

Elective II: Information Security

Con. 3121-07.

[REVISED COURSE]

ND-1864

(3 Hours)

[Total Marks : 100

N. B. 1) Answer any 05 questions.  
2) Figures to the right indicate full marks.

1. a) What are the different software and hardware controls used to deal with the risks in computer security. What are the aspects that can enhance the effectiveness of these controls. (10)
- b) What are covert channels and how they are created? In which cases, the closure of a covert channels can be bothersome? (10)
2. a) Compare the different separation methods used as a basis for protection in Operating Systems, citing their uses and disadvantages. (10)
- b) Explain why there should be some particular protection schemes for files other than the mechanisms for protecting a general object. Explain some of the generally used file protection mechanisms. (10)
3. a) What is an Intrusion Detection System? Compare the two approaches represented by pattern-matching and heuristic style of intrusion detection. (10)
- b) Compare the two encryption strategies – Link and end-to-end encryption – used as tools for network security, from all view points. (10)
4. a) What is a firewall? Compare the different types of firewalls. Cite a reason why an organization might want two or more firewalls on a single network. (12)
- b) What are the different message integrity threats and message confidentiality threats in networks? (08)
5. a) What are the different factors that makes data sensitive? How can we maintain perfect confidentiality with precision. (10)
- b) Explain the role of Kerberos for supporting authentication in distributed systems. (10)
6. a) How can we distinguish a risk from other project events? What are the different steps in risk analysis? (10)
- b) To what extent is patency applicable to computer objects? What are the moral or ethical issues in producing correct and usable software? (10)
7. Write short notes on : (any two)
- a) Secure E-mails
- b) Virtual Private Networks
- c) Multilevel secure Databases (20).