Seat No.: _____ **Enrolment No._____**

GUJARAT TECHNOLOGICAL UNIVERSITY

MCA SEM-V Examination- Dec.-2011

Subject code: 650002 **Date: 14/12/2011**

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)** Write answers in brief (Any 7) **07**

1. Give one major difference between a passive and an active attack.
2. Give one major difference between a stream and a block cipher
3. Name the technique to be used for protecting against active attacks.
4. Diffie Hellman is vulnerable to man in the middle. Prove.
5. What is the significance of Nonce in Kerberos?
6. Why Kerberos need a ticket granting server?
7. What is a key ring in PGP?
8. What is a clear signed message in SMIME?
9. How routers benefit from IPsec? Explain one benefit.

(b) Write answers in brief (Any 7) **07**

1. Differentiate between transport and tunnel mode in IPsec
2. At which layer of OSI model the SSL (or TLS) protocol works?
3. What is the need of acquirer in SET?
4. Write the principle on which the Intrusion detection is based.
5. What is a honey pot?
6. What is default discard policy in firewalls
7. What is dual home bastion in firewall configuration?
8. Write two rules needed for multilevel trusted systems
9. What is a protection profile in common criteria for Information security evaluation?

Q.2 **(a)** Explain following terms with example (Any 7) **07**

1. Non repudiation
2. Trojan horse defense
3. Stateful firewall
4. Proactive password checking
5. Dual signature (w.r.t. SET)
6. Anti-replay service (w.r.t. IPsec)
7. Key legitimacy field (w.r.t. PGP)
8. Authentication server (w.r.t. Kerberos)
9. Digital Signature

(b) Explain cipher block chaining mode with example. **07**

OR

(b) For a Feistel cipher structure, explain terms block size, key size, number of rounds, subkey generation algorithm, round function, fast software encryption-decryption and ease of analysis. **07**

Q.3 **(a)** 1. What is a hash function? (1) **07**

2. What is additionally required in a hash function to be used for authentication? (2)
3. What is HMAC? (2)

4. Why it is useful? (2)

(b) 1. Write any four important differences between Kerberos version 4 and 5. (4) **07**

2. Explain fields Serial Number, subject name and extensions for public key cryptography.(3)

OR

Q.3 **(a)** 1. How PGP constructs a secure mail? Write the steps involved in the process. (4) **07**

2. Site reasons for using encryption before compression and compression before authentication.(3)

(b) 1. How enveloped data is constructed in SMIME. Write all steps for the same (4) **07**

2. What is the need for using both, symmetric and asymmetric keys in construction of EnvelopedData? (2)

3. What is the need of smime-type field in EnvelopedData? (1)

Q.4 **(a)** 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**

(b) 1. How Oakley key exchange protocol improves on Diffie-Hellman? (4) **07**

2. Show what ISAKMP proposal, transfer and notification payloads are used for. (3)

OR

Q.4 **(a)** 1. Why web security is more important issue today? List at least four reasons for the same. (4) **07**

2. How message authentication code is computed in SSL? (2)

3. What does the ChagneCipherSpec protocol do? (1)

(b) 1. What is the need of pseudo random function used in TLS? (2) **07**

2. How pseudo random function is calculated? (2)

3. How pseudo random function is used in the calculation of secure hash function and other information? (3)

Q.5 **(a)** 1. Write at least four ways for intruder's to learn passwords of their victims.(2) **07**

2. List one advantage of Intrusion detection.(1)

3. Differentiate between profile based and threshold detection methods of statistical anomaly detection (2)

4. Differentiate between anomaly detection and penetration identification methods of rule based anomaly detection (2)

(b) 1. How Unix manages passwords to make it secure from attackers? (3) **07**

2. What is the problem if bad password list is stored and compared when user enters the password for proactive password checking? (2)

3. Explain how one can use Markov model for proactive password checking.(2)

OR

Q.5 **(a)** 1. What is a packet filtering router? (1) **07**

2. Explain how attacks like 1) IP address spoofing, 2) source routing and 3) Tiny fragments can be carried out on packet filtering routers? What are the counter measures? (6)

(b) Write down at least 7 characteristics of a bastion host and explain their need with an example. **07**

****