(3 Hours) [Total Marks: 80]

N.B. : (1) Question No 1 is Compulsory.
     (2) Attempt any three questions out of the remaining five.
     (3) All questions carry equal marks.
     (4) Assume suitable data, if required and state it clearly.

1   Attempt any FOUR [20]

  a Explain with examples keyed and keyless transposition ciphers.

  b Explain the different modes of block ciphers.

  c Differentiate between SHA-1 and MD5

  d What is Buffer overflow attack?

  e Explain ARP spoofing.

2 a Explain Diffie Hellman key agreement algorithm. Also discuss the possible [10] attacks on it. Consider the example where A and B decide to use the Diffie Hellman algorithm to share a key. They choose p=23 and g=5 as the public parameters. Their secret keys are 6 and 15 respectively. Compute the secret key that they share.

  b Explain AES algorithm. Highlight the difference between AES and DES. [10]

3 a Explain various types of firewalls. [10]

  b Discuss various attacks on digital signatures and the methods by which they can [10] be overcome.

4 a Elaborate the sign and verification process of RSA as a digital signature scheme. [10]

  b Write short notes on [10]

     1. Packet sniffing

     2. SQL injection

5 a State the rules for finding Euler's phi function. Calculate [10]
     a. $\varphi(10)$
     b. $\varphi(49)$
     c. $\varphi(343)$

  b Explain Kerberos as an authentication service. [10]

6 a Enlist the various functions of the different protocols of SSL. Explain the phases [10] of handshake protocol.

  b How does ESP header guarantee confidentiality and integrity of packet payload? [10] What is an authentication header (AH)? How does it protect against replay attack?