

3 hrs.

80 marks

Note :

1. Question 1 is compulsory.
2. Attempt any 3 questions out of the rest.
3. Make suitable assumptions whenever necessary and justify them
4. Each question carries equal marks.

Q1.

- a) Use the Play fair cipher with the keyword : "MEDICINE" to encipher the message "The greatest wealth is health". (5)
- b) Explain key rings in PGP. (5)
- c) Briefly define idea behind RSA and also explain (10)
 - 1) What is the one way function in this system?
 - 2) What is the trap door in this?
 - 3) Give Public key and Private Key.
 - 4) Describe security in this system.

Q2)a) Explain DES, detailing the Feistel structure and S-block design (10)

b) Consider a Voter data management system in E-voting system with sensitive and non-sensitive attributes. (10)

- 1) Show with sample queries how attacks (Direct, Inference) are possible on such data sets
- 2) Suggest 2 different ways to mitigate the problem.

Q 3)

- a) Explain Diffie-Hellman Key exchange algorithm with suitable example. Also explain the problem of MIM attack in it (10)
- b) What are Denial of Service attacks? Explain any three types of DOS attacks in detail (10)

Q 4)

- a) IPSec offers security at n/w layer. What is the need of SSL? Explain the services of SSL protocol? (10)
- b) What are the types of firewalls? How are firewalls different from IDS (10)

Q 5)a) What are the various ways in which public key distribution is implemented. (10)

Explain the working of public key certificates clearly detailing the role of certificate authority.

- b) Why are Digital Signatures & Digital certificates required? What is the significance of Dual Signature. (10)

Q6

Attempt any 4

(20)

- a) SHA-1
- b) Timing and Storage Covert Channel
- c) Session Hijacking and Spoofing
- d) Blowfish
- f) S/MIME