ACCESS 2002

Final project - Week 1

Due Friday, June 28

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. 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. Choose two primes greater than 10^50, so that their product has more than 100 digits, and so that each packet of information can safely contain up to 50 symbols of information. Send an email to the ACCESS list with your public keys.

Send an encoded message to each group using that group's public enryption key. Please use the same original message and signature for each group. Use the chart on page 9 of Davis' notes for conversion. Include the secure signatures feature which we discussed in the Alice-Bob-Evil picture. Let us agree that no message (including jumbled signature) shall be longer than three packets, If you have a wonderful longer message, send most of it in plain text and just encrypt the best part. Let us agree that each message will end with the numbers corresponding to a period and a space, followed by the jumbled signature numbers. You will discover that you need a few digits more than a packet's worth of space for your jumbled signature, since even it it started out short it got big when you decoded it. Use your private key to decode the messages you receive from each group, and then use that group's encryption key to read their signature.

In your project, describe the process you went through to set up your system and to find the keys. Write down your own group's pubic key, as well as its decryption power. List each group's message and signature which you have successfully deciphered. For (only) the group with number one less than yours (mod 7), show the encrypted message you sent them, and explain how these numbers were arrived at. For (only) the group with number one greater than yours (mod 7) show the encrypted message you received, the decrypted numbers and both forms of the signature.

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 (Nick) 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 28, at 5 p.m. Help each other, and take advantage of the fact that Emina and I love to explain math.