GUJARAT TECHNOLOGICAL UNIVERSITY
MCA - SEMESTER– V• EXAMINATION – WINTER • 2015

Subject Code: 650002   **Date:03/12/2015**
Subject Name: Network Security
Time:10.30 AM TO 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)** Attempt the following   **14**
1. What is data confidentiality?
2. Difference between passive and active attack.
3. Define MAC?
4. Define digital signature.
5. What are the two basic functions used in encryption algorithms?
6. What is the difference between a block cipher and a stream cipher?
7. What is firewall?
8. What is the difference between internal and external firewall?
9. What is salt in the context of Unix password management?
10. What is honeypot?
11. What is IP address spoofing?
12. What is the difference between SSL connection and SSL session?
13. Function of authentication server in Kerberos?
14. Give difference between signed data and clear signed data function of S/MIME.

Q.2 **(a)** Describe stream generation in variable key-size stream cipher with byte-oriented operations algorithm.   **07**
(b) Explain RSA and Perform encryption for plain text N using RSA algorithm with p=3 q=11 e=7 and N=33.   **07**

OR

(b) Users A and B use the Diffie Hellman key exchange technique a common prime q=23 and a primitive root alpha=11.
1. If user A has private key XA =6 what is A's public key YA?
2. If user B has private key XB =5 what is B's public key YB?
3. How man in middle attack can be performed in Diffi Hellman algorithm?   **07**

Q.3 **(a)** Explain how the messages are generated and received by PGP.   **07**
(b) Explain public key infrastructure.   **07**

OR

Q.3 **(a)** Explain three requirements with respect to different keys use by PGP. **07**
(b) List requirements of hash function.   **07**

Q.4 **(a)** 1. Write a short note on anti reply window.   **04**
          2. Draw diagram of HMAC.   **03**
(b) 1. Explain client hello message of handshake protocol.   **04**
          2. Explain key and policy information category of extension field in X.509 version 3. **03**

OR

Q.4 **(a)** Define SET. Explain SET participants.   **07**
(b) 1. Explain any four ISAKMP payload types.   **04**

2. Explain field of detection specific audit record developed by Dorothy denning. **03**

Q.5 **(a)** 1. List requirements not satisfied by X.509 version 2. **04**

2. Draw a diagram which gives the overview of KERBEROS. **03**

(b) 1. Explain any one technique for developing an effective and efficient proactive password checker. **04**

2. Give difference between transport mode and tunnel mode. **03**

OR

Q.5 **(a)** 1. Explain process for inbound packet in IPsec. **04**

2. Mention purpose of padding in ESP. **03**

(b) 1. Lists four general techniques that firewalls use to control access and enforce the site's security policy. **04**

2. What are the default policies uses by packet filter firewall? And also explain below rule set. **03**

Rule Set

Action	Src	Port	Dest	Port	Flag
allow	{our host}	*	*	25	-
allow	*	25	*	*	ACK

****