Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

MCA - SEMESTER–V • EXAMINATION – WINTER 2013

Subject Code: 650002 Date: 27-11-2013

Subject Name: Network Security

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)** Explain following terms in a sentence or two (Any 7) **07**

1. Denial of Service
2. Data Integrity
3. Message Authentication Code
4. Man in the Middle Attack
5. Ticket (W R T Kerberos)
6. Authenticator (W R T Kerberos)
7. Forward Certificate
8. Key rings in PGP
9. Clear Signed Data in S/MIME

(b) Describe the usefulness of the following in a sentence or two (Any 7) **07**

1. Tunnel mode
2. Oakley Key Determination Protocol over Diffi-Hellman
3. Delete Payload in ISAKMP
4. Integrity Check Value in IPsec.
5. Handshake protocol in SSL
6. PRF in TLS
7. Audit record in IDS
8. Salt in password management
9. Multi-level security

Q.2 **(a)** Give an example of following (Attemp Any Seven) **07**

1. Replay attack
2. Authentication
3. Encryption
4. Collision in hash function
5. Encryption system dependence in Kerberos 4
6. Subject name in X.509 certificate
7. A rule in firewall
8. Heuristic in rule based IDS
9. MIME message

(b) 1. Write any 2 **06**

a) Explain how 3DES works. Why it works on EDE mode rather than EEE mode?
b) How MAC is calculated using one-way hash function?
c) Write at least two important differences between a block and a stream cipher.

2. Write full form of PGP **01**

OR

(b) 1. Write any 2 **06**

a) Write two differences between session key and permanent key
b) Write two important advantages of public key cryptography over shared secret key based cryptography
c) Write any two objectives for HMAC design.

2. Write what is ciphertext only attack in brief **01**

Q.3 (a) 1. Answer any 2 **06**
a) Differentiate between ticket granting ticket and service granting ticket
b) What serial number and issuer name fields signify in X.509 certificate?
c) Write what are roles of Certification Authority, Registration Authority, CRL issuer and repository w r t PKI.

2. What is Kerberos realm? Explain in brief. **01**

(b) 1. Answer any 2 **06**
a) Write steps PGP performs to calculate digital signature of the mail
b) Write clear reasons for PGP to compress after the signature generation process and not before.
c) How SMIME generates EnvelopedData? Write all four steps.

2. Write the purpose of RFC 822 w r t S/MIME **01**

OR

Q.3 (a) 1. Write any 2. **06**
a) Write any two routing applications of IPsec.
b) What Sequence Counter Overflow and Anti-replay window fields mean for an SA?
c) How cookie exchange helps avoiding clogging attack by Oakley?

2, Write full form of IPsec **01**

(b) 1. Write any 2 **06**
a) Write any two reasons for web security being an important issue for administrators.
b) What are client and server random? Why they are used?
c) Explain what alert codes insufficient_security and export_restriction mean.

2. At which layer SSL or TLS works? **01**

Q.4 (a) 1. write any 2 **06**
a) Write any two methods of learning passwords
b) What are honey pots? How they help learning about attacker activities?
c) What is proactive password checking? Why it is better than other password checking techniques?

2. Write who Masquerader is **01**

(b) 1. Write any 2 **06**
a) Explain how firewalls provide service and directional control over the content.
b) Explain what a tiny fragment attack is
c) Differentiate between application level gateway and circuit level gateway.

2. Give one reason why firewall has become important component of the security infrastructure. **01**

OR

Q.4 (a) 1.write any 2 **06**

a) Explain terms cryptanalysis and brute force attack.
b) Give two reasons of choosing AES over 3DES
c) Explain what cipher feedback mode is with example.

2. explain what a denial of service attack is **01**

Q.4 (b) 1. Write any 2. **06**

a) Explain why one-way property of secure hash function is important to observe.
b) Explain the process of HMAC calculation from message
c) Show how Diffie-Hellman is vulnerable to man in the middle attack.

2. Write what a digital signature is **01**

Q.5 (a) 1. Write any 2 **06**

a) Show any two differences between Kerberos version 4 and 5.
b) Show the usefulness of nonce in Kerberos dialogs
c) Why the three way handshake in X.509 authentication process require additional message indicating the signed copy of nonce sent by the receiver?

2. write full form of PKI **01**

(b) 1. Write any 2. **06**

a) Write any two reasons for PGP popularity
b) List all PGP services.
c) List the content of PGP private key ring and explain any one of them

2. write full form of PGP **01**

OR

Q.5 (a) 1. Write any 2 **06**

a) Write any two benefits of IPsec
b) Explain what security association is w r t IPsec.
c) Why proposal and key exchange payloads are used in ISAKMP?

2. Write full form of ISAKMP **01**

(b) 1. Write any 2 **06**

a) What is the difference in message authentication code calculation process in SSL and TLS?
b) Write the steps taken by SSL to calculate master secret.
c) What is the role of function P_hash() in TLS?

2. Write full form of SET **01**

****