CSci 530 Midterm Examination (Fall 2003)

Instructions: Show all work. If a question asks for a numerical or algebraical result, indicate your answer clearly (for example, by drawing a box around it). No computers are allowed; handheld calculaters are permitted. This exam is open book, open notes. You have 90 minutes to complete the exam. If you need more space to answer any of the questions, attach a separate sheet of paper; if you do so, please use a di erent sheet of paper for each question. There are 100 points in all.

1. (24 points) In this problem, you will carry out a simple RSA key generation and encryption. For all parts, let p = 11; q = 29; e = 3.

   (a) (5 points) Find d.
   (b) (3 points) What is the largest number that can be encrypted using this key pair?
   (c) (8 points) What ciphertext c do you get when you encrypt the plaintext m = 23?
   (d) (8 points) What plaintext m encrypts to the ciphertext c = 23? (Reminder: Show all work!)

2. (21 points, 7 points each) Answer each question in one paragraph or so.

   (a) Why is AES (Rijndael) more efficient to implement in software than DES?
   (b) Clyde wants to add preauthentication to his own key distribution system, based on symmetric (conventional) cryptography. He decides to have the client (the user program) send the user's ID, encrypted using the user's long-term key, as the payload of the preauthentication. What do you think of his idea?
   (c) What are the weaknesses of pure transposition encryption when the block size is small? What are the weaknesses when the block size is large?

   Answer the following two questions in essay form. Be thorough, but not redundant.

3. (25 points) In class, we discussed how DES, with its 56-bit key, uses only a tiny fraction of the number of permutations between 64-bit plaintext blocks and 64-bit ciphertext blocks. Specifically, there are 2^56 ~= 7 x 10^16 different keys, but there are (2^64)! ~= 2^(2^70) ~= 10^(10^21) different permutations.
   To be able to specify all of those permutations would therefore require a key that is about 2^70 bits long. That's far above and beyond today's storage devices (a terabyte is 10^12 bytes, or 8 x 10^12 bits), but suppose that storing such a key became feasible. What other difficulties would there be in defining and using a cryptosystem with a key of that size? What attacks that work on DES would this new system be resistant to? What attacks, if any, would still work on it?

4. (30 points) You have been hired to advise the California Secretary of State on the next generation of electronic voting equipment. One system under consideration is manufactured by VoterID, Inc, and is marketed as providing absolute voter authentication over the Internet based on one of several forms of biometrics, so that voters may cast ballots using their own computer in the comfort and privacy of their own home. Describe the concerns you might have about such a system. How useful are the biometrics likely to be, balanced against the cost of deploying such a system? Discuss the relationship between the requirements for authentication, accountability of the votes cast (that is, can the voter be assured that his votes were tallied properly?), and the requirement for secrecy of individual votes cast (that is, can the voter be assured that no one else can determine how he voted?).