P1331

[3664]-349
B.E. (I.T.)
INFORMATION SYSTEM SECURITY
(2003 Course) (414441) Sem 1

Time : 3 Hours] *[Max. Marks : 100*

Instructions to the candidates:

1) ***Answer three questions from Section-I and three questions from Section-II.***
2) ***Answers to the two sections should be written in separate books.***
3) ***Neat diagrams must be drawn wherever necessary.***
4) ***Figures to the right indicate full marks.***
5) ***Your answers will be valued as a whole.***
6) ***Use of logarithmic tables, slide rule, Mollier charts, electronic pocket calculator and steam tables is allowed.***

SECTION - I

Q1) a) What are the two basic functions used in encryption algorithms? **[6]**

b) What is the difference between Monoalphabetics and Polyalphabetics cipher? **[6]**

c) What are the two problems with one time pad cipher? **[6]**

OR

Q2) a) Explain avalanche effect. **[6]**

b) What is the difference between block and stream cipher? **[6]**

c) Give examples of replay attacks. List approaches to deal with them. **[6]**

Q3) a) Show that enforcement rules of Clark-Wilson model can emulate the Biba model. **[8]**

b) Explain : **[8]**

i) Mandatory.
ii) Discretionary.
iii) Role based access controls.

OR

Q4) a) Discuss the role of trust in security policy. **[5]**

b) Discuss availability issues in security policies. **[5]**

c) Compare and contrast confidentiality Vs. integrity policies. **[6]**

P.T.O.

Q5) a) Compare and contrast the four modes of operation for block ciphers with respect to implementation complexity and strength of encryption. **[8]**

b) Explain meet-in-the-middle attack with help of Diffe-Hellman-algorithm. **[8]**

OR

Q6) a) Does repeated application of DES strengthens the security? Why or why not? **[8]**

b) What are the time and space complexities for a dictionary attack on MD5? **[8]**

SECTION - II

Q7) a) What are the limitations in using "rule based system" in general and firewalls in particular for peripheral security? **[6]**

b) Argue the merits and demerits of having specific servers (E-mail, web, etc) in DMZ **[6]**

"Authentication protocols that use random numbers are inherently more secure than the ones that don't use random numbers". Substantial or reject the statement. **[6]**

OR

Q8) a) The Alpha-Beta Corporation wants to provide a notarized email service with online notaries. The requirements for notaries are the same as human notary "Public" persons.

Identify and list the requirements for this service.
Provide a protocol that will meet your requirements.
Write the protocol in simple, clear and precise steps. **[8]**

b) In context of IDS systems compare and contrast **[10]**

i) Stateless Vs. Stateful IDS.
ii) Rule based system Vs. adaptive systems.
iii) Anomaly Vs. Misuse Detection.

Q9) a) What protocols comprise SSL? What is the difference between SSL session and SSL connection? **[8]**

b) Describe Kerberos Realm. **[8]**

OR

Q10) a) Distinguish between tunnel and transport mode. **[8]**

b) Define hash function, requirements of hash function and compare MD4 and MD5 algorithm. **[8]**

Q11) Write notes on (any two) : **[16]**

a) Vulnerability classification.

b) IPS (Intrusion Prevention Systems).

c) Storing and Revoking keys.

d) PGP.

OR

Q12) Write notes on (any two) : **[16]**

a) Cookies.

b) Penetration testing.

c) Steganography.

d) Digital immune system.