http://www.gujaratstudy.com

Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

MCA Integrated - SEMESTER– VIII • EXAMINATION – SUMMER - 2017

Subject Code: 4480603 Date: 03-May-2017

Subject Name: Network Security

Time: 10:30 AM – 1:00 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)**	Answer in brief (any seven):	**07**
	i)	Give digest size for SHA-1, SHA-224, SHA-256, SHA-384 & SHA-512.	
	ii)	Enumerate the security services and security mechanisms.	
	iii)	Differentiate between known plaintext and chosen plaintext.	
	iv)	What is peer entity authentication?	
	v)	Enumerate the ingredients of public key cryptography.	
	vi)	Write the full form of TGT.	
	vii)	MIME converts ASCII-data to Non-ASCII data. [True / False]	
	viii)	RC4 is an example of _____	
	ix)	What is ipad & opad in HMAC?	
	(b)	Write in one or two sentences (any seven):	**07**
	i)	What is a realm in Kerberos?	
	ii)	What is the purpose of alert message in TLS?	
	iii)	What is a Digital Signature?	
	iv)	What is a Subject in X.509 certificate?	
	v)	What is the purpose of the alert protocol in SSL?	
	vi)	How session keys are exchanged in PGP?	
	vii)	What is the job of the ticket granting server in Kerberos?	
	viii)	What does radix-64 step do in PGP?	
	ix)	What is Honeypot intrusion detection?	
Q.2	**(a)**	Discuss Symmetric Block Cipher? Explain AES with suitable diagram.	**07**
	(b)	Explain HMAC algorithm with suitable diagram.	**07**
		OR	
	(b)	Why mode of operation is defined? Explain any two cipher block modes of operations.	**07**
Q.3	**(a)**	Explain PGP Services.	**07**
	(b)	1. Write any four important differences between Kerberos version 4 and Kerberos version 5.	**04**
		2. Discuss the Man-In-The-Middle attack with suitable diagram.	**03**
		OR	
Q.3	**(a)**	Explain SHA-512 with diagram.	**07**
	(b)	Discuss SSL Alert and SSL Handshake Protocol.	**07**
Q.4	**(a)**	What is IPSec? What are the applications of IPSec? Explain the modes of IPSec operations.	**07**
	(b)	What is random number generator? Discuss TRNG, PRNG and PRF with suitable diagram.	**07**
		OR	
Q.4	**(a)**	1. Discuss Rule based Intrusion Detection.	**05**
		2. What do you mean by false positive and false negative in Intrusion Detection System?	**02**

http://www.gujaratstudy.com

	(b)	Discuss Password selection strategies in detail.	**07**
Q.5	**(a)**	1. What is an Audit record in IDS?	**02**
		2. How UNIX manages passwords to make it secure from attackers?	**02**
		3. Explain how one can use Markov model for proactive password checking?	**03**
	(b)	Draw ESP format for IPsec and show the need of fields SPI, sequence number, payload data, padding, pad length, next header and authentication data field.	**07**

OR

Q.5	**(a)**	Draw AH format for IPsec and discuss all the necessary fields.	**07**
	(b)	Explain how attacks like IP address spoofing, source routing and tiny fragments can be carried out on packet filtering routers? What are the counter measures?	**07**

****

http://www.gujaratstudy.com