Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

MCA - SEMESTER– V• EXAMINATION – WINTER 2015

Subject Code:2650002 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)** Write any seven in one or two sentences **07**

1. Differentiate between active and passive attacks
2. What is data origin authentication?
3. What is trusted third party?
4. How many keys one need in public key cryptography?
5. How a block cipher is different from stream cipher?
6. What is a one way hash function?
7. Write one advantage of counter mode
8. How can one achieve MAC without using any form of encryption?
9. Write any one use of public key encryption which is not possible with secret key encryption.
10. What is a realm in Kerberos?

(b) Write any seven in one or two sentences **07**

1. What is the job of the ticket granting server in Kerberos?
2. What is a subject name in X.509 certificate?
3. What is session in TLS?
4. What is the purpose of alert message in TLS?
5. Write any two types of tunnel in SSH.
6. What does happen during the discovery phase in 802.11i?
7. When are group master keys used in 802.11i?
8. Write the full form of WDP.
9. Write any two reasons for PGP being popular.
10. What does radix-64 step do in PGP?

Q.2 **(a)** Write any seven in one or two sentences **07**

1. What is clear signed data in SMIME?
2. Write one benefit of IPsec.
3. What is traffic flow confidentiality padding in IPsec?
4. Write one example of combining security association in IPsec.
5. Who is masquerader?
6. How distributed intrusion detection is is different from conventional IDS?
7. What is salt? Why it is used in password management?
8. Write any two things firewalls are capable of doing.
9. What is state-full inspection firewall?
10. How personal firewalls are different from normal firewalls?

(b) Write any two
1. Write two requirements for secure use of symmetric encryption. **07**
2. Write two different methods for constructing MAC using encryption.
3. Explain the process Kerberos V_4 uses for inter-realm communication

OR

(b) Write any two **07**
1. Explain the difference between anonymous and ephemeral Diffie-Hellman methods used in SSL.
2. Write the steps PGP uses to provide confidentiality to a document.
3. How IPsec helps routers in communication? Give one example.

Q.3 **(a)** Write any two **07**
1. Explain how statistical anomaly detection takes place in IDS.
2. Explain how packet filter firewall works with an example.
3. What is non repudiation? How it can be achieved?

(b) Write any two **07**
1. Explain what is cryptanalysis and write at least two types of them
2. Explain
    a. What is pre-image resistance and
    b. Weak collision resolution

    for a secure hash function.
3. Explain the difference between session and permanent keys in Kerberos.

OR

Q.3 **(a)** Write any two **07**
1. Explain how security mechanisms and services are related by giving one example
2. Explain peer entity authentication with example.
3. Write any four challenges faced by computer security today.

(b) Write any two **07**
1. Explain how counter mode works.
2. Write any two design considerations for stream cipher and explain in brief.
3. Write any four characteristics of feistel structure.

Q.4 **(a)** Write any two **07**
1. Explain how man in the middle attack is possible in Diffie Hellman.
2. Explain how RSA can help encrypt using one key while decryption is possible using another.
3. Write any four design objectives for HMAC

(b) Write any two **07**
1. In X.509 options for key and policy information, what is the need for
    a. Key usage and
    b. Private key usage period?
2. What is an authenticator? Why it is needed with the ticket in Kerberos?
3. Write any two improvements provided by Kerberos version 5 over version 4

OR

Q.4 **(a)** Write any two **07**

1. Explain how port forwarding is done in SSH
2. Write two important differences between TLS and SSL
3. Explain phase-2 of handshake protocol in SSL/TLS.

(b) Write any two **07**

1. Explain two different modes in which WPA2 security is provided in wireless security.
2. What is the purpose of HTML filter in WAP infrastructure?
3. How pre-shared key is used in 802.11i?

Q.5 **(a)** Write any two **07**

1. Explain how Enveloped Data is generated in SMIME
2. What is the meaning of
    a. Key owner,
    b. Partial trust,
    c. X is signed by y,
    d. Key is legitimate

    in web of trust by PGP?
3. Describe the structure of a PGP message, describing every component is brief.

(b) Write any two **07**

1. What is anti-replay service in IPsec? Explain.
2. Explain the difference between transport and tunnel mode in IPsec.
3. Explain how IP traffic is processed in IPsec for outbound packets.

OR

Q.5 **(a)** Write any two **07**

1. How proactive password checker works? Write any two challenges such a password checker would face.
2. How Unix manages passwords? Explain with example.
3. Explain the process of rule based intrusion detection.

(b) Write any two **07**

1. What is DMZ? Describe how DMZ is configured in firewalled network.
2. Explain what service level gateway is. How it is different from application-level gateway?
3. Write any two firewall categories and explain.

****