Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

M.E Sem-I Examination January 2010

Subject code: 710104 Subject Name: Information Security

Date: 27 / 01 / 2010 Time: 12.00 – 2.30 pm

Total Marks: 60

Instructions:

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

Q.1	**(a)**	Justify with your arguments, "Strength of any cryptographic system rests with the key distribution technique.	**06**
	(b)	What are the issues in effective use of IDS? Discuss some of them with effects.	**06**
Q.2	**(a)**	How can a list of all the groups of the domain be obtained? How can a list of the groups that are specific to the local computer be obtained? How can an attacker get the names of the computer visible on the network?	**06**
	(b)	(1) Which port scanner utility is available with UNIX distributions? (2) What "Type" of DNS query can be generated ? Does the query message contain any "answers"? (3) Write a snort rule applied to all packets except those that originate from class C	**06**
		OR	
	(b)	What do you mean by packet filtering? What are its limitations.	**06**
Q.3	**(a)**	What do you mean by security attack, mechanism and service? Clear all three with respect to your example.	**06**
	(b)	Give Fermat's theorem and its importance in public-key cryptography.	**06**
		OR	
Q.3	**(a)**	What are the key factors in designing secure encryption algorithm? Discuss them with your justification.	**06**
	(b)	What are the design goals of MD4? How does MD5 differ from MD4?	**06**
Q.4	**(a)**	What is S-box? What is role of S-box in encryption algorithm? Give their design approaches.	**06**
	(b)	Explain DSS signing and verifying with example.	**06**
		OR	
Q.4	**(a)**	Compare link and end-to-end encryption and discuss factors deciding choice between them.	**06**
	(b)	What is difference between diffusion and confusion? How are they important to make algorithm strong?	**06**
Q.5	**(a)**	Which are the two common types of nonessential services that an attacker might try to exploit when attempting to compromise a web server?	**06**
	(b)	Explain how does system key utility provide protection against password-cracking attacks?	**06**
		OR	
Q.5	**(a)**	If an organization is providing web services, Which common threats should be checked in penetration tests? What countermeasures should be taken against these threats?	**06**
	(b)	Directory browsing feature found on Web Server leads to which kind of threat? What is the countermeasure against this?	**06**

****