

<u>MODULE-1</u>	
01.	Explain Network Access Security Model and basic tasks in designing a particular security service.
02.	Explain a note on Symmetric Cypher model with a neat diagram.
03.	Write a note on classification of Cryptographic systems.
04.	Explain the following techniques with example for each. i) Caesar algorithm ii) Monoalphabetic Ciphers
05.	Explain Playfair Encryption and Decryption with an example.
06.	Write a note on the following with example for each: i) Hill Cipher Encryption. ii) Hill Cipher Decryption.
07.	Explain the following techniques with example for each. i) Polyalphabetic Cipher ii) Vernam Cipher iii) One Time Pad
08.	Explain Vigenere Cipher and Auto Key System with example for each.
09.	Write a short note on Steganography with an example.
10.	What is Block Cipher and Explain Feistel Cipher in detail with an example.
11.	Explain DES Encryption algorithm with a neat diagram and an example.
12.	Write a short note on Block Cipher Design Principles.

<u>MODULE-2</u>	
01.	What is Pseudorandom number Generators, and explain the following with example. i) Linear Congruential Generators ii) Blum Blum Shub Generator
02.	What is Public key cryptography? And Explain public-key encryption scheme with a neat diagram.
03.	Differentiate between Conventional Encryption and Public-Key Encryption.
04.	Justify, how Public-Key Cryptosystem achieves Confidentiality, Authentication and Security.
05.	Explain different requirements for Public-Key Cryptography.
06.	Explain RSA Algorithm in detail with an example.
07.	Write a note on Computational Aspects and Security of RSA.
08.	Perform encryption and decryption using the RSA algorithm for the following: i) $p = 3; q = 11, e = 7; M = 5$ ii) $p = 5; q = 11, e = 3; M = 9$
09.	Write a note on Diffie-Hellman key exchange algorithm with a neat diagram and explain Man-in-the-Middle Attack in Diffie-Hellman key exchange.

10.	Users A and B use the Diffie-Hellman key exchange technique with a common prime $q = 71$ and a primitive root $\alpha = 7$. i) If user A has private key $X_A = 5$, what is A's public key Y_A? ii) If user B has private key $X_B = 12$, what is B's public key Y_B? iii) What is the shared secret key?
11.	Explain Elliptic Curve Encryption/Decryption with an example, and Explain Security of Elliptic Curve Cryptography.

QUESTION BANK

Subject: CRYPTOGRAPHY and NETWORK SECURITY (BCS703)

<u>MODULE-3 (Next Half)</u>	
01.	Explain the Secret Key Distribution with confidentiality and authentication.
02.	Explain the different techniques proposed for the distribution of public keys with examples for each.
03.	What are X.509 standards? Explain the structure of X.509 certificate with neat diagram.
04.	Explain PKIX Architectural Model with different key Elements and management functions.

<u>MODULE-4</u>	
01.	Explain NIST Model for Electronic User Authentication with neat diagram.
02.	Explain Overview of Kerberos with neat diagram.
03.	What is Kerberos? And explain Kerberos 4.
04.	Explain Kerberos version 5 Authentication Dialogue and Flags.
05.	Write a note on Web security considerations.
06.	Explain TLS Architecture and TLS Record Protocol with neat diagram.
07.	Write a note on Email Threats and comprehensive email security.
08.	Write a note on the following: i) Confidentiality and Authentication for S/MIME functional flow. ii) S/MIME Message Content Types.
09.	Differentiate between S/MIME and OpenPGP.

<u>MODULE-5</u>	
01.	Explain different Applications and benefits of IPsec.
02.	Explain IPsec Architecture with neat diagram.
03.	Write a note on Security Association Database and Security Policy Database.
04.	Explain IPsec processing for Inbound and outbound traffic with neat diagram.
05.	Explain Top-level format of an ESP Packet & substructure of Payload data with neat diagram. And differentiate Transport and Tunnel mode of Encryption.
06.	Explain Basic Combinations of Security Associations with neat diagram.
07.	Write a note on the following: i) Features of IKE Key Determination ii) IKEv2 Exchanges iii) IKE Formats iv) IKE Payload Types