CS/B.TECH (CSE) (SUPPLE)/SEM-8/CS-802D/09
NETWORK SECURITY (SEMESTER - 8)

1. ....
Signature of Invigilator

2. ....
Signature of the Officer-in-Charge

Reg. No. | | | | | | | | | | | | | | | |

Roll No. of the Candidate | | | | | | | | | | | | | | | |

CS/B.TECH (CSE) (SUPPLE)/SEM-8/CS-802D/09
ENGINEERING & MANAGEMENT EXAMINATIONS, JULY – 2009
NETWORK SECURITY (SEMESTER - 8)

Time : 3 Hours] [Full Marks : 70

INSTRUCTIONS TO THE CANDIDATES :

1. This Booklet is a Question-cum-Answer Booklet. The Booklet consists of **32 pages**. The questions of this concerned subject commence from Page No. 3.
2. a) In **Group – A**, Questions are of Multiple Choice type. You have to write the correct choice in the box provided **against each question**.
   b) For **Groups – B** & **C** you have to answer the questions in the space provided marked 'Answer Sheet'. Questions of **Group – B** are Short answer type. Questions of **Group – C** are Long answer type. Write on both sides of the paper.
3. **Fill in your Roll No. in the box** provided as in your Admit Card before answering the questions.
4. Read the instructions given inside carefully before answering.
5. You should not forget to write the corresponding question numbers while answering.
6. Do not write your name or put any special mark in the booklet that may disclose your identity, which will render you liable to disqualification. Any candidate found copying will be subject to Disciplinary Action under the relevant rules.
7. **Use of Mobile Phone and Programmable Calculator is totally prohibited in the examination hall.**
8. You should return the booklet to the invigilator at the end of the examination and should not take any page of this booklet with you outside the examination hall, **which will lead to disqualification**.
9. Rough work, if necessary is to be done in this booklet only and cross it through.

No additional sheets are to be used and no loose paper will be provided

---

FOR OFFICE USE / EVALUATION ONLY

Marks Obtained

	Group – A										Group – B			Group – C				
Question Number																	***Total Marks***	***Examiner's Signature***
Marks Obtained																		

....
Head-Examiner/Co-Ordinator/Scrutineer

S-53029 (29/07)

DO NOT WRITE O

DO NOT WRITE ON THIS PAGE

CS/B.TECH (CSE) (SUPPLE)/SEM-8/CS-802D/09

NETWORK SECURITY

SEMESTER - 8

Time : 3 Hours] [Full Marks : 70

GROUP – A

(Multiple Choice Type Questions)

1. Choose the correct alternatives for any *ten* of the following : 10 × 1 = 10

i) Caesar Cipher is an example of

a) Substitution Cipher

b) Transposition Cipher

c) Substitution as well as Transposition Cipher

d) none of these. □

ii) Symmetric key cryptography is .... asymmetric key cryptography.

a) always slower than b) of the same speed as

c) faster than d) usually slower than. □

iii) In .... attacks, there is no modification to measage contents.

a) passive b) active

c) both of these d) none of these. □

iv) A .... replicates itself by creating its own copies, in order to bring the network to a halt.

a) virus b) worm

c) Trojan horse d) bomb. □

v) There are .... rounds in DES.

a) 8 b) 10

c) 14 d) 16. □

vi) A .... is used to verify the integrity of a message.

a) message digest b) decryption algorithm

c) digital envelope d) none of these. □

vii) SSL layer is located between

a) transport layer, network layer

b) application layer, transport layer

c) data link layer, physical layer

d) network layer, data link layer. □

viii) IPSEC provides security at the

a) application b) transport

c) network d) session. □

ix) .... is a message digest algorithm.

a) DES b) IDEA

c) MD5 d) RSA. □

x) In Kerberos, ... shares a unique password with every user in the system.

a) AS b) TCT

c) TGS d) file server. □

xi) Encryption in IPSEC is done by

a) tunnel mode b) Transport mode

c) IKE d) ESP. □

GROUP – B

(Short Answer Type Questions)

Answer any *three* of the following. 3 × 5 = 15

2. Explain different types of attacks with examples.

3. Explain the key generation process in DES.

4. What is the diffusion and confusion principle ? Which one is achieved by transposition cipher and substitution cipher ? 2 + 3

5. What is the difference between transport mode and tunnel mode used by IPSEC protocol ?

6. Why does PGP generate a signature before applying compression ? What is MIME and S/MIME ? 3 + 2

GROUP – C

(Long Answer Type Questions)

Answer any *three* of the following. 3 × 15 = 45

7. a) What do you mean by asymmetric key encryption ? Explain. 2

   b) What is the difference between symmetric key encryption and asymmetric key encryption ? 3

   c) Describe CBC mode of encryption process. What is Initialization Vector ? 2 + 1

   d) Encrypt the message 'meet me at the usual place at ten rather than eight O'clock' using the Hill cipher with the key $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$. Show your calculations and the result. 4

   e) Show the calculations for the corresponding decryption of the cipher text to recover the original plaintext. 3

8. a) Explain substituion, transposition cipher and product cipher with examples. (2 + 1) × 3

b) Briefly define the Playfair cipher. Find the cipher text for the plain text "WEST BENGAL UNIVESITY OF TECHNOLOGY" using Playfair cipher technique. The key here is "KOLKATA". Also find the decrypted cipher text. 2 + 4

9. a) Why is the SSL layer positioned between Application layer and Transport layer ? 4

b) Name the four key steps in the creation of a Digital certificate. 4

c) How is SHTTP different from SSL ? 3

d) What are the problems associated with clear text passwords ? 4

10. a) What do you mean by network security ? Explain with a suitable model. 3 + 1

b) Explain Brute-force attack with example. 3

c) What is Worm ? How is it different from a Virus ? 2 + 2

d) What are Trojan horse and Cookie ? 2 + 2

11. a) List three design goals for a firewall. 3

b) What are application-level gateway and circuit-level gateway ? 2 + 2

c) List and briefly define three classes of intruders. 3

d) What are two common techniques used to protect a password file ? 5

END