ACCESS 2001

Final project - Week 1

Due Friday, June 22

Many interesting questions in mathematics have to do primarily with the set of Natural Numbers {1, 2, 3, . . . }, and their properties. Number Theory, the area of mathematics devoted to these questions, may seem very abstract with little connection to the real world. Yet the concepts studied often have surprisingly useful applications to very practical problems.

You may recall that a prime number is a natural number other than 1 that has as factors only 1 and the prime itself. So for example, 2, 3, 5, 7, are prime, but 4, 6, 8, 9 are not prime and are called composite numbers. The number 1 is special and is called a unit. Prime numbers play a special role in Number Theory. In fact today large prime numbers of 200 digits or more are used in the encryption scheme known as the RSA public key method, a way to send information you want to keep secret, such as credit card numbers, over the internet. Do some research into prime numbers reporting both what is known and what are open conjectures about prime numbers, the largest known prime today and the number of digits it contains. You will find the internet very useful for this research. This part of the project should be 1-2 pages in length.

Now set up an RSA public-key cryptography system. Include the secure signatures feature which we discussed in the Alice-Bob-Eve picture. Choose primes with twelve digits (unlike the seven we used in class), so that each packet of information can safely contain up to 20 digits (10 letters) of information. Use the chart on page 9 of Davis' notes for conversion. Send an email to the ACCESS list with your public keys. Send an encoded message to each group using that group's public key. Then using your private key decode the messages you received. (Please send the same message to each group.)

In your project, describe the process you went through to set up your system and to find the keys. Also list the keys, both public and private, that you are using. Show the details of the process you went through to encode one of the messages you sent, and list the coded messages that you sent to each group. Also explain in detail how you decoded one of the messages you received and list the codes and deciphered messages you received. (When I finish reading the papers, I should know both the private and public keys, and the messages you received in both coded and deciphered form.)

Although different subjects and Professors may have different standards for how papers should be formatted, there are certain common elements. Reports should begin with a cover page or title area, containing the title, the authors, and the date. This should be followed with an introduction which summarizes the report's contents. The body of the project report may be split into sections, and a conclusion section may be appropriate. Include references, URL's, and footnotes if you have them. The RSA paper by Rivest-Shamir-Adelman is an excellent example of how to write a paper.

Please submit your paper to me by including it as an attachment in an email. Your document should either be a Microsoft Word or Word Perfect document. (My preference is MS Word.) This project is due by Friday June 22, at 5 p.m.

Enjoy!