Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

M. E. - SEMESTER – I • EXAMINATION – WINTER 2012

Subject code: 710104N Date: 16-01-2013

Subject Name: Information Security

Time: 02.30 pm – 05.00 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)** What is intrusion? What is intrusion detection system? Explain intrusion detection system types in detail. **07**

(b) (1) Discuss unigram frequency attack on Caesar cipher. **07**
(2) Polygram substitution is better than unigram substitution – Justify.
(3) One Time Pad (OTP) cipher is the most secure one – Justify.

Q.2 **(a)** Decipher the message YITJP GWJOW FAQTQ XCSMA ETSQU SQAPU SQGKC PQTYJ using the Hill cipher with the inverse key **07**

5	1
2	7

Show your calculation and the result.

(b) What is digital signature? What requirements should a digital signature scheme satisfy? Explain direct and arbitrated digital signature. **07**

OR

(b) (1) How substitution cipher differs from Transposition cipher? **07**
(2) What is the difference between an unconditional secure cipher and a computationally secure cipher?

Q.3 **(a)** (1) What is a product cipher? Explain diffusion and confusion. **07**
(2) Explain the avalanche effect.

(b) Explain the Single Round of DES Algorithm with diagram. **07**

OR

Q.3 **(a)** How AES differs from DES? Cipher Key = 2B 7E 15 16 28 AE D2 A6 AB F7 15 88 09 CF 4F 3C. Generate the Round 1 key from given Cipher Key. **07**

(b) What type of information might be derived from a traffic analysis attack? What is traffic padding and what is its purpose? **07**

Q.4 **(a)** (1) What is nonce? **07**
(2) What is a key distribution center?
(3) What is the difference between statistical randomness and unpredictability?

(b) Explain server-level web threats like repudiation, information disclosure, evaluation of privileges, and denial of service. **07**

OR

Q.4 **(a)** Explain fundamentals of secure network design scenario like Dual-Homed Host, Screened Host, Screened Subnets and Split Screened Subnets in detail. **07**

Q.4 **(b)** Explain a Message Authentication Code. What is the difference between a message authentication code and a one-way hash function? **07**

Q.5	**(a)**	(1) What is replay attack? Give examples of replay attacks. (2) List and explain three general approaches to dealing with replay attacks. (3) Explain a suppress-replay attack.	**07**
	(b)	Explain Message Digest Generation Using Whirlpool.	**07**
		OR	
Q.5	**(a)**	What characteristics are needed in a secure hash function? Discuss Birthday attack and its signification.	**07**
	(b)	Explain message digest generation steps using SHA-512.	**07**

****