CHAROTAR UNIVERSITY OF SCIENCE & TECHNOLOGY

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

May 2012

IT306 Cryptography & Network Security

Date: 08.05.2012, Tuesday | Time: 01:30 p.m. To 04:30 p.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) Define three security goals. Differentiate passive and active attacks. [05]

(c) List and briefly explain cryptanalysis attacks. [02]

Q - 2 (a) Given a plain text "*hi*" and cipher text "*HC*" find the key of 2 x 2 Hill cipher. [04]

(b) Explain the weakness in the cipher key in DES. What is avalanche effect? [07]

(c) Construct play fair matrix with the key *occurrence*. Encrypt "rijndeal" plain text using generated matrix. [03]

OR

Q - 2 (a) "The matrix [(2 2) (2 2)] cannot used as a key in Hill cipher". State true/false. Justify your answer. [04]

(b) Define feistal and non-feistel cipher. List the non-invertible components used in DES. Find round 1 key using input key AABB09182736CCDD. [07]

(c) Use the vigenere cipher with key word "HEALTH" to encipher the message "today we have examination". [03]

Q - 3 (a) Explain Cipher Block Chaining (CBC) Mode. What is cipher text stealing? [06]

(b) In a public-key cryptosystem using RSA, you intercepted the cipher text C = 8 sent to a user whose public key is e = 13, n = 33. What is the plaintext M? [04]

(c) Write the differences between symmetric and asymmetric encryption. Explain factoring problem. [04]

OR

Q - 3 (a) Explain Counter (CTR) Mode and list its advantages and disadvantages. [06]

(b) In an RSA system, the public key of a given user is e = 31, n = 3599. What is the private key of this user? [04]

(c) What is the important characteristic of public key cryptosystem? What are three broad categories of public-key cryptosystems? [04]

SECTION – II

Q - 4 (a) List and explain the criteria of a cryptographic hash function. [03]

(b) What is X.509 recommendation? Explain the signature field of X.509 certificate format. [04]

Q - 5 (a) What is Diffie-Hellman key distribution? What is man in middle attack? How it can be resisted? [07]

(b) What is cryptographic hash function? What is keyed and key less hash function? Explain the round structure of SHA-1. [07]

OR

Q - 5 (a) What is Kerberos? Explain how Kerberos distributes key with message transfer diagram. [07]

(b) Explain MAC. What is HMAC? What is the difference between MAC and digital signature? [07]

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

a. Handshake protocol in SSL

b. Content types in MIME

c. Key rings and calculation of Key legitimacy in PGP

****