CHAROTAR UNIVERSITY OF SCIENCE & TECHNOLOGY

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

Dec 2013

IT306 Cryptography & Network Security

Date: 04.12.2013, Wednesday **Time: 01:30 pm To 04:30 pm** **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) Explain the three goals of Information and Network Security. [03]

(b) What is extended Euclidian algorithm. Find the multiplicative inverse of 89 in Z_{100}. [04]

Q - 2 (a) Explain security service and security mechanism. Relate security service and security mechanism. [05]

(b) Explain mono alphabetic and poly alphabetic cipher. Which is more secure? Why? [05]

(c) Apply a brute-force attack to break the cipher "UVACLYFZLJBYL". Assume that algorithm used to encipher the message is Caesar cipher. [04]

OR

Q - 2 (a) Generate play fair cipher key matrix with key "awkward". Find the cipher text of "Hello". [05]

(b) Explain the procedure of Key inversion in a transposition cipher with example. [05]

(c) What is cryptanalysis? Explain four types of cryptanalysis attacks. [04]

Q - 3 (a) List and explain the components of modern block ciphers. [05]

(b) Encrypt the message "cryptanalysis" using following ciphers. Decrypt the message to get plain text. [05]

1. Vigenere cipher with key: "dell"
2. Auto key cipher with key = 5.

(c) Explain the Key generation process in DES. [04]

OR

Q - 3 (a) What are diffusion and confusion? Explain how they affect the security of block cipher. [05]

(b) Draw the block diagram of the DES function. Explain the working of it. [05]

(c) What is product cipher? Explain why DES uses S-boxes and D-boxes in encryption. [04]

SECTION – II

Q - 4 Explain the process of key expansion in AES cipher. [07]

Q - 5 (a) What is Cipher text Stealing? Explain with example. [05]

(b) Describe the working of RSA algorithm. [05]

(c) What are the requirements of cryptography hash function? List the applications of hash function in cryptography. [04]

OR

Q - 5 (a) Why man-in-the-middle attack is possible in Diffie-Hellman algorithm? Explain with example. [05]

(b) List and explain the functions used in SHA-512 hash algorithm with suitable example. [05]

(c) List and explain the fields of X.509 digital certificate. [04]

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

1. Master key generation in Secure Socket Layer (SSL)
2. Trust calculations in Pretty Good Privacy (PGP)
3. Secure MIME (SMIME)

****