

Total number of printed pages – 4

MCA
PEE 5001

Fifth Semester Examination – 2006

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
- (a) What are the essential ingredients of a symmetric cipher ?
 - (b) What are the basic functions of encryption algorithm ?

P.T.O.

- (c) What are the strengths of DES ?
- (d) Briefly define Caesar cipher.
- (e) Distinguish between mono and poly alphabetic cipher.
- (f) What are the two approaches to attack a cipher ?
- (g) What is a transposition cipher ? What are the basic techniques used ?
- (h) Distinguish between confusion and diffusion.
- (i) What are the purposes of the S-boxes in DES ?
- (j) Explain the avalanche effect.

2. A message was received as :

KXJEY UREBE ZWEHE WRYTU HEYFS
 KREHE GOYFI WTTTU OLKSY CAJPO
 BOTEI ZONTX BYBWT GONEY CUZWR
 GDSON SXBOU YWRHE BAAHY USEDQ

The key used was *royal new zealand navy* in a playfair cipher. Decrypt the message. 10

- 3. (a) Draw the block diagram of DES encryption. 5
 - (b) Explain how Hill cipher works ? 5
4. Given the same bit pattern for key 0,1,2,3 and plain text E,F [in hexadecimal].

$P_{10} = [35274101987]$, $P_8 = [637485109]$,
 $P_4 = [2431]$, $IP = [26314857]$,
 $IP(inv) = [41357286]$, $E/P = [41232341]$

$$S_0 = \begin{bmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{bmatrix} \quad S_1 = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \end{bmatrix}$$

Find the cipher text after with one round in S-DES. 10

- 5. Distinguish between : 10
- (a) Conditionally and Computationally Secure Encryption.
- (b) Monoalphabetic and Polyalphabetic Cipher.
- (c) Block and Stream Cipher.
- (d) Diffusion and Confusion.
- (e) Network security vs. program security.

6. (a) What do you mean by database security?
What are the possible attacks to a
database? 5

(b) What is the purpose of encryption in a
multilevel secure DBMS? 5

7. Write notes on any four: 2.5x4

(a) Virus

(b) Worms

(c) Firewalls

(d) Honey pots

(e) Role of proxy server.

8. (a) What are the different possible attacks to a
program execution? Hence define salami
attacks and list the controls to detect and
prevent salami attacks. 5

(b) State the controls against the program
threats. 5