CNS QUESTION BANK

Chapter-1

Long Question

1. What do you mean by cryptography? Explain the type of attack.
2. What is the need of security? Classify the Security services in Cryptography.

Short Question

1. Specify the four categories of security threats:
    1. Interruption
    2. Interception
    3. Modification
    4. Fabrication
2. Explain active and passive attack with example.
3. Define integrity and non-repudiation.
4. Why network need security?
5. Define network security.
6. Define computer security.

Chapter-2

Long Question

1. Explain Substitution technique?
2. Explain various transposition ciphers in detail?
3. State and explain the principles of public key cryptography?

Short Question

1. Define cryptography.
2. Compare Substitution and Transposition techniques.
3. Define Diffusion & Confusion.
4. Difference between plain text and cipher text.
5. Difference between Symmetric Key and Asymmetric Key cryptography.

Chapter-3

Long Question

1. Explain Data Encryption Standard (DES) in detail.
2. How AES is used for encryption/decryption? Discuss with example.
3. Explain RSA algorithm in detail with an example?
4. Explain the Key Generation, Encryption and Decryption of DES algorithm in detail.
5. (i)Draw the general structure of DES and explain the encryption decryption process.
   (ii) Mention the strengths and weakness of DES algorithm.

6. Discuss clearly Secure Hash Algorithm (SHA).
7. Compare the Features of SHA-1 and MD5 algorithm.
8. Briefly explain Deffie Hellman key exchange with an example.
9. Write and explain the Digital Signature Algorithm.
10. Describe the MD5 message digest algorithm with necessary block diagrams.

Short Question

1. List out the attacks to RSA.
2. What you meant by hash function?
3. Differentiate MAC and Hash function?
4. Any three hash algorithm.
5. What are the requirements of the hash function?
6. What you meant by MAC?
7. What is the meet in the middle attack?
8. What is the role of compression function in hash function?
9. Compare MD5, SHA1 algorithm.
10. What requirements should a digital signature scheme should satisfy?
11. What are the properties a digital signature should have?

Chapter-4

Long Question

1. Explain Digital Signature.
2. Why Digital Certificate is introduced. Explain.
3. Explain the format of the X.509 certificate.
4. Explain about PKI in detail

Short Question

1. Difference between Digital certificate and digital signature.
2. What is a Digital Signature Certificate?
3. How does a Digital Signature Certificate work?
4. What is an electronic document?
5. What is the difference between Electronic Signature and Digital Signature?
6. How is Digital Signature Validated and Secured?

Chapter-5

Short Question

1. What are SSL Certificates?
2. How SSL uses both asymmetric and symmetric encryption?
3. Discuss some public-key encryption algorithm used in SSL.
4. What is Transport Layer Security (TLS)?
5. What's the difference between TLS and SSL?
6. What's the difference between TLS and HTTPS?

7. What is S-HTTP (Secure Hypertext Transfer Protocol)?
8. What is Time Stamping?
9. What are the steps involved in SET transaction?
10. Which is the better security measure, HTTPS or SSL?
11. Define S/MIME?
12.

Long Question

1. Explain how SSL works?
2. How does TLS work?
3. Explain secure electronic transaction.

Chapter-6

1. Why Authentication is required?
2. What is the means of User Authentication?
3. What is Kerberos? Explain how it provides authenticated service.
4. What is token-based authentication?

Chapter-7

1. What is VPN explain?
2. Short note on :
   i. FIREWALL
   ii. VIRUSES

Long Question

1. Explain TCP/IP .
2. Write notes on IP Security.