

# Eighth Semester Examination – 2011

## COMPUTER SECURITY

Full Marks – 70

Time : 3 Hours

Answer Question No. 1 which is compulsory and any **five** from the rest.

The figures in the right-hand margin indicate marks.

1. Answer the following questions :

2×10

- (i) What is data integrity and confidentiality ?
  - (ii) Distinguish between cryptography and steganography.
  - (iii) How does Caesar cipher differ from Hill cipher ?
  - (iv) What is a malicious program ? Give examples of malicious errors.
  - (v) What is the tradeoff between threat, attack and control ?
  - (vi) What is a boot sector virus ?
  - (vii) What is a buffer-overflow attack in a program ?
  - (viii) Define 'multilevel security' in a database.
  - (ix) What is a substitution box (S-Box) ?
  - (x) What is intrusion ? Give an example of it.
2. (a) What is a Hill cipher ? Using a key  $K = \begin{pmatrix} 03 & 02 \\ 05 & 07 \end{pmatrix}$ , encrypt the message "the\_north\_star". 5
- (b) In a RSA crypto system, for  $n = 12091$  and  $e = 13$ , encrypt the message "enemy of state". 5

- ✓ 3. (a) Distinguish between worm and viruses. 5
- ✓ (b) Write down the causes of a trap-Door and briefly discuss the SALAMI attack. 5
4. (a) What is the basic process for designing a trusted operating system ? 5
- ✓ (b) What is required to achieve temporal separation ? What condition must be met to make two processes sufficiently separated ? 5
5. (a) What is user authentication ? Briefly discuss the two different approaches for achieving authentication. 5
- (b) What is database security ? In this regard discuss the approaches to multilevel security for a database system. 5
6. (a) Categorize the possible types of threats to a network. And in this context define "Firewall" and list the types of Firewall and their functions. 5
- ✓ (b) What is a risk ? Discuss the essentiality of risk analysis and briefly explain the steps required for it. 5
7. (a) What is a cyber crime ? Discuss various cyber laws and briefly explain, how does a cyber criminal commit the crime. 5
- (b) Give a brief account of ethical issues in computer security and also define security policy and its viability to an organization. 5
- ✓ 8. Write short notes on any two : 5×2
- (a) Affine ciphers
- ✓ (b) Intrusion detection system
- ✓ (c) Access control matrix
- (d) Sensitive data.