(2 ½ Hours) [Total Marks: 75]

N.B. 1) All questions are compulsory.

2) Figures to the right indicate marks.

3) Illustrations, in-depth answers and diagrams will be appreciated.

4) Mixing of sub-questions is not allowed.

Q. 1 Attempt All(Each of 5Marks) (15M)

(a) Multiple Choice Question

i) prevents either sender or receiver from denying a transmitted message. a) Access Control b) Non repudiation c) Masquerade d) Integrity

ii) Which one of the following is active attack? a) Masquerade b) Traffic analysis c) Eavesdropping d) Shoulder surfing

iii) A firewall that uses two TCP connections is a) Bastion b) Application gateway c) Circuit level gateway d) Packet filtering

iv) Vigenere cipher is an example of a) Polyalphabetic cipher b) Caesar cipher c) Mono alphabetic cipher d) Product cipher

v) There are encryption rounds in DES. a) 5 b) 16 c) 10 d) 14

(b) Fill in the blanks

(RSA, shift, brute force, denial of service ,asymmetric cryptography, cryptanalysis)

i) attack is trying every possible key on a piece of

cipher text to
find intelligible translation.

ii) is based on mathematical functions rather than substitution/permutation.

iii) cipher is sometime referred as caeser cipher.

iv) algorithm is based on difficulty of finding the prime factors of a
composite number.

v) is a network attack that floods it with useless traffic.

(c) Short Answers

i) What is transposition cipher?

ii) What is the purpose of S-Box?

iii) List out any two drawbacks of DES.

iv) What is steganography?

v) What is intruder?

Q. 2 Attempt the following (Any THREE)(Each of 5Marks) (15M)

(a) List and explain different categories of security mechanisms.

(b) Explain playfair cipher giving proper example.

(c) Write an overview of AES algorithm.

(d) Explain RSA algorithm.

(e) Explain public key cryptography. Explain its application.

(f) Explain Passive Attacks and its type?

Q. 3 Attempt the following (Any THREE) (Each of 5Marks) (15M)

(a) Discuss the requirements of message authentication.

(b) Explain SHA-512 algorithm.

(c) Write a short note on digital signature.

(d) Explain public key infrastructure. Explain its key elements.

(e) Write a short note on Kerberos.

(f) Explain the format of X.509 certificate.

Q. 4 Attempt the following (Any THREE) (Each of 5Marks) (15)

(a) Explain S/MIME with its different functionalities.

(b) Discuss SSL record protocol in detail.

(c) Discuss different intrusion techniques. What precautions can be taken to prevent intrusion.

(d) Write a short note on Honeypots.

(e) Explain firewall with its types.

(f) Explain DDOS.

Q. 5 Attempt the following (Any THREE) (Each of 5Marks) (15)

(a) Explain symmetric key cryptography. Discuss different techniques used in traditional ciphers.

(b) Explain IPSec in detail.

(c) Explain different types of viruses.

(d) What is the role of audit record in intrusion detection?

(e) Encode message ‘CEASE FIRE’ using additive cipher with key 7. Also
explain decoding process.