CHAROTAR UNIVERSITY OF SCIENCE & TECHNOLOGY

Sixth Semester of B. Tech. Examination (CE/IT)

Nov 2012

IT306 Cryptography & Network Security

Date: 06.11.2012, Tuesday **Time: 10:00 a.m. To 01:00 a.m.** **Maximum Marks: 70**

Instructions:
1. The question paper comprises of two sections.
2. Section I and II must be attempted in separate answer sheets.
3. Make suitable assumptions and draw neat figures wherever required.
4. Use of scientific calculator is allowed.

SECTION – I

Q - 1 (a) Distinguish between Information Security and Network Security. [05]

(c) What is brute force analysis? Explain how it weaken the Caesar Cipher algorithm. [02]

Q - 2 (a) Explain the working of Rotor Cipher with the help of example. [04]

(b) Use the playfair cipher to encipher the message "The algorithm is very strong". Use the key "repetitive". [07]

(c) What is Key less and keyed transposition ciphers? Write steps to find the inverse of key in keyed transposition ciphers. [03]

OR

Q - 2 (a) What are the differences between mono alphabetic and poly alphabetic ciphers? Give the examples of each. [04]

(b) Use a Hill cipher to encrypt the message "The algorithm is very strong". Use the following key: $\begin{bmatrix} 03 & 02 \\ 05 & 07 \end{bmatrix}$ [07]

(c) What is Vigenere cipher? How it differs from Caesar cipher? [03]

Q - 3 (a) Explain DES key generation algorithm. [06]

(b) Define ECB and list its advantages and disadvantages. [04]

(c) Show the P-box defined by the following: [04]

[8 1 2 3 4 5 6 7]

OR

Q - 3 (a) What are semi-weak keys and weak keys in DES cipher key? [06]

(b) Define ECB and list its advantages and disadvantages. [04]

(c) Design 8 x 8 permutation tables for a straight P-box that moves the two middle bits in the input word to the two ends in the output words. Relative positions of other bits should not be changed. [04]

SECTION – II

Q - 4 (a) Write the differences between Symmetric key ciphers and Asymmetric key ciphers. [03]

(b) Explain the factorization and Chosen-cipher text attacks on RSA. [04]

Q - 5 (a) Define cryptographic hash function. List the main features of the SHA-512 cryptographic hash function. [07]

(b) Write the steps of RSA key generation algorithm. [07]

OR

(b) In RSA, given n=12091 and e=13, encrypt the message "This is tough" using 00 to 26 encoding scheme. [07]

Q - 6 **Write a short note on *any TWO*.** [14]

a. Digital Signature

b. Symmetric Key Distribution

c. Pretty Good Privacy (PGP)

****