(a) What is dual signature is SET ? How are they generated ? Explain the process with a schematic. 4+6=10

(b) What is the importance of "no write down" rule for a multilevel secure system having firewalls ? Explain. 10

E7906

M. E. (Comp. Sc. & Engg.) Sem. I Examination, January – 2007

Information System Security

Time : 3 Hours] [Total Marks : 80

*Attempt **four** questions.*
Marks of questions are indicated against each question.

1 Look at the **Fig. 1**.

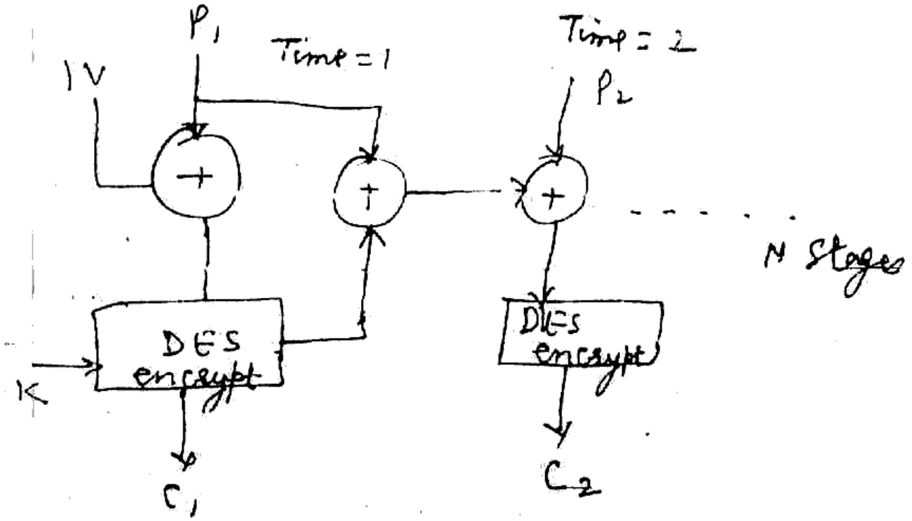

Fig. 1 (For Encryption)

This mode is called Propagating Block Cipher Chaining mode (PCBC).

(a) Draw its corresponding decryption schematic. 5

(b) What happens if a random error occurs in one block of ciphertext during

(i) encryption

(ii) transmission.

Justify your answer mathematically. 10

(c) Represent the process of encryption and decryption in mathematical equations. 5

2 (a) Suppose that in the above PCBC mode, blocks C_i and C_{i+1} are interchanged during transmission What will be the effect on plain text generated ? Give mathematical reasoning. 10

(b) Explain and differentiate the terms :

(i) Security model

(ii) Security policy and

(iii) Security audit. 10

3 A system allows the user to choose a password with length of one to eight characters. Assume that 10000 passwords can be tested per second. The system administrator wants to expire a password once they have a probability of 0.10 of having been guessed. Determine the expected time to meet this probability under each of the following conditions :

(a) Password characters may be any ASCII characters from 1 to 127 inclusive. 6

(b) Password characters may be any alphanumeric character. (A to Z, a to z and 0–9). 8

(c) Password characters must be digits. 6

4 (a) An X 509 certificate revocation list contains a field specifying when the next such list is expected to be issued. Why is this field present ? Justify your answer. 10

(b) A network consists of n hosts. Assuming that cryptographic keys are distributed on a per-host-pair basis compute how many different keys are required ? 10

5 (a) In PGP, the user is required to set a flag to indicate whether the filp being protected is text or binary data. Explain why such a flag is necessary ? 10

(b) In IPSec, when two transport mode SAs are bundled to allow both AH and ESP protocols on the same end-to-end flow, only one ordering of security protocols is appropriate. Find that ordering and give reasons/justification for the ordering. 10