Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

MCA- Vth SEMESTER–EXAMINATION –JUNE - 2012

Subject code: 650002 Date: 12/06/2012

Subject Name: Network Security (NS)

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)**

1. Briefly explain the terms: a) Message Confidentiality b) Message Integrity c) Message Authentication d) Non Repudiation e) Denial of Service **[05]**
2. Differentiate between Security Threat and Security Attack. **[01]**
3. Differentiate between Security Mechanism and Security Service. **[01]**

(b)

1. Explain giving examples Active Attacks and Passive Attacks. **[06]**
2. What is meant by the term "Hacking"? **[01]**

Q.2 **(a)**

1. Mention and very briefly explain any three design features/parameters considered while designing a symmetric block cipher. **[03]**
2. Mention the two major reasons why AES was introduced even though Triple DES was already there. **[02]**
3. "Arrival of Asymmetric key cryptography has made Symmetric key cryptography obsolete." State True/False with reason. **[02]**

(b)

1. What is meant by: a) Session Key b) Permanent Key? **[02]**
2. Mention and briefly explain any five properties necessary for a hash function to be useful for message authentication. **[05]**

OR

(b)

1. Mention and very briefly explain any five fields/elements of the format of X.509 Public Key Certificate. **[05]**
2. Just by using a schematic diagram, show how authentication can be achieved in public key cryptography. Assume that confidentiality is not required. **[02]**

.

Q.3	**(a)**	1.	Briefly explain the functionality of Tunnel mode for AH, ESP (encryption only) and ESP (encryption and Authentication)	**[06]**
		2.	What is the reason for having IPSEC even though SSL is already there?	**[01]**
	(b)	1.	Show in a tabular format different security services which are available in ESP (Encryption + Authentication) protocols in IPSEC.	**[06]**
		2.	Briefly explain "Security Association" in IPSEC.	**[01]**

OR

Q.3	**(a)**	1.	Mention and briefly explain the services available in PGP.	**[05]**
		2.	Which algorithms are used for compression and email compatibility in PGP?	**[02]**
	(b)			
		1.	Briefly explain the structure/format indicating the different fields of Private Key Ring in PGP.	**[05]**
		2.	Mention any one algorithm used in PGP for digital signature and message encryption.	**[02]**
Q.4	**(a)**	1.	Briefly explain different categories of intruders.	**[03]**
		2.	Briefly explain the different metrics useful for profile based intrusion detection.	**[04]**
	(b)	1.	Explain: Rule based Intrusion Detection	**[05]**
		2.	Write a note on: Honey-Pots	**[02]**

OR

Q.4	**(a)**	1.	Explain the general format of Intrusion Detection specific audit records.	**[06]**
		2.	What do you mean by false positive and false negative in Intrusion Detection System?	**[01]**
Q.4	**(b)**	1.	Draw the schematic diagram of SSL protocol stack and briefly explain the purpose of any three SSL protocols.	**[05]**
		2.	What is the reason for having SSL even though IPSEC is already there?	**[02]**
Q.5	**(a)**	1.	Mention and briefly explain the different parameters/fields based upon which packet filtering is normally done.	**[06]**
		2.	Between default discard and default accept policy in packet filtering firewalls, which one is better and why?	**[01]**

	(b)	1.	Briefly explain Access Control List and Capability List	**[04]**
		2.	Briefly explain the "No Read Up" and "No Write Down" rules for Multi-Level Security.	**[02]**
		3.	What is a state-full inspection firewall?	**[01]**

OR

Q.5	**(a)**	1.	Draw the schematic diagrams of popular firewall configurations/topologies.	**[06]**
		2.	Differentiate between stand-alone/desktop firewall and enterprise firewall.	**[01]**
	(b)	1.	Mention the general guidelines for creating a good password.	**[03]**
		2.	Just by drawing schematic diagram, show how new password is loaded and existing password is verified in Unix Systems.	**[04]**

****