kerberos version and authentication service and how are they addressed in version 5. (10 Marks)
b. Describe the sequence of steps in providing
i) AUTHENTICATION and ii) CONFIDENTIALITY services by PGP. (10 Marks)
- 7 a. With neat diagrams, describe the basic combination of security associations. (10 Marks)
b. What is SSL? Illustrate the SSL Handshake protocol action with a neat diagram. (10 Marks)
- 8 Write short notes on:
a) VPN b) Stream ciphers
c) SET d) Malware. (20 Marks)

* * * * *

Important Note : 1. On completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages.
2. Any revealing of identification, appeal to evaluator and /or equations written eg. 42+8 = 50, will be treated as malpractice.