Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

ME - SEMESTER– II(Old course) • EXAMINATION (Remedial) – WINTER- 2015

Subject Code: 1722302 **Date: 10/12/2015**

Subject Name: Advance Cryptography and Information Security

Time:2:30 pm to 5:00 pm **Total Marks: 70**

Instructions:

1. **Attempt all questions.**
2. **Make suitable assumptions wherever necessary.**
3. **Figures to the right indicate full marks.**

Q.1 **(a)** **I.** Define the following terms in brief; **04**

1. Access Control
2. Data Integrity
3. Authentication
4. Traffic Analysis

II. Distinguish between Cryptography and Steganography. **03**

(b) **I.** Use the Playfair Cipher to encipher the message ñTall trees in the campusò using the key ñoccurrenceò. Ignore the space between words. Show your calculations and result. **04**

II. Explain the avalanche effect. **03**

Q.2 **(a)** **I.** Explain diffusion and confusion in brief. How are they important to make algorithm strong? **04**

II. Explain key generation in DES. **03**

(b) Explain Mix Columns and Add Round Key operations of AES in detail. **07**

OR

(b) **I.** Encrypt message ñKey is hiddenò using Hill Cipher with the key $\begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix}$ Ignore space between words. Show your calculations and results. **04**

II. Explain triple DES with two keys. **03**

Q.3 **(a)** What is the difference between master key and session key? Explain the key distribution scenario in which each user shares a unique master key with key distribution center. **07**

(b) **I.** Write the Euclidean algorithm. How it can find the greatest common divisor of two numbers, explain with example. **04**

II. Explain linear congruential generations. **03**

OR

Q.3 **(a)** Explain Diffie-Hellman key exchange algorithm in brief. Users A and B use the Diffie-Hellman key exchange technique with a common prime q=71 and a primitive root Ŭ=7. **07**

I. If user A has private key $X_A = 5$, what is Aôs public key Y_A?
II. If user B has private key $X_B = 12$, what is Bôs public key Y_B?
III. What is shared secret key?

(b) Explain following with example; **07**

I. Eulerôs Totient Function
II. Fermatôs Theorem

Q.4	**(a)**	What are the three broad categories of applications of public key cryptosystems? Explain RSA algorithm.	**07**
	(b)	What is the common weakness of Direct Digital Signature schemes? How this can be addressed by Arbitrated Digital Signature? Explain different Arbitrated Digital Signature Techniques.	**07**

OR

Q.4	**(a)**	What is hash code? Describe a variety of ways in which hash code can be used to provide message authentication.	**07**
	(b)	What is Mutual Authentication? Explain different symmetric key encryption approaches that can be used to achieve the mutual authentication.	**07**
Q.5	**(a)**	Explain necessity of Intrusion Detection System in detail.	**07**
	(b)	Explain dual homed host, bastion host and screened host. Explain split screened subnet.	**07**

OR

Q.5	**(a)**	Explain cross site scripting attack. Explain the counter measures for this.	**07**
	(b)	Explain server-level web threats like repudiation, information disclosure, Evaluation of privileges and denial of service.	**07**

****