* 0 1 5 0 *

Printed Pages : 4 TIT701

(Following Paper ID and Roll No. to be filled in your Answer Book)

PAPER ID : 0150 Roll No. □□□□□□□□□□

B.Tech

(SEM VII) ODD SEMESTER THEORY EXAMINATION 2009-10
CRYPTOGRAPHY & NETWORK SECURITY

Time : 3 Hours] *[Total Marks : 100*

Note : *(1) Attempt all questions.*

(2) Each question carries equal marks.

1 Attempt any four parts of the following : 5×4=20

(a) What is mono-alphabetic ciphor? How it is different from caesar cipher?

(b) Explain the principle of differential cryptanalysis. Describe active and passive security attacks.

(c) What is transposition cipher? Illustrate with an example.

(d) What is double DES? Explain the term MEET in the middle attach ?

(e) What do you understand by Feistel cipher structure? Explain with example.

(f) A Hill cipher uses the following key for enciphering the message.

$$K = \begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix}$$

Obtain the decryption key to be used for deciphering the cipher text.

2 Attempt any two parts of the following : 10×2=20

(a) Describe in brief IDEA encryption and decryption. Also explain. How can we generate cryptographically secure pseudorandom numbers?

(b) Explain the following :

(i) MAC (Message Authentication Code)

(ii) HMAC (Hash based Message Authentication Code)

(c) Explain the Blowfish cryptographic algorithm. Also differentiate between differential and linear cryptanalysis.

3 Attempt any two parts of the following : 10×2=20

(a) Why the middle portion of triple DES in a decryption rather than encryption? Discuss the strength of DES algorithm and also explain the substitution method including the P-Box?

(b) Explain the Euler's coefficient function. State and prove Fermat's theorem.

(c) Explain RSA algorithm. Perform encryption and decryption using RSA algorithm for p = 17, q = 11, e = 7, M = 88.

4 Attempt any two parts of the following : 10×2=20

(a) Explain the Pretty Good Privacy (PGP) algorithm. List various services supported by PGP.

(b) Given that the First 16 bits of the 128 bit message digest in a PGP signature are translated in the clear. Explain to what extent this compromises the security of the hash algorithm.

(c) What do you understand by Elgamel encryption system? Explain its encryption and decription? What do you understand by digital signature?

5 Attempt any two parts of the following : 10×2=20

(a) What is Kerberos? Discuss Kerberos version 4 in detail. What is S/MIME and its main functions?

(b) What are the typical phases of an operation of a virus or worm and how does behaviour blocking S/W work?

(c) Give the format of X.509 certificate showing the important element of the certificate. Explain the format.
