Assignment 5 (5% of total grade)

Instructions

Turn in hard copy of your answers at the beginning of the class next week.

Questions

1. Consider 5 processes that need to agree on their joint state. To protect against Byzantine failures, the processes adopted a protocol in two rounds. On the first round, each process broadcasts its own state to all others. On the second round, each process broadcasts its own view of the global state. Suppose that on the second round, process 1 receives the information provided below. Identify the faulty process(es), if any. Briefly justify your answer. (1%)

   From 2 got (3,4,1,5,8)

   From 3 got (3,3,1,5,8)

   From 4 got (3,3,1,5,8)

   From 5 got (3,3,1,5,8)

2. What is the difference between predictability and consistency in distributed software systems? (1%)
3. The goal of the call-return style of communication, such as adopted in RPC and RMI, is to allow callers to treat remote calls the same way as local calls. How is this goal affected by failures? Specifically, enumerate the kinds of failures that may affect this goal, and briefly explain how they can be mitigated. (1%)
4. What are the pros and cons of symmetric versus asymmetric cryptography? (1%)
5. Suppose that user A wishes to send a 500Kb message *m* to user B such that the message is authenticated as coming from user A and can only be read by user B. Furthermore, user A wishes to formulate the message so that it can be encrypted/decrypted within 15 seconds. Define the message that user A should send to user B, assuming that no symmetric keys are initially shared, and knowing that
   (a) the available public key algorithm can encrypt messages at the rate of 1Kbps,
   (b) the available symmetric key algorithm can encrypt/decrypt at a rate of 1Mbps,
   (c) a hashing algorithm can process messages at a rate of 100Kbps producing a 256 bit hash code, and
   (d) the size of both A's id, and symmetric key is 256 bits. (1%)