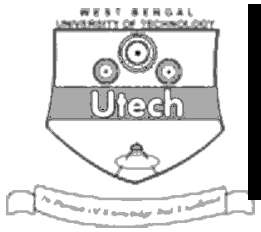
NETWORK SECURITY (SEMESTER - 8)

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



1. .....
Signature of Invigilator

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

Reg. No.

Roll No. of the Candidate

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

ENGINEERING & MANAGEMENT EXAMINATIONS, APRIL – 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

---

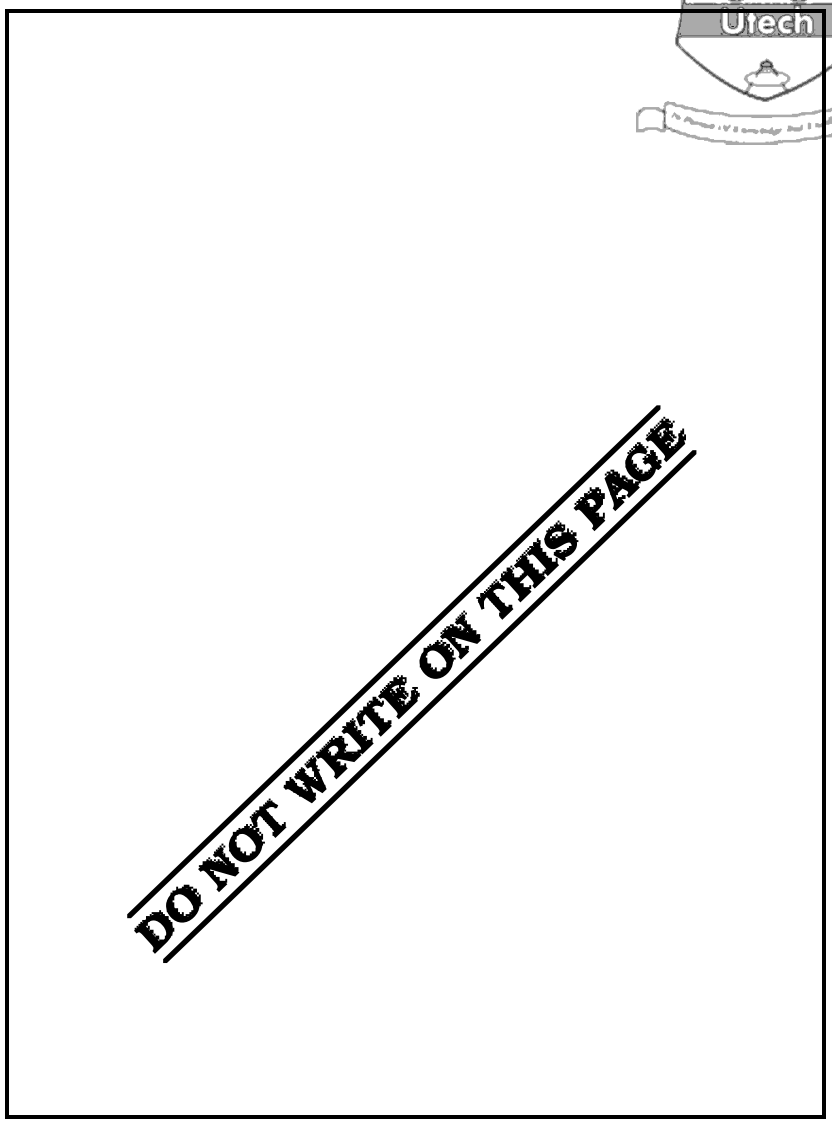
FOR OFFICE USE / EVALUATION ONLY

Marks Obtained

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

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

8876 D/F (27/04)


DO NOT WRITE ON THIS PAGE

ENGINEERING & MANAGEMENT EXAMINATIONS, APRIL – 2009

NETWORK SECURITY

SEMESTER - 8

Time : 3 Hours] [Full Marks : 70

GROUP – A

(Multiple Choice Type Questions)

