Total No. of Questions : 5]

SEAT No. : ____

P1793

[Total No. of Pages : 2

[5233]-33

M.Sc.

COMPUTER SCIENCE

CS 23-303 : Information Systems Security

(2008 Pattern) (Semester - III)

Time : 3 Hours] ***[Max. Marks : 80***

Instructions to the candidates:

1) ***All questions are compulsory.***
2) ***All questions carry equal marks.***
3) ***Neat diagrams must be drawn wherever necessary.***

Q1) Attempt all of the following. **[8×2=16]**

a) Define.

i) Fabrication

ii) Interruption

b) What is self signed certificate?

c) Explain the process of key wrapping.

d) Write any two objectives of designing Blowfish algorithm.

e) What are MIME headers in an e-mail message?

f) Explain Expansion permutation step of DES algorithm.

g) What are the problems with passwords?

h) What is address spoofing?

Q2) Attempt any four of the following. **[4×4=16]**

a) Explain one time initialization process of AES algorithm.

b) How does certificate based authentication works?

c) Explain in detail Handshake protocol of SSL.

d) Discuss working of Kerberos protocol.

e) Consider the plain text "ABCDEFGHIJKL" and one time password "QOPTSRWVUZYX". Using vernam cipher construct cipher text.

P.T.O.

Q3) Attempt any four of the following : **[4×4=16]**

a) Explain cipher feedback (CFB) mode of an algorithm.

b) Why digital certification revocation is needed? How online certificate revocation status check is done?

c) Explain SET process in detail.

d) Explain Biometric authentication process.

e) Consider the plain text "EXAM SECTION" and keyword " JACK AND JILL". Using playfair cipher construct cipher text.

Q4) Attempt any four of the following : **[4×4=16]**

a) Compare MD-5 and SHA-1 algorithms.

b) How does the CA signs the digital certificate?

c) Which security features are supported by PGP? Also explain steps of PGP.

d) Explain AH and ESP protocol.

e) Consider $n = 11$, $g = 7$, $x = 3$ and $y = 6$. Use Define Hellman Algorithm and find K_1 and K_2.

Q5) Attempt any four of the following : **[4×4=16]**

a) Explain key generation process of each round of IDEA.

b) What are different variations of DES algorithm?

c) Explain working of time stamping protocol (TSP).

d) How firewall perform network address translation?

e) Explain any four security principles.

✡ ✡ ✡