ME (ICE) 2nd Semester Examination, 2012

Internet and Web based Technology (ICE 1002)

Time: 3hr Full Marks: 70

Use separate sheet for each half

First Half

Answer any 7 questions

1. Distinguish between active attack and passive security attack. Name some passive and active security attack. [3+2]
2. What is the block size in DES? What is the cipher key size in DES? What is the round key size in DES? Why does the DES function need an expansion permutation? [1+1+1+2]
3. Briefly explain the idea behind the RSA cryptosystem with a suitable example. Can you generate the public key and private key of RSA algorithm using two numbers like 19 and 21? [4+1]
4. Showing all the major steps explain how Kerberos generates the session key for two users. [5]
5. How session key is generated using "Diffie-Hellman" method when more than two people are involved in key generation? How man-in-the-middle-attack occur in above algorithm? [3+2]
6. Let us consider a class which inherits an abstract class and don't want to use all its abstract methods. Is that possible in JAVA? Justify your answer. [5]
7. Do you think that a member variable or method of any class can be accessed in JAVA from main class without any object reference? Explain the dynamic method dispatch in JAVA with suitable code. [2+3]
8. Briefly discuss JDBC architecture and types of JDBC drivers with suitable diagram. Write the advantages of JDBC. [3+2]
9. Describe the JSP lifecycle with suitable block diagram. With suitable diagram describe the execution steps of JSP. [2+3]

Second Half

Answer any 5 questions

Each question carries 7 marks

1. Target of ARPANET was to design a distributed system that could even survive after nuclear war. The ARPANET is the predecessor of today's Internet. Describe how much of its original target (to qualify as a distributed system) have been achieved by the Internet. In your discussion, mention the (application layer) protocols/ technologies which enable you to view the Internet as a distributed system.
   What are the challenges to be addressed, in your opinion, to make the Internet as a proper distributed system?
2. It is traditionally considered that arrival of packets in a network follows Poisson distribution. Do you believe that this consideration is alright for today's Ethernet / Internet? If yes, present a model for such kind of traffic.
   If not, state the properties of the traffic of Ethernet/ Internet. You should provide the reasons behind such behavior. Can you propose some model for such traffic?
3. Suppose, one has some reservation regarding TCP, and so, regarding the Transport layer. He/she wants to remove the layer from his/her network architecture. Propose a new architecture or modifications over existing one, so that the user processes in such situation can also get reliable service. Here, you may propose some new technologies to be incorporated in some layer, or assign some extra tasks to be performed by other layers.
4. Compare Path Vector Routing, Distance Vector Routing and Link State Routing. Which protocols use these routing techniques?
   Propose a new routing technique which does not require flooding (like Link State Routing), but can even work in mobile environment.
5. How does Ethernet decide to forward data to IP or to ARP or to other protocols?
   Write a scheme to discover the path from a source to destination.
6. Design $G(x)$ for CRC so that the burst error can be captured. Does CRC-32 (standardized by IEEE and used in Ethernet frame) capture all kinds of errors?
   Propose a hardware implementation of CRC using LFSR.
7. Write short notes on: ARQ protocols, virtual circuit switching, IP.