Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

MCA - SEMESTER–V • EXAMINATION – WINTER • 2014

Subject Code: 2650002 Date: 01-12-2014

Subject Name: Network 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)** Answer in brief (any seven) **07**

1. What is message integrity?
2. What is peer entity authentication?
3. Differentiate between known plaintext and chosen plaintext.
4. How triple DES operation is carried out?
5. Differentiate between True and Pseudo random numbers.
6. Give one reason to have authentication without encryption.
7. Give digest size for SHA-1.
8. If $C = M^e \bmod n$, what is the value of M in RSA?
9. Write the full form of TGT.
10. What is a personal firewall?

(b) Answer in brief. (Any seven) **07**

1. What are the content of an authenticator in Kerberos v 4?
2. What is a *Subject* in X.509 certificate?
3. Write one reason for increment in security requirements of web in today's environment.
4. What is the purpose of the alert protocol in SSL?
5. What is Channel in SSH?
6. Write full form of WPA.
7. What is a controlled port in 802.1X?
8. Write full form of WAE.
9. How session keys are exchanged in PGP?
10. Write full form of DMZ.

Q.2 **(a)** Answer in brief. (Any seven) **07**

1. How key id is calculated in PGP?
2. What is clear signed data in SMIME?
3. Write one benefit IPsec provides to communication between routers.
4. What is stored in security policy database?
5. Write how original IP packet's addresses treated differently in transport and tunnel mode?
6. Who is a masquerader?
7. What is Gauge w.r.t. intrusion detection?
8. What is a honey pot?
9. What is IP address spoofing?

(b) 1. How security services, mechanisms and attacks are associated with each other? Give examples of each **04**

2. Differentiate between active and passive attacks **03**

OR

	(b)	1. What is a CIA triad? Explain each component if CIA triad in detail.	**04**
		2. Give any three examples of security violations.	**03**
Q.3	**(a)**	1. Give any four uses of random number in security applications.	**02**
		2. Give six requirements of the secure hash function.	**03**
		3. Provide two differences between transport and tunnel mode.	**02**
	(b)	1. Give six advantages of the counter mode.	**03**
		2. Explain how man in the middle attack takes place in Diffie Hellman key exchange.	**02**
		3.Give one example of how security associations are possible to be combined in IPsec.	**02**

OR

Q.3	**(a)**	1. Explain the process of generating message authentication code without using encryption.	**02**
		2. Explain two requirements for a secure use of symmetric encryption. Give proper examples.	**03**
		3. Explain how anti replay window works in IPsec.	**02**
	(b)	1. Write any three design requirements of HMAC.	**03**
		2. Write at least four important differences between a block and a stream cipher.	**02**
		3. Write how outbound traffic is processed with the first packet on a new secure connection in IPsec.	**02**
Q.4	**(a)**	1. Why is TGS introduced when AS can alone authenticate users?	**03**
		2. Differentiate between a session and a connection in SSL	**02**
		3. Differentiate between statistical anomaly detection and rule based detection.	**02**
	(b)	1. Write any two important differences between Kerberos 4 and 5.	**07**
		2. Explain three different ways to secure the web traffic using different layers.	
		3. What is the importance of salt value in password management?	

OR

Q.4	**(a)**	1. Differentiate between forward and backward certificates.	**02**
		2. Differentiate between fixed, ephemeral and anonymous Diffie Hellman in SSL.	**03**
		3. Differentiate between a proactive and reactive password checking.	**02**
	(b)	1. Explain these terms, key pair recovery, key pair update and cross certification.	**03**
		2. How connection close is processed in SSH?	**02**
		3. Write any two heuristic rules for intrusion detection.	**02**
Q.5	**(a)**	1. Explain Discovery phases for 802.11i.	**02**
		2. Explain the PGP process of generating a secure document from a plaintext document.	**03**
		3. Write any four requirements of a bastion host.	**02**
	(b)	1.Explain the process of four way handshake used in 802.11i	**03**
		2. Why compression is applied before encryption in PGP?	**02**
		3. Explain any two controls provided by firewalls except the service control.	**02**

OR

Q.5	**(a)**	1. Explain Authentication phases for 802.11i.	**02**
		2. Explain how enveloped data is generated in SMIME	**03**
		3. Explain how circuit level gateway works.	**02**
	(b)	1. Explain any three security services provided by WAP architecture.	**03**
		2. Explain any two enhanced security services by SMIME.	**02**
		3. Write how distributed firewalls are different from conventional firewalls.	**02**

****