

Time: 3 Hrs

Marks: 80.

Note:

- 1. Question 1 is compulsory.**
- 2. Attempt any 3 questions out of the remaining questions.**

Q1. Attempt any Four.

- Define the security Mechanisms and attacks for OSI security architecture. 05
- List various types of security that are applied on database. 05
- Define web security. Explain the role of cookies. 05
- Explain the different types of firewalls and layer in which it operate. 05
- Explain the different modes of block ciphers. 05
- Differentiate between Digital signature and digital certificate. 05

Q2.

- Explain various authentication protocols detail. 10
- List and explain in detail security features of operating system. 10

Q3.

- Explain the role of SSH. What is the difference between HTTP and HTTPS? 10
- List different poly-alphabetic substitution ciphers. Use Hill cipher to encrypt the text "short". The key to be used is "hill". 10

Q4.

- Define digital signature.
P=7 and Q=17 are two prime numbers. If E=5 as public key,
find the cipher text for 5. Also decrypt the cipher text back to get plain text. 10
- Explain MD-5 hash function. Compare with SHA 256. 10

Q5.

- Explain Penetration testing in detail. 10
- Explain Needham Schroeder Authentication protocol. 10

Q6. Attempt any Four.

- List and explain security requirements of a website 10
- Explain DES algorithms in detail. 10

55343