Ex/PG/CSE/T/1210C/2024

M.E. COMPUTER SCIENCE AND ENGINEERING FIRST YEAR SECOND SEMESTER - 2024

Network Security

Time: 3 hours Full Marks: 100

Answer ANY FIVE (5) questions

1.

a. What are the aspects of security? What is *security mechanism*? What are the different categories of *security mechanism*? What is the property of *integrity*? What are the main concerns of military applications? What is the aim of developing *integrity policy*? Give an example where *integrity policy* would be required.

b. What is *threat*? Give any two examples of *threat.* What is the relation between a *threat* and an *attack*? [(3+2+3+2+2+1+2) + (1+2+2) = 20]

2.

a. What is *parallel session attack*? How can one write *safe* program code to counter *buffer overflow attack*?

b. What are the issues in providing *anonymity* in mobile environment?

c. What is *clone phishing*? What does it exploit?

d. What are the properties of *cryptographic hash function*? [4X5=20]

3.

a. How does *virus* work? What is *Ransomware*?

b. What is *Botnet*? How can a computer get infected with malicious programs?

c. What are *Certification Authorities*? What is the process of obtaining a *digital certificate*? What information does a *digital certificate* contain?

[5+5+(2+5+3)=20]

4.

a. What are the security problems of WLAN? Mention any two key generation algorithms used in IEEE802.11iRSN. What are the schemes of *data transfer* in IEEE802.11iRSN?

b. How can *digital* signature be created and verified?

c. What is *Kerberos*? How does *Kerberos* work? [(2+2+3)+5+8=20]

5.

a. What are the problems of key exchange between any two parties X and Y? How can the problem be solved with Needham-Schroeder key exchange protocol? How is *replay attack* handled in Otway-Reese protocol?

b. How does *Man-In-The-Middle* attack happen while using public key?

c. Show how and what key/s will be generated using Diffie-Hellman key exchange protocol with prime no. 7 and primitive root 3. [(3+4+4)+4+5=20]

[Turn over

6.
a. When does Distributed Denial of Service (DDoS) attack happen? Why is DDoS attack considered more severe than Denial of Service (DoS) attack? How does packet filtering work?
b. What is SYN flood? How can it be mitigated? What is the Peer to Peer attack technique in DoS?
c. Show with the help of a diagram how IP spoofing works. [(2+3+3)+(3+3+2)+4=20]

7.
a. What are used for confidentiality and authentication in SSl/TLS? What does the *Change Cipher Spec* protocol do? What are the characteristics of SSL Sessions? What does SSL Record Header contain?
b. How will you protect an IP packet? How will you determine which IPSec protocol to use on an IP packet? What is meant by Security parameters Index (SPI)? [(3+2+3+3)+(3+2+4)=20]

8.
a. How are confidentiality and authentication both used in PGP? With respect to message compression, when are encryption and signature used? Why are different types of keys used in PGP? How is the concept of trust used in PGP?
b. How does S/MIME provide authentication? Mention the content types used in S/MIME. What encoding techniques are used in S/MIME? [(3+3+2+2)+(3+4+3)=20]