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 and 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.

STAGE #1

Go to the class site, and click on the link to "Dr. Bill's Lazarus Software". That link will take you to a DropBox repository with two folders, one for Mac and one for Windows. Click on whichever one corresponds to the type of computer you own.

1. **Windows:** Select either the 64-bit folder or the 32-bit folder (most people will select the 64-bit folder, but the applications exist for 32-bit machines as needed). Download the three following files into a single folder on your computer:

   SteganographyProject.exe
   RSA_Key_Generator_Project.exe
   RSA_Encrypt_Decrypt_Project.exe

   There is no installation process.

   Mac: Download the three following files into a single folder on your computer:

   Steganography.zip
   RSA Key Generator.zip
   RSA Encrypt Decrypt.zip

   Double-click each file when the download is complete. Each `.ZIP` archive will automatically unpack to a folder containing two files as part of the download process. One of those files (the larger) is the actual executable, but the other (the smaller) which may have a file extension of **.app** is the file that you double-click to launch the program. The first time you run any of these programs right-click (two-finger click) the **.app** file, and select Open from the pop-up. You'll get a dialog asking if you sure you want to run the program; click Open. The program will run, but from now on you need only double-click the .app file to run the program. (These programs should run on any Mac; if you cannot get them to work, there may be an issue with the security settings on your computer.)

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, 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.

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. Find the image called **Carrier.gif** on the class Web site. 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.

2. Run the Steganography program. Click the Open button in the Steganography program to load in the image file.

3. Click on the Decode button. In the Enter Password box enter the four-digit number you obtained in stage 2. In the Pick A Folder dialog, select where you will want any decoded file to appear (I recommend your desktop). You will get a response dialog. If the password number is not correct you will see an error message. When the password number is correct the dialog will show a lot of information, including the name of the contained file, how big it is, and where it will be stored. The payload file should appear inside the selected folder.

4. Find and open the target folder, as necessary, and examine the file stored there, decoded from the image. Read the contents of that 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.