CSS Module Wise Imp Questions by LMT

Module 1:

MODULE 1 -INTRODUCTION - NUMBER THEORY AND BASIC CRYPTOGRAPHY

Q. Numerical Based on Ciphers ➡ [Auto Key, Play fair, Affine]

- Encrypt the given message using Autokey Cipher, Key=7 and the Message is: "The house is being sold tonight".
- Use the playfair cipher with the keyword: "HEALTH" to encipher the message "Life (10) is full of Surprises"
- Encrypt the plaintext message "SECURITY" using affine cipher with the key pair (3, 7). Decrypt to get back original plaintext.

Q. Explain the Relationship Between Security Services and Mechanism in Details

Q. What are traditional ciphers? Discuss any one substitution and transposition cipher with example. List their merits and demerits.

Module 2:

MODULE 2 - SYMMETRIC AND ASYMMETRIC KEY CRYPTOGRAPHY AND KEY MANAGEMENT

Q. Discuss DES with reference to following points [VV IMP]

1. Block size and key size
2. Need of expansion permutation
3. Role of s-boxes.
4. Weak Keys and Semi Weak Keys.
5. Possible attacks on DES

Q. Numerical in RSA [VV IMP]

- Elaborate the steps of key generation using the RSA algorithm. In RSA system the public key (E, N) of user A is defined as (7,187). Calculate Φ(N) and private key D' What is the cipher text for M= 10

Q. Explain man in the middle attack on Diffie Hellman. Explain how to overcome the same.or Numerical Based on Diffie Hellman

Q. Discuss in detail block cipher modes of operation.

Q. Explain Kerberos ? [V IMP]

Module 3:

MODULE 3 - CRYPTOGRAPHIC HASH FUNCTIONS

Q. What are the properties of a hash function? Explain role of hash function in security [V IMP]

Q. MD 5 & SHA-1 (Difference) (MUST DO)

Module 4:

MODULE 4 - AUTHENTICATION PROTOCOLS & DIGITAL SIGNATURE SCHEMES

Q. Why are digital certificates and signatures required ? What is the role of digital signature in digital certificates? Explain any one digital signature algorithm. [V IMP]

Module 5:

MODULE 5 – NETWORK SECURITY AND APPLICATIONS

Q. What is the Need for SSL ? Explain Handshake Protocol in SSL . [VV IMP]

Q. What is meant by DOS Attack? What are different ways to mount DOS attacks? [V IMP]

Q. How is security achieved in Transport and Tunnel modes of IPSEC? Explain the role of AH and ESP

Q. Explain Different Types of Firewall (firewall & IDS - difference)

Module 6:

MODULE 6 – SYSTEM SECURITY

Q. Explain Buffer Overflow attack [V IMP]

Q. List various Software Vulnerabilities. How vulnerabilities are exploited to launch an attack.[V IMP]

Q. How does PGP achieve confidentiality and authentication in emails ?