Cryptography and Network Security

UNIT 1: Security and cryptographic concepts

1. Explain the principles of security in detail with the help of diagram?
2. Discuss single columnar transposition cipher with an example?
3. Explain different security attacks?
4. Define non-repudiation?
5. Explain the relationship between security services and security mechanisms?
6. Discuss OSI security architecture?
7. Differentiate between active and passive attacks?
8. What are security services. Explain?
9. Illustrate the steps for deriving cipher text using play fair substitution with an example?
10. Describe the network security model with a neat diagram?
11. What are security goals?
12. Explain various security mechanisms?
13. Explain any two substitution techniques?
14. What is meant by steganography .Explain?
15. Explain about pervasive and specific security mechanisms?
16. Differentiate modification and fabrication?
17. What is steganography. How is it useful for providing security?
18. What is the role of firewall in network security?
19. Explain the various types of security attacks in information transmission?
20. What is crypt analysis?

UNIT 2: Symmetric and Asymmetric key ciphers

1. What do you meant by cipher block chaining?
2. If the cryptographic key length is larger, what will be the impact on security? Justify it.
3. Explain briefly the importance of key distribution in security aspects?
4. Explain fiestel cipher structure with its design criteria?
5. Illustrate how some cipher block modes of operation only use encryption while others use both encryption and decryption?
6. Generate a session key using diffie-hellman for q=3,alpha=7,X(A)=5 and X(B)=2.
7. What is cipher text attack only?
8. With neat diagram explain DES algorithm?
9. Write a short note on public key infrastructure?
10. Consider p=7, q=19 and plaintext (m)=5.Perform encryption and find public – private key pair?
11. List and explain different types of block cipher modes of operation?
12. Explain any two kinds of block cipher modes and also explore their advantages and disadvantages?
13. Explain diffie-hellman key exchange protocol with an example?
14. State the requirements of public key cryptography?
15. Explain in detail the sub key generation and round function of DES algorithm?
16. Discuss linear and differential cryptanalysis?

17. Discuss about RC4 stream cipher?
18. List out the basic steps in public key encryption?
19. Find the n and phi(n) values in RSA if p=7,q=17?
20. Differentiate Interruption and Interception?
21. Enumerate in detail the steps in AES?
22. Explain the methods used for distribution of public keys?
23. State and Explain Elgamal algorithm with an example?
24. Explain the concept of public key and private key used in cryptography?
25. Explain the advantage of having 2 keys in cryptographic algorithms?
26. A & B wants to establish a secret key using diffie-hellman key exchange protocol, using a common prime q=353 and a primitive root alpha=3. A's secret key X(A)=97 and B's secret key X(B)=233.Compute A's public key Y(A) , B's public key Y(B) and A's & B's common secret keys?
27. Write RSA algorithm and also show how signing and verification of digital signatures is done using RSA?
28. How data integrity and confidentiality is provided as a part of security?

UNIT 3: Cryptographic hash functions and key management

1.Write a short note on digital signature?
2.Explain HMAC algorithm with diagram?
3.Explain digital signature and hoe it is used for authentication,explain by giving specific application?
4. Explain the scenario where Kerberos is preferred?
5. Mention the benefits where the Kerberos scheme if preferred(Advantages)?
6. Draw the diagram of compression function of SHA-1 and explain?
7. What are Kerberos and explain the hypothetical dialogues in Kerberos v4?
8. List the requirements of secure hash function?
9. Briefly explain the steps in HMAC, with it's advantages?
10. Explain SHA-512 message digest with flowcharts and intermediate results?
11. Illustrate the basic uses of MAC with neat diagram?
12. Describe the general format of X.509 certificate?

UNIT – 4:Transport Level and Wireless Network Security

1. What protocol is used to convey SSL related allots to the peer entity. Give the Protocol format and describe the format?
2. Explain the operations of SSL record protocol?
3. What is SSL? Write about functionality of TLS protocol?
4. List the differences between SSL and TLS?
5. Define Extended Service Set?
6. What security areas are addressed by IEEE 802.11i?
7. Briefly describe the IEEE 802.11i phases of operation?

8. Is Distribution system a wireless system?
9. List and briefly define 802.11i services?
10. What is the difference between TKIP and CCMP?
11. List and briefly define the SSH protocol?
12. For what application is SSH useful?
13. What is the purpose of HTTPS?
14. Write the steps for packet exchange in SSH protocol?
15. Explain the protocol stack of SSH?
16. Discuss the parameters to identify security association?

UNIT 5: Email security

1.Explain key management techniques in ISAKMP.
2.Specify the various documents in IPsec architecture.
3.Draw the frame structure for ISAKMP and explain its fields.
4.List different MIME content types.
5.Explain Transport and Tunnel modes in IPsec.
6.Describe various PGP services
7.Draw and Discuss the PGP cryptographic function for authentication only.
8.Difference between transport and tunnel mode of IPsec Protocol.
9.What is MIME .Difference between MIME and S/MIME functionalities
10.Discuss about functionalities of encapsulating security payload protocol.
11.What are the applications of IPsec.
12.What are the roles of the Oakley key determination protocol and ISAKMP in IPsec.
13.Draw the Authentication Header and give the description of each field.
14.What is radix-64 format.Explain how both PGP and S/MIME perform the radix-64 conversion.
15.What services are provided by IPsec.
16. What parameters identify an SA and what parameters characterize the nature of a particular SA.
17.State the limitations of SMTP RFC 822 and how is it overcome in MIME.
18.What is the need to combine security association .Explain basic combination of SA?
19.Why does ESP include a Padding field.