

**FACULTY OF ENGINEERING**

**B.E. IV/IV (CSE) I SEMESTER (New) (Main) Examination, Nov./Dec., 2009**  
**INFORMATION SECURITY (ELECTIVE – I)**

**Time : 3 Hours ]**

**[ Max. Marks : 75**

**Note :** Answer **all** questions from Part – A. Answer any **five** questions from Part – B.

**PART – A**

**[25 Marks]**

1. Differentiate between a threat and an attack. (3 M)
2. What are the characteristics of information ? (2 M)
3. Define a firewall and its characteristics. (3 M)
4. List and define security services. (2 M)
5. Define a cryptographic hash function and an iterated cryptographic hash function. (3 M)
6. List the services provided by SSL. (2 M)
7. What do you mean by security threats ? (2 M)
8. Differentiate between passive and active security attacks with examples. (3 M)
9. What is Data Confidentiality ? (2 M)
10. What is Traffic analysis ? State with an example. (3 M)

**PART – B**

**[50 Marks]**

11. What is the need for security and write about security investigation phase ? (10 M)
12. (a) Explain about the design of SDLC. (6 M)  
(b) What is intrusion ? (4 M)
13. (a) Explain about the different types of firewalls. (6 M)  
(b) What is the role of hash function in security ? (4 M)

(This paper contains 2 pages)

14. Explain in detail about DES and triple DES algorithms. (10 M)
15. (a) Explain chosen plain text attack and a known-plain text attack. (4 M)  
(b) How many exclusive – or operations are used in DES cipher ? Why does DES function need an expansion permutation ? (6 M)
16. Explain about MD-5 in detail. (10 M)
17. (a) What is a digital signature ? (5 M)  
(b) Explain a blind digital signature scheme. (5 M)
-