Question Bank for Information Security

Unit 1 : Overview and Classical Encryption Techniques

1) List and briefly define categories of security services.
2) Explain X.800 security mechanism?
3) Explain model for network security?
4) Explain types of attacks on encrypted message.
5) List and briefly define types of cryptanalytic attacks based on what is known to the attacker.
6) Explain substitution ciphers Caesar, Monoalphabetic, Playfair, and Hill.
7) Explain Polyalphabetic substitution ciphers Vigenere, autokey, and one-time pad.
8) Briefly define the Caesar cipher.
9) Briefly define the monoalphabetic cipher.
10) Briefly define the Playfair cipher.
11) Explain transposition techniques.
12) Explain operation of Rotor machine.

Question Bank for Information Security

Unit 2: Block Ciphers and Advanced Encryption Standard

1) What are the parameters and design features for realization of a Feistel network.
2) Explain Feistel decryption algorithm.
3) Explain encryption and decryption in Data Encryption Standard (DES).
4) Explain key generation in Data Encryption Standard (DES).
5) What is the purpose of the S-boxes in Data Encryption Standard (DES)?
6) Explain operation of S-Boxes in Data Encryption Standard (DES).
7) Explain Single Round of DES Algorithm with neat diagram.
8) Explain general structure of Advanced Encryption Standard (AES).
9) Explain detailed structure of Advanced Encryption Standard (AES).
10) Explain Advanced Encryption Standard (AES) transformation functions.
11) Explain Advanced Encryption Standard (AES) key expansion.

Question Bank for Information Security

Unit 3: Public Key Cryptography

1) What are three broad categories of applications of public-key cryptosystems?
2) What requirements must a public key cryptosystems fulfill to be a secure algorithm?
3) Explain Rivest-Shamir-Adleman (RSA) algorithm.
4) Explain security of Rivest-Shamir-Adleman (RSA) algorithm.
5) What are four possible approaches to attack the Rivest-Shamir-Adleman (RSA) algorithm?
6) Explain Optimal Asymmetric Encryption Padding (OAEP).
7) Explain Diffie-Hellaman key exchange algorithm.
8) Explain Man-in-the-Middle Attack against Diffie-Hellaman Key Exchange Protocol.
9) Explain Elgamal Cryptographic System.

Question Bank for Information Security

Unit 4: Cryptographic Data Integrity Algorithms

1) Explain general structure of secure hash function.
2) Explain SHA-512 Logic with neat diagram.
3) What is MAC? What are the requirements of MAC?
4) With neat diagram explain basic uses of message authentication code.
5) Explain MACS based on hash functions HMAC.
6) Explain Message Authentication Code (MAC) based on block ciphers Data Authentication Algorithm (DAA) and Cipher Based Message Authentication Code (CMAC).
7) Explain Data Authentication Algorithm (DAA).
8) Explain generic model of digital signature process.
9) Explain ELGAMAL digital signature scheme.
10) Explain SCHNORR digital signature scheme.
11) Explain Digital Signature Standard.
12) Explain Signing and verification process in Digital Signature Standard.

Unit 5: Key Management and Distribution

1) Explain symmetric key distribution using symmetric encryption.
2) Explain symmetric key distribution using asymmetric encryption.
3) Explain four ways to distribute public key.
4) List four general categories of schemes for the distribution of public keys.
5) What is a public-key certificate?
6) What are the requirements for the use of a public-key certificate scheme?
7) Explain X.509 certificates format.
8) Explain X.509 Version 3 certificate format.
9) Why an X.509 certificate is revoked?
10) Explain hierarchy of Certificate Authorities (CA's) for distribution of other CAs public key.
11) Explain PKIX architectural model.

Question Bank for Information Security

Unit 6: Network And Internet Security

1) Explain Secure Socket Layer (SSL) architecture.
2) What protocols comprise Secure Socket Layer (SSL)?
3) Explain Secure Socket Layer (SSL) record protocol.
4) What services are provided by the SSL Record Protocol?
5) Explain Secure Socket Layer (SSL) Handshake protocol action.
6) Explain Transport Layer Security (TLS).

7) What are the services provided by Pretty Good Privacy (PGP)?
8) What are the five principal services provided by PGP?
9) Explain Pretty Good Privacy operations.
10) Explain Pretty Good Privacy message generation and reception process.
11) What are the functions provided by S/MIME?
12) What are the Cryptographic algorithms used by S/MIME to provide different functions?
13) What are the steps for preparing an enveloped data MIME entity?
14) What are the steps for preparing signed data MIME entity?

15) Explain IPSec architecture.
16) Explain transport and tunnel modes of IPSec.
17) Explain processing model for outbound and inbound IPSec packets.
18) Explain IPSec Encapsulating Security Payload (ESP) service.
19) Explain IPSec Encapsulating Security Payload (ESP) packet format.
20) Explain IPSec Anti-replay mechanism with neat diagram.