Q.P. code: 40273

Total Marks: 80

(3 Hours)

N.B. (1) Question No. 1 is compulsory.
(2) Attempt any three out of remaining questions.
(3) Figures to the right in parenthesis indicate full marks.

Q.1 (a) Define Network security. Explain different types of attacks in network security. [10]

(b) What is cryptography? Differentiate between private key and public key cryptography. [10]

Q.2 (a) What is Hash? Discuss briefly HMAC. [10]
(b) What are digital certificates? Explain the stepwise process of certificate generation. [10]

Q.3 (a) Explain RSA algorithm with an example. [10]
(b) Explain mutual authentication and reflection attack with the help of an example. Suggest one method for fixing it. [10]

Q.4 (a) Explain working of KDC and multi domain KDC. [10]
(b) Give overview of DES along with problems and variations in DES. [10]

Q.5 (a) Explain firewalls. How is a circuit gateway different from an application gateway? [10]
(b) Explain WEP Authentication. Illustrate data protection in TKIP . [10]

Q.6 Write short Notes on: (Any four) [20]
a) Database Encryption
b) Digital Signatures
c) SET participants
d) PGP
e) Web services security

****