Total number of printed pages – 4   **B. Tech**

PEEC 5403

Eighth Semester Examination – 2008

INTERNET SECURITY AND PROFESSIONAL ETHICS
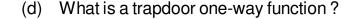
Full Marks – 70

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 two basic functions used in encryption algorithm ?

   (b)   What is a transposition cipher ?

   (c)   Differentiate between a block cipher and stream cipher.

   (d)   What is a trapdoor one-way function ?

   (e)   What are the two basic ways of transforming plain text into cipher text ?

   (f)   Differentiate between worm and virus.

   (g)   Give an example of Digital Rights Management (DRM).

   (h)   Differentiate between a weak key, a semi weak key and a possible weak keys.

   (i)   What is the basic difference between digital signature and public key cryptography ?

   (j)   What do you understand by replay attack ?

2.   (a)   Explain the operation of Feistel cipher.   5

   (b)   Explain the RSA algorithm.   5

3.   (a)   Explain how man-in-middle attack can be launched in Diffie-Hellman protocol.   5

   (b)   Give a comparison between linear and differential cryptanalysis.   5

4. (a) Explain the structure of DES and list few of its weakness. 5

(b) The encryption key in a transposition cipher is (3, 2, 6, 1, 5, 4). Find the decryption key. 5

5. (a) Explain the key expansion in AES-128. 5

(b) List security requirements in a database. 5

6. (a) Explain any one of the digital signature scheme . 5

(b) Compare and contrast key management in PGP and S/MIME. 5

7. (a) Describe how master secret is created from pre-master secret in SSL. 5

(b) Define security policy and explain its purpose with relation to IPSec. 5

8. (a) What is single sign on (SSO) and why is it required ? 5

(b) How digital signature and encryption can be used in virtual elections ? 5

_____