CMPSCI 145
Encryption & Steganography
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. That information is the key needed to decode a special message steganographically hidden inside a publicly viewable **`.GIF`** file. With the three programs (all for Windows) and the email exchange, you will be simulating the browser and I will be simulating the secure server.

STAGE #1

1. Download from the class web site the three following files into a single folder on your computer:

   ```
   Steganography_Distribution_V1_0.zip
   RSA_Key_Generator_Distribution_V1_0.zip
   RSA_Encrypt_Decrypt_Distribution_V1_0.zip
   ```

   Unpack the contents into that same folder. You will have three **`.EXE`** files, totaling about 1.6 megabytes in size.

2. Run the Key Generator program. Press the Generate Keys button a few times, until you get a key set you like.

   WRITE DOWN AND DO NOT LOSE THESE NUMBERS

3. Email your PUBLIC key pair to me personally (**`verts@cs.umass.edu`**), with the Subject line of your message set to CMPSCI 145 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 next stage of the assignment.

STAGE #2

When I get your email from stage #1, I will send you a personalized reply message, which will be a long, multidigit number encrypted with your public key and signed with my private key.

1. Run the Encrypt/Decrypt program and plug that number into the first edit box.

2. Put your own PRIVATE key into the first Enter Key Pair edit box (as two numbers separated by comma) and click the Encode/Decode button.

3. Put my PUBLIC key (5, 754157461) into the second Enter Key Pair box and click the second Encode/Decode button. The plain-text message will appear in the final box. It should be a four-digit number. Write down the four-digit number for the next stage.

STAGE #3

1. Run the Steganography program, and load in the image called **`Carrier.gif`** from the class Web site. You can do this in a couple of ways.

   One method is to right-click the image in a Web browser, select Save Image As from the popup, save the image into the folder with the other programs from this assignment, and then click File-Open in the Steganography program to load it in.

   An alternate method is to select File-Open From Web in the Steganography program and type in the following Web address (the file will be stored automatically in the **`\DATA\WEB`** folder of your hard disk):

   `http://www.cs.umass.edu/~verts/cmpsci145/Steganography_and_Encryption/Carrier.gif`

2. Click on Steganography-Decode. In the Enter Password box enter the four-digit number you obtained in stage 2. If the password number is not correct you will see an error message. When the password number is correct, the dialog will tell you that the payload file will be stored in the **`\DATA\DECODE`** folder on your disk.

3. Open up the **`\DATA\DECODE`** folder and examine the text file stored there, decoded from the image. Read the contents of that text file, and follow its instructions. When you have performed the step(s) listed therein, you will be done with the assignment.

NOTE: It is possible that the key pair that you select in stage #1 won't work. This may be due to a bug on my part, or an incomplete understanding of the math involved, but I haven't yet found out how to solve the problem. If this happens, I'll email you asking you to generate and send to me several more sets of key pairs, and I'll send you back the one that works.