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

06CS/IS835

Eighth Semester B.E. Degree Examination, June/July 2011
Information and Network Security

Time: 3 hrs. Max. Marks:100

Note: ***Answer FIVE full questions selecting at least TWO questions from each part.***

PART – A

1 a. Define policy and explain issue specific security policy. **(10 Marks)**

b. Explain the importance of incident response planning strategy. **(10 Marks)**

2 a. What is firewall? Explain categories of firewalls based on processing mode. **(10 Marks)**

b. What are virtual private networks? Explain different techniques to implement a virtual private network. **(10 Marks)**

3 a. Explain network based intrusion detection and prevention systems. **(10 Marks)**

b. Describe the need of operating system detection tools. **(10 Marks)**

4 a. List out the elements of cryptosystems and explain transposition cipher technique. **(10 Marks)**

b. Who can attack cryptosystems? Discuss different categories of attacks on cryptosystems. **(10 Marks)**

PART – B

5 a. Compare active and passive attacks. **(05 Marks)**

b. With a neat diagram, explain network security model. **(07 Marks)**

c. List out the differences between Kerberos version 4 and version 5. **(08 Marks)**

6 a. Explain PGP message generation and PGP message reception techniques. **(10 Marks)**

b. Describe S/MIME functionality. **(05 Marks)**

c. Explain S/MIME certificate processing method. **(05 Marks)**

7 a. Describe SA parameters and SA selectors in detail. **(10 Marks)**

b. Describe Oakley key determination protocol. **(10 Marks)**

8 a. Explain SSL handshake protocol with a neat diagram. **(10 Marks)**

b. List out the key features of secure electronic transaction and explain in detail. **(10 Marks)**

* * * * *

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

06CS/IS835

Eighth Semester B.E. Degree Examination, December 2011

Information and Network Security

Time: 3 hrs. Max. Marks:100

Note: ***Answer any FIVE full questions, selecting at least TWO questions from each part.***

PART – A

1 a. Define the terms : policy, standards and practices in the context of information security. Draw a schematic diagram depicting the inter-relationship between the above. **(06 Marks)**

b. What are the policies that must be defined by the management (of organizations) as per NIST SP 800 – 14? Describe briefly the specific areas covered by any two of these policies. **(07 Marks)**

c. What are the components of contingency planning? Describe briefly the important steps involved in the recovery process after the extent of damage caused by an incident has been assessed. **(07 Marks)**

2 a. What is a firewall? List the type of firewalls categorized by processing mode. Draw a schematic diagram of a packet-filtering router used as a firewall and explain its function using a sample firewall rule. **(10 Marks)**

b. Describe the steps involved in Kerberos login and Kerberos request for services, with suitable illustrations. **(10 Marks)**

3 a. Define the following terms related to IDS :
i) Alert
ii) False attack stimulus
iii) False negative
iv) False positive
v) True attack stimulus. **(05 Marks)**

b. Discuss the reasons for acquisition and use of IDSs by organizations. **(06 Marks)**

c. Discuss the differences between host IDS and network IDS, with the help of a schematic diagram. **(06 Marks)**

d. Define the terms honey pots, honey net and padded cells. **(03 Marks)**

4 a. Define the following terms related to cryptography :
i) Algorithm
ii) Cipher
iii) Key
iv) Link encryption
v) Work factor. **(05 Marks)**

b. Distinguish between symmetric encryption and asymmetric encryption, with suitable examples. **(06 Marks)**

c. Describe the terms : authentication, integrity, privacy, authorization and non-repudiation. **(05 Marks)**

d. Discuss the "man-in-the-middle" attack. **(04 Marks)**

PART – B

5 a. Describe briefly the various security attacks and specific security mechanisms covered by X.800. **(14 Marks)**

b. Describe briefly the authentication procedures covered by X.809. **(06 Marks)**

6 a. Describe the steps involved in providing authentication and confidentiality by PGP, with suitable illustrations. **(10 Marks)**

b. Discuss the limitations of SMTP/RFC 822 and how MIME overcomes these limitations. **(10 Marks)**

7 a. Describe the benefits of IPSec. **(05 Marks)**

b. What is security association? Discuss briefly the parameters that are used to define a security association. **(05 Marks)**

c. Describe the transport and tunnel modes used for IPSec AH authentication bringing out their scope relevant to IPV4. **(10 Marks)**

8 a. Discuss the SSL protocol stack. **(04 Marks)**

b. What are the services provided by SSL record protocol? Describe the operation of this protocol, with suitable illustration. **(08 Marks)**

c. What is SET? Discuss its specifications. **(08 Marks)**

* * * * *