Seat No.:	Enrolment No.
Scal No	Emonicit No.

GUJARAT TECHNOLOGICAL UNIVERSITY

M. E SEMESTER – II • EXAMINATION – WINTER • 2014				
Subj	ect o	code: 1720205 Date: 05-12-2	014	
Subj	ect I	Name: Cryptography and Network Security		
Time	: 02	2:30 pm - 05:00 pm Total Marks	: 70	
Insti	·uct	ions:		
	1.	Attempt all questions.		
		Make suitable assumptions wherever necessary.		
	3.	Figures to the right indicate full marks.		
Q.1	(a)		07	
		1. Vulnerabilities		
		2. Integrity		
		3. Anonymity		
	<i>a</i> >	4. Authorization	0.5	
	(b)	Discuss Various Active & Passive Threats.	07	
Q.2	(a)	Write a short note on Advance Encryption Standard with an example.	07	
	(b)	· -	07	
		Take $P = 11$ and $Q = 13$ as two large prime number.		
		Make necessary assumption, if required [mention it clearly, in answer] OR		
	(b)	Explain triple DES with necessary Example.	07	
Q.3	(a)	Note: Hash Function. Explain any One Hash Algorithm in detail.	07	
	(b)	Write a detail note on Public Key Infrastructure. Explain What is Digital	07	
		Signature?		
		OR		
Q.3	(a)	How the SSL helps to maintain Web security? Provide detail idea.	07	
	(b)		07	
		Certificate & Digital signature?		
Q.4	(a)	How will you achieve Network security using IP Security?	07	
۳.٠	(b)	· · · · · · · · · · · · · · · · · · ·	07	
	(6)	OR	07	
Q.4	(a)		07	
		Network Security?		
	(b)	What is Kerberos server? Provide the execution detail of Kerberos	07	
		server.		
Q.5	(a)	Differentiate warms & viruses. Provide brief description for Viruses and	07	
	()	its type.		
	(b)	**	07	
	` ′	OR		
Q.5	(a)	What is the meaning of Biometric Authentication?	07	
		Discuss various type of Biometric Authentication in detail.		
		Provide brief idea: How to achieve finger print authentication?		
	(b)		07	
		RFID.		
