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

10SCS333

Third Semester M.Tech. Degree Examination, December 2011

Information Security

Time: 3 hrs. Max. Marks:100

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

1 a. Which are the five criteria that must be met for the security policy to be effective and legally enforceable in an organization? Explain each. **(10 Marks)**

b. Information security safeguards provide three levels of control. What are they? Briefly describe each. **(10 Marks)**

2 a. Under the processing-mode category of firewalls, draw the diagram of packet filtering firewall and explain. **(10 Marks)**

b. What is DMZ in screened subnet firewalls? Draw the diagram of a screened subnet firewall with DMZ and explain. **(10 Marks)**

3 a. Distinguish between configuration management and change management. **(05 Marks)**

b. Identify the four steps associated with configuration management. **(05 Marks)**

c. Under information security management and maintenance, what is the primary goal of internal monitoring domain? Draw the diagram of a typical internal monitoring system. **(10 Marks)**

4 a. Using a suitable diagram, illustrate the principle of Cipher block chaining mode (CBC) for decryption. Indicate the appropriate equation. **(10 Marks)**

b. In CBC mode, a single-bit error in cipher text block C_1 corrupts P_1 and P_2 on decryption. Are any blocks beyond P_2 affected? Explain. **(10 Marks)**

5 a. Define the terms "primitive root" and "discrete logarithm", if a is the primitive root of a prime number "p". **(05 Marks)**

b. Using the above definition, prove that 2 is a primitive root of 11. **(05 Marks)**

c. Discuss the act of man-in-the-middle attack in Diffie-Hellman key exchange. **(10 Marks)**

6 a. Under Kerberos version 4, write the suitable equations and discuss the steps involved to achieve : Ticket-granting service exchange to obtain service-granting ticket. **(10 Marks)**

b. Describe any five "environmental shortcomings" of Kerberos version 4 with respect to version 5. **(10 Marks)**

7 a. Under PGP each user will have a private key ring and a public key ring. Illustrate, using a diagram, for "PGP generation" that uses the above two rings. **(10 Marks)**

b. Describe how "anti-replay" is executed under IP security. **(10 Marks)**

8 a. Under software flaws, give a brief description of any two methods deployed to detect malware. **(10 Marks)**

b. What is digital rights management (DRM)? Illustrate the method of deploying DRM for a P2P application. **(10 Marks)**

* * * * *