

CS 574
Midterm Exam
October 12, 2001

Please note the following instructions. There will be a **ten point deduction** for failure to comply with them:

- This exam is open book and open notes. You may feel free to use whatever additional reference material you wish, but **no calculators** are allowed.
- start each problem on a new sheet of paper.
- write your social security number, but not your name, on each sheet of paper you turn in.
- be succinct. I will take points for facts that, while true, are not relevant to the question at hand.

You have until 10:30 to finish the exam. The questions are equally weighted.

1. In the Clouds paper, a comment is made to the effect that file abstractions such as those used by Unix and Plan 9 are “hardware-based.” Discuss whether or not this comment is accurate.
2. Both FFS and Reiserfs set a goal of better performance on small files. Which is more successful in achieving this goal? Why?
3. The DES standard makes the point that the algorithm is well-suited to a hardware implementation. What features of the algorithm make this true? Why is RSA less well-suited to a hardware implementation than DES?
4. Netscape supports the use of encryption for transmission of sensitive information (such as credit card numbers). At one time, the keys it used were based on requesting the operating system for the current time of day. Speculate on why this turned out to be a bad idea.