Ex/CSE/PC/H/T/411/2025

B.E. Computer Science & Engineering Fourth Year First Semester Examination 2025

COMPUTER AND NETWORK SECURITY (Hons.)

Time: 3 hours Full Marks: 100

Group A (Total Marks: 30) [CO1]
Answer Question No. 1 OR Question no. 2.

1. [6+4+5+3+5+3+4=30]

a) Why is *availability* considered to be an aspect of security? What are the other aspects of security? Can you relate *reliability* to *availability*? How?

b) Why would you consider *disclosure* to be a threat? Suppose Z finds that X is communicating with Y, the fact that Z is not supposed to know. Is this a threat to the system? Why or why not?

c) Can RSA be used for generating key pair? How? How are encryption and decryption done in Public Key cryptosystem?

d) What is *message authentication code* (MAC)?

e) Consider a situation in which a user logs into system from different types of devices. Can you include this information in any type of *access control* for that system and the corresponding user? What type of *access control* would be suitable and why?

f) How can *replay attacks* be avoided?

g) What are the contents of *digital certificate*? Where can it be used?

2. [6+4+5+3+5+3+4=30]

a) What is *integrity*? What are the types of integrity? What measures can be taken to ensure these different types of integrity?

b) Is there any difference between *disruption* and *usurpation*? Explain briefly with suitable examples.

c) How can Diffie – Hellman algorithm be used in Symmetric Key Cryptosystem? How are encryption and decryption done in Symmetric Key Cryptosystem?

d) What is the *pre-image resistance* property of hash function?

e) Consider a situation in which a user is a college student and always logs in at the same time? What type of *access control* would be suitable and why? What will happen if he wants to log in at some different time someday?

f) What is *integrity policy*? Give an example where it is useful.

g) What is *digital signature*? What does it provide?

Group B (Total Marks: 40) [CO2]
Answer Question No. 3 [Compulsory] AND Question No. 4 OR Question no. 5.

3. [5+5+10=20]

a) How does *Needham Schroeder* protocol work? What are its problems?

b) Briefly explain the *modes* of operation of *IPSec*.

c) How does Kerberos work? What are its drawbacks?

4. [3+4+3+5+5=20]

a) What are the problems with timestamps in the *Needham Schroeder Denning-Sacco* modified protocol for key exchange?

b) How can *man-in-the-middle* attack happen during session key transfer involving trusted third party?

c) How does Authentication Header (AH) work?

d) Differentiate between the modes of operation of the IPSec protocol.

e) What does the Security Parameters Index (SPI) indicate in IPSec protocol? Is this field present in both AH and ESP?

5. [4+4+4+8=20]

a) How does *Otway-Rees* protocol take care of *replay attacks*?

b) How can symmetric session key be exchanged between two parties with the help of public key cryptosystem?

c) What is Encapsulation Security Payload (ESP)? Generally Virtual Private Networks (VPNs) are found to use ESP. Why?

d) What steps are followed in the *Negotiation* phase? Name the corresponding protocol. What are the protocols in Transport Layer Security (TLS)? Why are all these needed?

Group C (Total Marks: 20) [CO3]

6. Answer ANY FOUR (4) from the following Questions. [5X4=20]

a) How can *virus* and *worm* be differentiated?

b) What is *botnet*? What is *rootkit*?

c) Why *IP address spoofing* happens? What are the defences against spoofing?

d) What is *smurf attack*?

e) What is *reflection attack*?

f) How does *ransomware* work? Why is *trojan horse* so called?

Group D (Total Marks: 10) [CO4]

7. Answer ANY TWO (2) Questions from the following: [5X2=10]

a) What should be the security features of an operating system?

b) What is *user authentication*? In what different ways can a user be authenticated?

c) What is *access control matrix*? Mention any two implementations of it.

==. ==. ==. ==. ==. ==. ==. ==. ==. ==. ==. == ==. ==. ==. ==. ==.