

December 16, 2002

Return to Bruce McNair by 5:00 pm, December 23, 2002

- Email (bmcnair@stevens-tech.edu)
- FAX: 732-335-9709

The midterm is open book/open notes, based on an individual effort. Total value is 30 points. All questions are equally weighted. Do any 5 of 7 questions. Do more than 5 for extra credit.

1. What are the fundamental differences between IP and ATM networks in terms of delay, buffering and survivability?
2. What are the fundamental limitations of an ATM network with respect to a DDoS (Distributed Denial of Service) attack?
3. Describe the relationship between traffic volume, delay and cell loss probability in an ATM network. How can this be used in a denial of service attack?
4. In the zero-knowledge proof security protocol, one party is either asked to demonstrate knowledge of the solution to an NP-complete problem, like the Hamiltonian cycle of a graph or is asked to demonstrate isomorphism between two different problems. Why is it necessary that they be prepared to perform *either* task? Why would not one *or* the other suffice?
5. What is the purpose of making the oblivious transfer *oblivious*?
6. A professor at a university has a large class to which a final exam must be administered to three sections on three separate days. The test is to be an open notes exam. For fairness and consistency in testing and grading, it is desired to give the same exam to all three sections, but there is the threat that students from the first section will copy the exam and give it to their friends taking the exam the second or third day to use as part of their notes. Of course, all students will be asked to return the test questions with their answers, but the students in the earlier sections might briefly leave the room to copy their exam questions for their friends. Describe a technique that might be used to detect exam copying that would be capable of identifying the cheaters.
7. Your organization is considering replacing an existing password-only user authentication scheme for both on-site and remote (off-site) network access. Candidates are a fingerprint-based biometric scheme or a security device that displays a user-specific time-varying authentication value (like a SecureID token). What are the advantages and disadvantages of each scheme?