ACCESS 2003

Final project - Week 1 - Due Friday, June 27

Part of your project this week is to set up an RSA public-key cryptography system for the 7 ACCESS groups. Each team should choose two primes between 10^50 and 10^51, so that the modulus formed by their product is greater than 10^100 - and thus will have at least 101 digits. This means that people sending you messages can use up to 100 digits in each packet , **before** encoding. (After they encode a packet it will quite likely have 101 or 102 digits, but it will still be smaller than your modulus because of how encoding works.) After picking your primes find a suitable encryption power e. Make sure you have done everything correctly and then send a plain text email to the ACCESS list and to "us" (korevaar@math.utah.edu, putnam@math.utah.edu, mbell@math.utah.edu, sundell@math.utah.edu, Erika.Roner@m.cc.utah.edu), with your public key information. Make sure to mention which group number you are, and which email address(es) you would like messages sent to.

Create a cool secret message and signature. You will be encrypting and sending this message to two groups: the groups with residue numbers one less than yours and one greater than yours, mod 7. For example, group 7 is congruent to group 0, and sends a message to group 6 and to group 1.) Please use the same plain text message and signature for both groups. Use the chart on page 9 of Davis' notes for conversion. Include the secure signature feature which we discussed in the Alice-Bob-Evil picture. Let us agree that each plain text message will end with the numbers corresponding to a sentence ender (period, exclamation mark or question mark) 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 almost as long as your modulus when you decrypted it. Let us agree that no message (including jumbled signature) shall be longer than three packets. The consequence of these agreements is that your original plain text message better not be more than 97 characters long. If you have a wonderful longer message, send most of it in plain text and just encrypt the best part.

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.

The first section of your project report should be a 2-4 page discussion of the general ideas behind public key cryptography. Explain why its advent was such a revolutionary development. Explain the RSA algorithm as best you can. We have given you plenty of source material for this part of your report, but feel free to do more research if you wish. Make sure to cite all references.

In the second section of your report describe the process you went through to set up the ACCESS RSA system. Exhibit your public and private keys, your original plain text message and signature, and the various transformations of your message and signature as you prepared them for transmission to your two target groups. Exhibit the encoded messages you received, explain how you decoded them, and exhibit the final results.

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 in mathematics.

Please submit your paper to Nick, Emily and Maria by including it as an attachment in an email. Your document should either be a Microsoft Word or Word Perfect document. This project is due by Friday June 27, at 5 p.m. Help each other, and take advantage of the fact that your teachers love to explain math.