

(3 hours)

Total marks: 80

- N.B
- 1) Question no 1 is compulsory
 - 2) Attempt any **three** questions from remaining five questions
 - 3) Assume suitable data if required
 - 4) Draw neat diagram wherever necessary

Q.1 Answer any **Four**

- a) Why digital signature and digital certificates are required? (05)
- b) Explain with example keyed and keyless transposition cipher (05)
- c) Explain key rings in PGP? (05)
- d) What are properties of hash function? Explain role of hash function in security (05)
- e) Using Chinese remainder theorem solve the following: (05)
 $x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{5}$, $x \equiv 2 \pmod{7}$, Find x ?

- Q.2 a) If A and B wish to use RSA to communicate securely. A chooses public key (e, n) as (7, 247) and B chooses public key (e, n) as (5, 221) (10)
- i. Calculate A's Private key.
 - ii. Calculate B's Private Key.
 - iii. What will be the cipher text sent by A to B, if A wishes to send $M=5$ to B
- b) What is meant by DOS Attack? What are different ways mount DOS attacks? (10)

- Q.3 a) How does ESP header guarantee confidentiality and integrity of packet payload? (10)
- b) Explain structure of DES wrt: (10)
- i. Feistel structure and its significance
 - ii. Significance of extra swap between left and right half blocks
 - iii. Expansion
 - iv. Significance of S-box
 - v. DES function

- Q.4 a) What is the need of SSL? Explain SSL Handshake Protocol (10)
- b) Encrypt the given message using Autokey Cipher, Key=7 and the Message is: (10)
 "The house is being sold tonight".

- Q.5 a) Explain man in the middle attack on Diffie Hellman . Explain how to overcome the same. (10)
- b) Use the playfair cipher with the keyword: "HEALTH" to encipher the message "Life is full of Surprises" (10)

- Q. 6 a) Explain Kerberos in detail (10)
- b) What are different types of firewall? How firewall is different than IDS? (10)

-----X-----