

- 1) Explain Security goals
- 2) Security Mechanism
- 3) Security Services
- 4) Type of Security attack \rightarrow Active
 \rightarrow Passive
- 5) Substitution Cipher
- 6) Transposition Cipher
- 7) Play Fair Cipher
- 8) Hill cipher
- 9) Symmetric key Encryption
- 10) Asymmetric key Encryption
- 11) Block Cipher
- 12) Stream Cipher
- 13) Comparison betⁿ block and Stream cipher
- 14) Sbox in DES, Fiestel
- 15) Public key cryptosystems
- 16) RSA algorithm
- 17) Diffie-Hellman Key Exchange
- 18) MD5
- 19) SHA-1
- 20) SHA-512
- 21) HMAC
- 22) AES
- 23) Kerberos
- 24) Digital Signature (X.509)
- 25) MAC (Message Authentication Code)
- 26) SSL (Secure Socket Layer)
- 27) What is role of hash function in security
- 28) What are the properties/characteristics of hash function.
- 29) Explain Birthday Attack.

- 30) What is access control?
- 5-32 31) What is firewall and types of firewall?
- 5-7 32) Short note on Dos and DDos.
(Denial of Service) & (Distributed Denial of Service)
- 3-10 33) Diff. betⁿ mps & SHA

Module - 5

- 34) What is authentication header?
- ~~35) List the functions of different way in which an attacker can mount a Dos attack on a system.~~
- 5-12. 35) List the functions of different protocols of SSL. Explain the handshake protocol.
- 5-26 36) Write in brief about email security. How does PGP achieve confidentiality and authentication in email.
- 5-31 37) Explain S/MIME Algorithm
- 38) Short note on IDS (Intrusion Detection System)
- 39) Short note on IP spoofing

Module-6

- 6-1 40) List various Software Vulnerabilities
How vulnerabilities are exploited to launch an attack?
- 6-3 41) Write short note on Buffer overflow?
- 21 42) Write short note on SQL injection.
- 31 43) What are the different type of malware.
- 32 44) Write a brief - Viruses and their types.