1. Choose the correct alternatives for the following : 10 × 1 = 10

i) Rail Fence Technique is an example of

a) Substitution cipher b) Transposition cipher

c) Product cipher d) Caesar cipher. ☐

ii) SET is a

a) Electronic payment system

b) Security protocol

c) Credit card payment infrastructure

d) Internet payment system. ☐

iii) Public Key Cryptography is advantageous over Symmetric key Cryptography because of

a) speed b) space

c) key exchange d) key length. ☐

iv) The sub-key length at each round of DES is ..... bits.

a) 32 b) 56

c) 64 d) 48.

v) MAC is used to ensure

a) authentication

b) confidentiality

c) authentication and integrity

d) authentication and confidentiality.

vi) Total number of messages used in SSL handshake protocol is

a) 12 b) 10

c) 8 d) 14.

vii) A worm ..... modify a program.

a) does not b) does

c) may or may not d) none of these.

viii) Differential cryptanalysis can be mounted on

a) DES encryption algorithm

b) AES encryption algorithm

c) RSA encryption algorithm

d) Deffie-Hellman key exchange algorithm.

ix) Which one is the strong attack mechanism ?

a) Chosen plaintext attack

b) Chosen ciphertext attack

c) Chosen plaintext-ciphertext attack

d) Addative Chosen plaintext attack. [ ]

x) In DES encryption algorithm, which of the following is used for converting 32-bit right half into 48-bit ?

a) Permutation b) Expansion / Permutation

c) Substitution d) None of these. [ ]

GROUP – B

(Short Answer Type Questions)

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

2. What is digital certificate and why is it used ?

3. Explain Cipher Block Chaining mode with diagram.

4. Give a brief description of UNIX password management. Describe the utility of secure DNS. 3 + 2

5. Describe briefly the Alert protocol and Record protocol in SSL. 2 + 3

6. For security consideration, how can you select password ? Let H be a cryptographic hash function with message digest length is 160-bit and password (PW) be of 24-bit long. Then, discuss how dictionary attack can be mounted for guessing a password from H (PW). 2 + 3

GROUP – C

(Long Answer Type Questions)

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

7. a) How many round are there in DES ?

   b) Describe a single round of DES with block diagram.

   c) What is Triple DEA ? Why is it more secure than DES ?

   d) "Authentication can be achieved using DES." — Comment on it. 1 + 7 + 5 + 2

8. a) What is electronic money ?

   b) What is SET ? Explain with a suitable model.

   c) How pre-master-secret and master-secret is prepared in SSL handshake protocol ?

   d) Describe the fields of SSL record protocol header. 1 + 7 + 4 + 3

9. a) Describe SHA-1 (message digest) algorithm.

   b) How SHA-1 is differing from MD5 ?

   c) It is known that, in symmetric-key cryptography, it is difficult to share the same secret between two communicating parties. How can public-key cryptography solve this problem ?

   d) Give an example of a message authentication using symmetric-key and asymmetric-key cryptography. 7 + 2 + 4 + 2

10. a) What is factorization problem ?

    b) What is RSA cryptosystem ? Explain in detail.

c) How can chosen-plaintext attack be mounted on RSA ?

d) Let Alice, Bob, Chris and Eve communicate over a public network. They encrypt all messages they send using the RSA system. Bob and Chris have the RSA-modulus n_B and n_C respectively with $n_B = n_C$, but different public encryption exponents : $e_B \neq e_C$. Suppose that gcd $(e_B, e_C) = 1$, and that Alice sends the same secret message to Bob and to Chris. Show how Eve can decipher the message. 1 + 5 + 2 + 7

11. a) Explain briefly the Kerberos version 4.

b) Explain briefly, in the PGP, that how Bob and Alice exchange the secret key for encrypting messages.

c) Compare and contrast key management in PGP and S/MIME. 6 + 6 + 3

END