Module No.4
Digital signature schemes and authentication Protocols

Topic:

4.1 Digital signature and authentication protocols : Needham Schroeder Authentication protocol, Digital Signature Schemes – RSA, EI Gamal and Schnorr, DSS.

Questions :

1. Explain Needham -Schroeder protocol for secret key distribution with suitable diagram.
2. List the steps for key generation,message signing and signature verification in :
   (i) RSA Digital signature scheme.
   (ii) El-Gamal Digital signature scheme
   (iii) Schnorr &
   (iv) Digital Signature Standard (DSS)
3. Compare: Hash,MAC &Digital Signature.
4. What is a digital signature? Explain any digital signature algorithm.