



Name :
Roll No. :
Invigilator's Signature :

CS / B.TECH (CSE) / SEM-8 / CS-802D / 2011

2011

NETWORK SECURITY

Time Allotted : 3 Hours

Full Marks : 70

The figures in the margin indicate full marks.

*Candidates are required to give their answers in their own words
as far as practicable.*

GROUP - A

(Multiple Choice Type Questions)

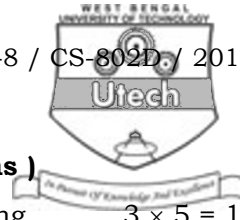
1. Choose the correct alternatives for any *ten* of the following :

10 × 1 = 10

- i) Which one of the following is active attack ?
 - a) Masquerade
 - b) Traffic analysis
 - c) Evaesdropping
 - d) Shoulder surfing.
- ii) Which one of the following is passive attack ?
 - a) Masquerade
 - b) Traffic analysis
 - c) Replay attack
 - d) Denial of service.
- iii) A Firewall that uses two TCP connections is
 - a) Bastion
 - b) Application gateway
 - c) Circuit level gateway
 - d) Packet filter.
- iv) IP Sec services are available in layer.
 - a) application
 - b) data link
 - c) network
 - d) transport.



- v) Caesar Cipher is an example of
 - a) Substitution cipher
 - b) Transposition cipher
 - c) Substitution as well as Transposition cipher
 - d) none of these.
- vi) DES encrypts blocks of bits.
 - a) 32
 - b) 56
 - c) 64
 - d) 128.
- vii) The Authentication Header (AH) protocol, part of IPsec, provides which of the following security functions ?
 - a) Source authentication
 - b) Data integrity
 - c) Data confidentiality
 - d) Source authentication and data integrity.
- viii) To verify a digital signature, we need the
 - a) Sender's private key
 - b) Sender's public key
 - c) Receiver's private key
 - d) Receiver's public key.
- ix) The Secure Sockets Layer (SSL) provides
 - a) encryption for messages sent by both client and server
 - b) server authentication
 - c) optional client authentication
 - d) all of these.
- x) A worm modify a program.
 - a) does not
 - b) does
 - c) may or may not
 - d) none of these.
- xi) A macro virus is platform
 - a) dependent
 - b) independent
 - c) limited
 - d) none of these.
- xii) prevents either sender or receiver from denying a transmitted message.
 - a) Access control
 - b) Non-repudiation
 - c) Encryption
 - d) Integrity.



GROUP – B
(Short Answer Type Questions)

Answer any *three* of the following. $3 \times 5 = 15$

2. What is Triple DEA ? Why is it more secure than DES ?
3. What is digital signature and why is it used ?
4. Explain briefly Diffie-Hellman symmetric key exchange algorithm.
5. Explain Cipher Block Chaining mode with a suitable diagram.
6. Differentiates between transport and tunnel modes of operation of IPsec.

GROUP – C
(Long Answer Type Questions)

Answer any *three* of the following. $3 \times 15 = 45$

7.
 - a) What are different classes of intruders ?
 - b) Explain briefly host-based, network-based and application-based intrusion detection systems.
 - c) Give a brief description of UNIX password management.
 - d) Explain briefly how stealth viruses work.
8.
 - a) What is a firewall ?
 - b) What are different types of firewall ? Briefly explain working principle of each.
 - c) What are the limitations of firewall ?
 - d) What is a worm ? How does it differ from a virus ?

$3 + 6 + 3 + 3$

$2 + 6 + 3 + 4$



9. a) What are the different security services provided by PGP ?
- b) Explain how PGP provides confidentiality and authenticity of electronic mails.
- c) Explain the necessity of base-64 conversion in PGP.
- d) Distinguish between active attack and passive attack with suitable examples.
- e) What is message digest ? $3 + 5 + 2 + 3 + 2$
10. a) Describe the role of the Ticket Granting Ticket and Service Granting Ticket in Kerberos ?
- b) What are the services provided by IPsec ?
- c) What are the applications and advantages of IPsec ?
- d) What are the differences between authentication and authorisation ?
- e) What are the different entities involved in a secure electronic transaction ? $4 + 2 + 3 + 2 + 4$
11. Write short notes on any *three* of the following : 3×5
- a) SSL
- b) Cookies
- c) IP spoofing and DOS attacks
- d) Cryptanalysis
- e) Authentication Header
- f) RSA.

=====