USN | | | | | | | | | | |

12SCN14

First Semester M.Tech. Degree Examination, February 2013
Information Security

Time: 3 hrs. Max. Marks:100

Note: ***Answer any FIVE full questions.***

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.

1 a. Compare top-down and bottom-up approach to implement security. **(04 Marks)**

b. Define the following keyterms:
   i) Hacking
   ii) Security blueprint
   iii) Threats
   iv) Vulnerability. **(04 Marks)**

c. What are the types of security policies? Where would each be used? **(07 Marks)**

d. What are the three components of the C.I.A triangle? What are they used for? **(05 Marks)**

2 a. Describe firewall architectures. **(07 Marks)**

b. What are honey pots, honey net and padded cell systems? **(05 Marks)**

c. Define the following terms:
   i) Signature based IDS
   ii) Statistical anomaly based IDS
   iii) Network based IDS
   iv) Host based IDS. **(04 Marks)**

d. What is RADIUS? What advantage does it have over TACACS? **(04 Marks)**

3 a. What is the purpose of S-boxes in DES? **(04 Marks)**

b. Summarize the various types of cryptoanalytic attacks based on the amount of information known to the cryptoanalyst. **(04 Marks)**

c. Compare stream cipher and block cipher. **(04 Marks)**

d. Explain block cipher modes of operation. **(08 Marks)**

4 a. Compare convectional encryption and public key encryption. **(04 Marks)**

b. Write the possible approaches to attack the RSA algorithm. **(03 Marks)**

c. Describe the Diffe-Hellman key exchange algorithm. **(10 Marks)**

d. What are the applications for public – key cryptosystem? **(03 Marks)**

5 a. With a neat diagram illustrate the overall operation of HMAC. **(10 Marks)**

b. What is the purpose of X.509? **(03 Marks)**

c. Write the summary of notations used in PGP. **(03 Marks)**

d. Draw the general format of the PGP message and explain in brief. **(04 Marks)**

6 a. Draw the format of encapsulating security payload [ESP] and explain in brief. **(04 Marks)**

b. List out and explain the key features of secure electronic transaction [SET]. **(08 Marks)**

c. Write the services provided by IP security. **(04 Marks)**

d. With a neat diagram, explain SSL record protocol operation. **(04 Marks)**

7 a. With a neat diagram, explain SSL handshake protocol. **(08 Marks)**
b. What is S/MIME? Explain in brief. **(04 Marks)**
c. Compare transport mode and tunnel mode functionality in IP security. **(04 Marks)**
d. Write a summary of Kerberos version 4 message exchange. **(04 Marks)**

8 Write short notes on:
a. RSA algorithm
b. Digital signature
c. Packet-filtering router
d. Passive and active security attacks. **(20 Marks)**

* * * * *