Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

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

Subject code: 1722302 **Date: 31-12-2012**

Subject Name: Advance Cryptography and Information Security

Time: 10.30 am – 01.00 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)**	Define the term information security. List and briefly define the categories of security attacks and services.	**07**
	(b)	Explain in detail the categories into which intrusion detection system can be classified?	**07**
Q.2	**(a)**	Explain the following two issues of the complexity of the computation required to use RSA. i) Encryption/decryption ii) Key generation.	**07**
	(b)	i) RSA algorithm is vulnerable to which cryptanalytic attack? Why?	**03**
		ii) Prove Fermat's and Euler's theorem.	**04**
		OR	
	(b)	i) Explain Euler's totient function.	**03**
		ii) Explain Deffie Hellman key exchange scheme in detail.	**04**
Q.3	**(a)**	i) Which two criteria are used to validate that a sequence of numbers is random? Explain the linear congruential method to generate pseudorandom numbers.	**03**
		ii) Explain the key distribution scenario in which each user shares a unique master key with key distribution center	**04**
	(b)	i) What is traffic padding and what is its purpose?	**03**
		ii) Using Vigenere cipher, encrypt the word 'cryptography' using the key house.	**04**
		OR	
Q.3	**(a)**	i) Compare the substitution in AES and DES. Why do we have only one substitution table(S-box) in AES, but several in DES?	**03**
		ii) Briefly Explain the byte substitution in AES (Advanced Encryption standard).	**04**
	(b)	i) What is the purpose of S-boxes in DES? Explain the avalanche effect.	**03**
		ii) How security of polyalphabetic cipher is improved over monoalphabetic cipher?	**04**
Q.4	**(a)**	What is message authentication code? Describe the situations in which message authentication code is used.	**07**
	(b)	Why do nonessential services appeal to attackers? How services can be	**07**

enumerated on Domain Controller?

OR

Q.4	**(a)**	What are the properties digital signatures should have? Write digital signature algorithm.	**07**
	(b)	How can it be verified that a machine is connected to SMTP service? Explain how to spoof e-mail. Is it server level or client level threat? List other threats in that category	**07**
Q.5	**(a)**	i) Explain the inspection technique used in TCP and higher layer for filtering process?	**03**
		ii) Why is it that an ICMP packet does not have source and destination port numbers? How many bytes are in the IP header? How many bytes are in the payload *of the IP datagram*?	**04**
	(b)	i) Write a snort rule that filters all the HTTP traffic that is generated by class C address and destination is class B address.	**03**
		ii) Explain with example snort rule header and the rule options	**04**

OR

Q.5	**(a)**	i) Explain screened subnet	**03**
		ii) “A customer keeps on adding items to basket in E-commerce site”. This leads to which kind of attack and which mode of intrusion detection can detect this attack?	**04**
	(b)	i) Write the tricks and techniques that spammers use.	**03**
		ii) Explain cross site scripting attack and explain the countermeasures for this	**04**

****