Paper / Subject Code: 56303 / Information security

[3 hours] [Marks: 80]

a) Question No. 1 is compulsory
b) Attempt **any three** from the remaining six questions
c) Assumptions should be made whenever required and should be clearly stated
d) Answers to sub questions should be answered together
e) Illustrate answers with diagrams wherever necessary
f) Use of Calculators is permitted

Q1	A	What is information security? Discuss the various principles of network security	10
	B	Discuss one round structure of the DES	10
Q2	A	Explain the methods of implementing security on databases	10
	B	What are the pros and cons of symmetric and asymmetric key encryption? Explain a method that adapts the advantages of both the techniques	10
Q3	A	Define message digest. Explain SHA for getting the message digest and compare it with MD5	10
	B	What are web services? Explain and discuss the hierarchy of providing security to the web services	10
Q4	A	Explain Kerberos as a third party authentication service.	10
	B	What are the objectives of SET? Explain how are the objectives achieved	10
Q5	A	Explain the WEP and WEP2 used in the IEEE 802.11i standard .	10
	B	Explain the various implementations of Firewalls	10
Q6	A	Write short notes on <u>any four</u> of the following a) KDC b) Modes of Encryption c) TLS d) DDoS e) Reflection attack	20

****

58799