CHAROTAR UNIVERSITY OF SCIENCE & TECHNOLOGY

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

May 2013

IT306 Cryptography & Network Security

Date: 01.05.2012, Wednesday **Time: 10:00 a.m. To 01:00 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) Explain the attacks threatening integrity of data with suitable example. [04]

(b) What is cryptanalysis? What are the different ways to do cryptanalysis? [03]

Q - 2 (a) What is DES? Explain round-key generation in detail. What are the weak keys and partial weak keys in DES? [06]

(b) Eve very briefly obtains access to Alice's computer and has only enough time to type two letters plaintext: "om". She gets "CG". Eve knows the algorithm is affine. Demonstrate how Eve will find actual keys using above mapping. [05]

(c) The encryption key in a transposition cipher is (3, 1, 5, 2, 6, 4). Find the decryption key. [03]

OR

Q - 2 (a) What is AES? Explain four types of transformation use in AES. [06]

(b) Find the inverse of following matrices in mod 26: [05]

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}$$

(c) Generate play fair cipher table with the key "Rijndael". How many possible keys does the Play fair cipher have in general? [03]

Q - 3 (a) What is Cipher Feedback (CFB) mode? Explain the security issues and error propagation in CFB. [06]

(b) Explain how a substitution block cipher can be modeled as a permutation. [04]

(c) What is Cipher block stealing? [04]

OR

Q - 3 (a) Write the steps for initialization in RC4. Differentiate between RC4 and CAST. [06]

(b) What is feistel and non-feistel cipher? Why full size key cipher is not possible in modern block cipher? [04]

(c) Write the differences between following: [04]

1. Block Cipher and Stream Cipher
2. Mono alphabetic cipher and poly alphabetic cipher

SECTION – II

Q – 4 Given p = 31, q = 23, e = 223 and m (plain text) = 439. Demonstrate the working of RSA algorithm (encryption and decryption) using given values. (To calculate exponential values use appropriate algorithm) **[07]**

Q - 5 (a) What is keyless and keyed hash function? List main features of the MD5 cipher. What is the padding for MD5 if the length of message is 513 bits? **[07]**

(b) What is Kerberos? Name its servers. Briefly explain the duties of each server. **[07]**

OR

Q - 5 (a) Explain the three primary requirement of cryptographic hash algorithm. What is Markel-Damgard (MD) scheme? If input size is 4096 how many bits are required for the padding in SHA-512? **[07]**

(b) Define the Diffie-Hellman protocol and its purpose. In this protocol what happens if x and y have the same value? Are R1 and R2 the same? Do the session keys calculated by Alice and bob have the same value? Use an example to prove your answer. **[07]**

Q - 6 Attempt ***any TWO***. **[14]**

1. What is MIME and S/MIME? Explain Radix-64 and Quoted-printable content transfer encoding.
2. Explain the cryptography parameter generation in SSL. Distinguish between a session and connection in SSL
3. Explain the process of extracting information from key rings at sender site and receiver site in PGP. What is key legitimacy in PGP?

****