CMPSCI 120 / 145
Encryption
Professor William T. Verts

This assignment is to simulate the process that goes on between your browser and a remote secure Web site for exchanging public encryption keys. Once the key exchange has been made, information can be securely transmitted between the two participants. With the email exchange, you will be simulating the browser and I will be simulating the secure server. This is not a difficult assignment, but it does take some time because there are several required email exchanges with me.

Go to the class site, and click on the link to "ENCRYPTION (WEB BASED)". That link will take you to a page containing a key-generator and two separate places to encrypt a message.

1. Click the Generate New RSA Keys button a few times, until you get a key set you like.

WRITE DOWN AND DO NOT LOSE THESE NUMBERS

2. Email your PUBLIC key pair to me personally (**verts@cs.umass.edu**), with the Subject line of your message set to CMPSCI PUBLIC KEY. Make sure your name is part of the body of the message. DO NOT email me your private key pair, but keep that pair handy for the later parts of the assignment.

   When I get your email, I will (eventually) send you a personalized secret (numeric) message, first signed with my private key and then encrypted with your public key. The result I send you will appear as a long, multi-digit number.

3. Plug that number into the first Numeric Message to Encrypt edit boxes.

4. Put your own PRIVATE key into the first Encryption Key edit box (as two numbers separated by a comma) and click the Encrypt the Message button.

5. Copy the result into the second Numeric Message to Encrypt edit box.

6. Put my PUBLIC key (5, 37380929) into the second Encryption Key box and click the second Encrypt the Message button. The plain-text message will appear in the final Encrypted Message box. It should be a four-digit number. I have just successfully sent you a secret (numeric) message!

7. Send me a personal email telling me the four-digit number. Make sure that your name is part of the body of the message. If the number is correct, you will get full credit on the assignment.

It is possible that the key pair that you send me won't work. If this happens, I'll ask you to generate and send several more sets of key pairs, and I'll respond with the one that works.