Network Security & Cryptography Sample Questions

Short Question 2 marks:-

1. What is network security?
2. What is passive attack?
3. Define encryption.
4. What do you mean by digital signature?
5. What is access control?
6. Define TSP used in internet security.
7. Define s-box substitution.
8. What is trusted system?
9. Define cryptography.
10. Define cryptanalysis.
11. Define decryption.
12. Distinguish between streams and block cipher.
13. What is key wrapping?
14. What is authentication token?
15. What is active attack?
16. What is masquerade?
17. What is replay attack?
18. What is denial of service attack?
19. What is plain text?
20. What is cipher text?
21. Discuss the concept of Caesar cipher.
22. Define CA?
23. Define role of RA.
24. Name the four key steps in the creation of a digital certificate.
25. Name different type of key participant in SET?
26. Define static web page.
27. Define Dynamic web page.
28. Define Active Web page.
29. What is firewall?
30. What are the three main action of a packet filter?
31. What is a VPN?
32. Define transposition technique.
33. Define substitution technique.
34. Define polygram substitution technique.
35. Define stream cipher.
36. Define block cipher.
37. Define CRL.
38. Define private key.
39. Define public key.
40. Where SSL layer is located in TCP/IP?
41. Define seed.

42. Define Biometric.
43. What is NAT?
44. Define clear text password.
45. Name three configuration of firewall.
46. Define IP address spoofing.
47. Name the different components of a digital certificate.
48. Define Rail Fence technique.
49. Define SHTTP
50. Name the SET Participants

Long Question (6 marks) :-

1. Why is confidentiality an important principal of security? Describe the way of achieving it.
2. What is plain text? What is cipher text? Give an example of transformation of plain text into cipher text by using Caesar cipher substitution technology.
3. Explain about symmetrical and Asymmetrical key cryptography.
4. What are public key cryptography standards?
5. Explain about SHTTP and TLS.
6. Describe about biometric authentication.
7. What are the several approaches implement in security model? Explain briefly.
8. Differentiate between active and passive attack.
9. What are the steps required for creating the digital certificate? Explain briefly.
10. Discuss the reason behind the significance of authentication. How in real life the message integrity ensured?
11. Differentiate between SSL and SET.
12. What is the role of a CA and a RA?
13. What is worm? What is the significant difference between a worm and virus?
14. What is access control? How different is it from availability?
15. What is non repudiation? How can it be prevented in real life?
16. Discuss Homophonic substitution cipher with reference to Mono-alphabetic cipher.
17. What is main feature of Polygram substitution cipher?
18. What is encryption? What is decryption technique? Draw a block diagram showing plain text, cipher text, encryption and decryption.
19. What are the problems with symmetric key encryption?
20. Discuss the history of asymmetric key cryptography in brief.
21. What is the real crux of RSA?
22. What are the typical contents of a digital certificate?
23. Discuss any one mechanism used by a RA for checking the user's proof of possession of the private key.
24. What is the idea behind certification authority hierarchy?
25. Why is a self-signed certificate needed?
26. Describe how cross-certification is useful.
27. What are the common causes for revoking a digital certificate?
28. Describe the mechanism of protecting the private key of a user.

29. Discuss password based Encryption.
30. Why is SSL layer positioned between the application layer and the transport layer?
31. What is the significance of the time stamping protocol?
32. Discuss about the key participant of SET?
33. What are the problems associated with clear text passwords?
34. What is the improvement over clear text passwords? What is its drawback?
35. What is the difference between challenge/response token and time-based token?
36. How does one prevent the misuse of another user's certificate in certificate-based authentication?
37. List the characteristics of a good firewall implementation.
38. What is the disadvantage of a screened host firewall, single –homed bastion?
39. How is screened host firewall, Dual-homed bastion different from screened host firewall, single-homed bastion?
40. Discuss about IP datagram Format.
41. Discuss about TCP Segment.
42. Discuss about SET and explain purchase request.
43. How does certificate –based authentication works?
44. How TCP/IP protocol works.
45. Discuss about PKIX services.

Long Question 8 marks:-

1. Discuss about the need for network security .What are the modern nature of attacks?
2. Discuss about the various principles of network security. Give example of each of them.
3. What is cipher text in the context of network security? Differentiate it from plain text with suitable example.
4. Explain mono –alphabetic cipher with suitable example.
5. Discuss about the various data encryption standards (DES) used in case of network security?
6. Discuss about the asymmetric key cryptography in brief .Give suitable example to illustrate your answer.
7. What is a digital certificate? Narrate the technical details of digital certificates.
8. What is private key management? Discuss about the PKIX services available.
9. Differentiate between static, dynamic and active web page of a web site. Give suitable example of each.
10. What is a secure socket layer (SSL)? Explain how a SSL works, by giving suitable examples.
11. Discuss about SHTTP and TSP. Compare and contrast the features of both the protocols.
12. Define firewalls .Discuss about various types of firewalls. Explain how they work towards network security.
13. Describe about the different types of security attacks in a computer system.
14. Write the RSA algorithm and explain it with example.
15. Discuss the key steps for creating Digital certificate.
16. Why is SSL layer positioned between the application layer and transport layer? Explain the SSL handshake protocol.

17. Explain briefly transposition technique used in network security.
18. What is the key principle of security? Why is confidentiality an important principle of security?
19. Explain substitution technique in network security.
20. Explain briefly PKIX model .What are the standards used in public key cryptography?
21. Briefly analysis the DES algorithm works in symmetric key cryptography.
22. Discuss the play fair cipher.
23. Define SSL and How SSL Works?
24. What are the broad level difference between CRL, OCSP and SCVP?
25. What is the purpose of the SSL alert protocol?
26. Explain the SSL handshake protocol.
27. Explain how NAT works with an example.
28. Discuss about IP Sec Protocol.
29. Define firewall. How application Gateway and Packet filter works.
30. Define SET and describe the process of SET.