(2½ 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) Rail Fence Technique is an example of

a) Substitution

b) Transposition

c) Product cipher

d) Caesar cipher

ii) Which of the following is passive attack? a) Relay attack b) Masquerade c) Traffic analysis

d) Denial of Service

iii) IPsec services are available in Layer. a) Application b) Data link c) Network d)

Transport

iv) To verify a digital signature we need the a) Sender's Private key b) Sender's Public key c)

Receiver's Private key d) Receiver's Public key

v) A polymorphic virus undergoes a) Crossover b) Mutation c) Genetic processing d) None
of these.

(b) Fill in the blanks

(MD5,2,4,steganography,cryptanalysis)

i) attack rely on the nature of algorithm and general characteristics of plain text.

ii) is a message digest algorithm.

iii) is a technique for hiding a secret message within a larger one.

iv) Each AES round consists of separate functions.

v) No. of keys used in Asymmetric key Cryptography is

(c) Short Answers

i) What is mono alphabetic substitution cipher?

ii) List out different types of components available in Fiestel cipher.

iii) List out any two advantages of AES over DES.

iv) What is worm?

v) What is MAC?

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

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

(b) What is substitution cipher? Explain any one substitution technique in detail.

(c) Write a short note on DES.

(d) What are different modes of operation to apply a block cipher? Explain any one in detail.

(e) Discuss asymmetric key cryptosystem. List out the differences between symmetric
and asymmetric cryptography.

(f) Explain Active Attacks and its type?

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

(a) Explain Diffie-Hellman key exchange algorithm.

(b) Write a short note on HMAC.

(c) What is hash function? Discuss its characteristics.

(d) What is digital signature? List out its desired properties.

(e) Discuss Kerberos in detail.

(f) Write a short note on X509 standard.

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

(a) Write a short note on PGP.

(b) What is SSL? Discuss its architecture.

(c) Define intruder. Explain different types of intruders.

(d) Discuss different approaches of intrusion detection.

(e) What is firewall? Explain its limitations.

(f) What is virus? Explain its counter measures.

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

(a) Discuss how public key cryptography compliments private key cryptography rather being
a replacement of it.

(b) Discuss Man in middle attack.

(c) Write short note on i)Trapdoor ii)Logic bomb

(d) Explain additive cipher with proper example.

(e) Explain two general approaches of attacking a cipher.