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

12SCS31

Third Semester M.Tech. Degree Examination, Dec.2013/Jan.2014

Information Security

Time: 3 hrs. Max. Marks:100

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

1 a. Define information security. Briefly explain the characteristics of information. **(10 Marks)**

b. Explain the different phases of the security systems development life cycle. **(10 Marks)**

2 a. Briefly explain the criteria a policy must meet to be effective and legally enforceable. **(04 Marks)**

b. Explain the different firewall architectures with necessity diagrams. **(12 Marks)**

c. Write a short note on packet sniffers. **(04 Marks)**

3 a. With a neat diagram, explain transport and tunnel mode of operation of VPN. **(07 Marks)**

b. Explain the different types of intrusion detection methods. **(09 Marks)**

c. Differentiate between active vulnerability scanners and passive vulnerability scanners. **(04 Marks)**

4 a. With a neat diagram briefly explain the information maintenance model. **(10 Marks)**

b. Explain the different types of passive and active attacks for the information transmitted from information source to information destination. **(06 Marks)**

c. Write a short note on cryptanalysis. **(04 Marks)**

5 a. With a neat diagram, explain advanced encryption standard for encryption and decryption. **(08 Marks)**

b. Consider a Diffie-Hellman scheme with a common prime q = 11 and primitive root $\alpha = 2$.

i) If user A has public key $Y_A = 9$, what is A's private key X_A?

ii) If user B has public key $Y_B = 3$, what is the shared secret key K? **(06 Marks)**

c. With a necessary diagram, explain the use of PGP for confidentiality and authentication of E-mail messages. **(06 Marks)**

6 a. Perform encryption and decryption using RSA algorithm for p = 17, q = 11 and M = 88. **(06 Marks)**

b. List the properties of hash function for message authentication. **(06 Marks)**

c. List the security services provided by IPSec. Also explain the use of IPSec for solving replay attack. **(08 Marks)**

7 a. With necessary diagram, explain the use of dual signature in SET. **(08 Marks)**

b. Explain the services provided by SSL record protocol. **(07 Marks)**

c. Write a short note on software-based attacks. **(05 Marks)**

8 Explain the following:

a. Digital signatures

b. Wireless network security

c. Encapsulating security payload

d. Honey pots. **(20 Marks)**

* * * * *