Total number of printed pages – 4

B. Tech

PECS 3406

Eighth Semester Examination – 2007

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 full marks of the questions.

1. Answer the following questions : 2×10

   (a) What do you mean by Interception and Interruption ?

   (b) What do you mean by confidentiality ?

   (c) Distinguish between cryptographer and cryptanalyser.

P.T.O.

(d) How encryption is done in Caesar Cipher ? Explain with an example.

(e) What do you mean by transposition ? Explain with an example.

(f) What is boot sector virus ?

(g) Write different security separation methods of operating systems.

(h) List different threats to electronic mail.

(i) Draw the block diagram for public key cryptosystem.

(j) Define the 'frequency attack on Caesar Cipher'.

2. (a) Discuss the tradeoff between Conventional and Public key Cryptosystems. 5

(b) Draw the block diagram for DES cryptosystem. Explain the key generation process for different rounds. 5

3. Discuss the Hill Cipher algorithm. Encrypt the word "friday" using Hill Cipher with following key :

$$K = \begin{bmatrix} 7 & 19 \\ 8 & 13 \end{bmatrix}$$ 10

4. (a) What is trapdoor ? Write down the causes of trapdoor. Briefly describe the SALAMI attack. 5

(b) Discuss various File protection mechanisms in brief. 5

5. (a) What do you mean by Sensitive data ? Discuss various factors that make data sensitive. 5

(b) Discuss different security mechanisms for database. 5

6. (a) What is firewall ? Discuss different types of firewall in brief. 5

(b) Discuss different threat in Network. 5

7. (a) What is risk analysis ? Discuss the different steps of risk analysis in brief. 5

(b) What is security policy ? Discuss its usefulness in an organization. 5

8. Write short notes on any *two* : 5×2

(a) RSA algorithm

(b) Virus

(c) AES

(d) Playfair Cipher.