

**JK Lakshmipat University Jaipur**  
**INSTITUTE OF ENGINEERING AND TECHNOLOGY**

End Term Examination (Regular), April- May 2016  
B.Tech. in Computer Science and Engineering, Semester VI



Roll No.....

CSE609: INFORMATION SECURITY

Time: 03 hours

Max. Marks: 100

**Instructions to students:**

1. Do not write anything other than your roll number on question paper.
2. Assume suitable data wherever required and mention it clearly.
3. Writing appropriate units, nomenclature, and drawing neat sketches/schematics/ flow chart wherever, required are an integral part of the answer.

**Q.1A Objective type multiple choice questions (10 questions @ 1 mark)**

**10**

- i. Network layer firewall works as a
  - a) frame filter
  - b) packet filter
  - c) both (a) and (b)
  - d) none of the mentioned
- ii. Message digest needs to be
  - a) Public
  - b) private
  - c) kept secret
  - d) None
- iii. The primary goal of the ..... protocol is to provide a private channel between communicating application, which ensures privacy of data authentication of the partners, and integrity.
  - A) SSL
  - B) ESP
  - C) TSL
  - D) PSL
- iv. The DoS attack is which the attacker sends deluge of packets to the targeted host
  - a) Vulnerability attack
  - b) Bandwidth flooding
  - c) Connection flooding
  - d) All of the mentioned
- v. State whether true or false.
  - i) A worm mails a copy of itself to other systems.
  - ii) A worm executes a copy of itself on another system.
  - A) True, False
  - B) False, True
  - C) False, False
  - D) True, True
- vi. An intrusion detection system does not perform which of the following?
  - a) Tries to identify attempts to hack into a computer system.
  - b) May monitor packets passing over the network.
  - c) May transmit message packets to the correct destination.
  - d) Set up deception systems that attempt to trap hackers.
- vii. In Information Security, a "Trojan Horse" refers to a:
  - a) a computer virus
  - b) a useful, or apparently useful, program or command procedure but with

|       |                                                                                                                                                                                                                                                                                                                           |           |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
|       | hidden (malicious) side-effects                                                                                                                                                                                                                                                                                           |           |
|       | c) program that sends large volumes of unauthorized e-mail                                                                                                                                                                                                                                                                |           |
|       | d) program which secretly takes over another networked computer, and then uses it to launch further attacks                                                                                                                                                                                                               |           |
| viii. | For which type of communication is mostly used the "one-way authentication"?                                                                                                                                                                                                                                              |           |
|       | a) Web surfing                                                                                                                                                                                                                                                                                                            | b) Telnet |
|       | c) FTP                                                                                                                                                                                                                                                                                                                    | d) E-mail |
| ix.   | Which three functional areas are provided by IPSec?                                                                                                                                                                                                                                                                       |           |
|       | a) Authentication, Confidentiality, and Key management                                                                                                                                                                                                                                                                    |           |
|       | b) Authentication, Error detection, and Error correction                                                                                                                                                                                                                                                                  |           |
|       | c) Authentication, Key generation, and Certificate exchange                                                                                                                                                                                                                                                               |           |
|       | d) Encryption, Decryption, and Certificate validation                                                                                                                                                                                                                                                                     |           |
| x.    | In direct digital signatures, signing can be done                                                                                                                                                                                                                                                                         |           |
|       | a) only on the whole message                                                                                                                                                                                                                                                                                              |           |
|       | b) only on the hash of the message                                                                                                                                                                                                                                                                                        |           |
|       | c) either on the whole message or on the hash of the message                                                                                                                                                                                                                                                              |           |
|       | d) on the public key of the receiver                                                                                                                                                                                                                                                                                      |           |
| Q.2   | Short answer type questions (4 questions @ 2.5 marks)                                                                                                                                                                                                                                                                     | 10        |
| i.    | How does an authentication system differ from a firewall in functioning?                                                                                                                                                                                                                                                  |           |
| ii.   | Please classify each of the following as a violation of<br>(1) confidentiality (2) integrity (3) availability (4) non-repudiation<br>(a) A copies B's homework<br>(b) A crashes B's operating system<br>(c) A changes the amount on B's check from 100 to 1000<br>(d) A does not honor the contract between him/her and B |           |
| iii.  | What is one -way authentication?                                                                                                                                                                                                                                                                                          |           |
| iv.   | List the types of cryptanalytic attacks.                                                                                                                                                                                                                                                                                  |           |
| Q.3A  | Use Play fair cipher with key 'firstamend' to decrypt the cipher text "gixqiupeelqs"?                                                                                                                                                                                                                                     | 05        |
| Q.3B  | Which parameters and design choices determine the actual algorithm of a feistel cipher?                                                                                                                                                                                                                                   | 05        |
| Q.4A  | Vigenere cipher is under consideration. Use the following tableau with key "cipher" to decrypt the message -<br>"Kbxzirugivvrkatuyddmgzxfrwllvj"                                                                                                                                                                          | 05        |
| Q.4B  | Can a MAC provide non-repudiation? If yes, explain. If no, explain why not?                                                                                                                                                                                                                                               | 05        |
| Q.5A  | A plaintext has been double transposed using first 632415 and then 564231 as the key. As a result we obtain cipher text<br>"ASFCENKREREEOEELTQDIECEOUVD AJW"                                                                                                                                                              | 05        |

Decrypt the cipher text.

Q.5B What is difference between a message authentication code and a one-way hash function? 05

OR

Q.5B What is PGP? How authentication and confidentiality is maintained in PGP. 05

Q.6A Users A and B use the Diffie Hellman key exchange technique, a common prime  $q=11$  and a primitive root  $\alpha=7$ . 05

(i) If user A has private key  $X_A=3$ . What is A's public key  $Y_A$ ?

(ii) If user B has private key  $X_B=6$  What is B's public key  $Y_B$ ?

(iii) What is the shared secret key?

Q.6B What is digital certificate? What information does it contain? Give its use in present day applications. 05

Q.7A What is the difference between virus and worm? What are typical phases of virus operation? 05

Q.7B Describe the following with respect to Kerberos Version. 4: 05  
i. Authentication Server ii. Ticket Granting Server

OR

Q.7B Bob has public RSA key ( $n = 65$ ,  $e = 5$ ) Show that Bob's private key is ( $d = 29$ )? 05  
Alice wants to send the message  $m = 11$  to Bob. She encrypts the message using Bob's public key. What is the value of the cipher text that Alice sends to Bob?

Q.8A What is role of firewall in network security? List the different types of firewalls and give the functioning of any one of them. 10

Q.8B What are the steps for preparing an enveloped data for a MIME entity? 05

OR

Q.8B What services are provided by IPSec? Also describe the security associations and SA parameters required for IPSec implementation. 05

Q.9A Discuss the following with respect to SSL Architecture: 10  
i. SSL session ii. SSL Connection

Q.9B What is SET? Explain how Secure Electronic Transaction is used for E- Banking with suitable block diagrams in terms of card holders purchase request and verification by the merchants. 05

OR

Q.9B What are the three benefits provided by IDS (Intrusion Detection System)? 05

