# CHAROTAR UNIVERSITY OF SCIENCE & TECHNOLOGY

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

**May 2014**

## IT306/IT306.01 Cryptography & Network Security

**Date: 08.05.2014, Thursday** **Time: 10:00 am To 01:00 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) List and explain the possible attacks on security goals. [05]

(b) Why one time pad is not feasible to practically implement? [02]

Q - 2 (a) Generate the cipher text for the following plain text using auto key cipher: [05]
"Attack is delayed". Use initial key = 'M'.

(b) 1. Differentiate stream cipher and block cipher. [05]
2. Differentiate feistel and non-feistel cipher.

(c) Find the inverse key for the given transposition key: [5 3 1 2 6 8 7 4] [04]

OR

Q - 2 (a) Prove that the following matrix is valid key for the Hill cipher: [05]

$$\begin{bmatrix} 02 & 03 & 07 \\ 05 & 07 & 09 \\ 01 & 02 & 11 \end{bmatrix}$$

(b) Assume that digits (0.....9) are added to the encryption alphabet of a Play fair cipher, so key is a 6 x 6 matrix of characters. Encrypt a message "MINDBLOWING007" using Play fair cipher, where the secret word is "spiderman2". [05]

(c) What is multiplicative inverse in modular arithmetic? Find the multiplicative inverse of 89 in $Z_{300}$. [04]

Q - 3 (a) Explain why modes of operation are needed even if modern block cipher are to be used for en-cipherment. Draw diagrams for encryption and decryption in CBC mode. [05]

(b) Find the multiplication of a = $(X^3 + X^2 + X + 1)$ and b= $(X^2 + 1)$ in GF $(2^4)$, With irreducible polynomial $(X^4 + X^3 + 1)$ modulus. How GF $(2^8)$ is used in AES. [05]

(c) Why few keys from the key domain of DES are considered as weak keys and semi weak keys? Count the total no of effective keys in DES. [04]

OR

Q - 3 (a) Generate 8 bit round keys for round 1 and round 2 in S-DES for a given 10 bit cipher key as 1011100110. [05]

Straight P box : 3 5 2 7 4 10 1 9 8 6

Compression P box : 6 3 7 4 8 5 10 9

(b) List out and explain the invertible and non-invertible components used in feistel cipher. [05]

(c) What is avalanche effect? Explain why avalanche effect is generated in modern block cipher. [04]

## SECTION – II

Q - 4 (a) Explain the three basic requirements of any cryptographic hash function. [03]

(b) The cipher text 146 obtain using RSA with n=437 and e=17. One of the Plain text is either 40, 41, or 42. Determine the actual plain text without factoring n. [04]

Q - 5 (a) What are the discrete logarithm attack and the man in middle attack in Diffie-Hellman key exchange? How they can be prevented? [05]

(b) What is chosen cipher text attack in RSA? Explain with example. [05]

(c) Calculate $9^{667}$ mod 780 using fast exponential algorithm. [04]

OR

Q - 5 (a) What is key distribution center? Explain why Kerberos requires authentication server and ticket granting server. [05]

(b) What is digital certificate? Explain how digital certificate distributes public key securely. [05]

(c) Calculate the padding bits (SHA512) require for the messages having length following: [04]

1. 1
2. 896
3. 897
4. 1024

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

1. Secure Socket Layer (SSL)
2. Pretty Good Privacy (PGP)
3. Cipher Feedback (CFB) Mode

*******