Total No. of Questions : 8]

SEAT No. :

P4895

[Total No. of Pages : 2

[5155]-21
M.E. (Computer Engineering)
DISTRIBUTED SYSTEMS
(2008 Pattern)

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

Instructions to the candidates:

1) ***Answer any three questions from each section.***
2) ***Answer to the two sections should be written in separate answer books.***
3) ***Figures to the right indicate full marks.***
4) ***Assume suitable data, if necessary.***

SECTION -I

Q1) a) Explain the trends in distributed systems. **[8]**

b) Explain the tiered architectural pattern for distributed system. **[8]**

Q2) a) Explain the design issues in Remote Method invocation. **[8]**

b) Elaborate "Web Search" as an example of distributed system. **[8]**

Q3) a) Explain bully algorithm. In the bully algorithm, a recovering process starts an election and will become the new coordinator if it has a higher identifier than the current incumbent. Is this a necessary feature of the algorithm? **[8]**

b) Explain the Cristian's method for synchronizing clocks. **[8]**

Q4) Write short notes on (any three) **[18]**

a) IP Multicast

b) Sun RPC

c) Clocks

d) Mutual Exclusion

P.T.O

SECTION -II

Q5) a) With the help of a schematic of file service architecture, explain different modules in it. **[8]**

b) Explain why iterative navigation is necessary in a name service in which different name spaces are partially integrated, such as the file-naming scheme provided by NFS. **[8]**

Q6) a) Explain the "Structure of data" as a design and implementation issue in distributed shared memory. **[8]**

b) Explain in brief-Causal and Processor Consistency models. **[8]**

Q7) a) Explain the role of servlet container in deploying of a web service and execution of a client request. **[8]**

b) Outline the main difference between TLS and XML security. Explain why XML is particularly suitable for the role it plays, in terms of these differences. **[8]**

Q8) Write short notes on (any three) **[18]**

a) Digital signatures with secret keys

b) WSDL

c) Global Name Service

d) Potential Attacks to computer systems

▲ ▲ ▲