In this lab you will exchange encoded messages with other groups, using the RSA cryptosystem to encode and decode messages.

1. **Before lab on Thursday**, as a group, choose two large primes (each should have at least 35 digits) for your code, and create the "public key" (the m and k in Shahriari's description of the RSA cryptosystem), and enter this information into the spreadsheet in the Collaborative folder on the M-drive. (3.5.8)

2. **In lab on Thursday**, compose a secret message for the group that is listed after your group on the spreadsheet. Encode the message using their public key, and give it to them, keeping the original message secret. Use 10-digit blocks for the encoding. (3.5.9)

3. When you receive an encoded message from the group listed before your group on the spreadsheet, decode the message, using the procedure you discovered in last week's lab. Keep the decoded message secret. The encoded message, however, is *public* information. If another group wants to look at it, you must let them. (3.5.9)

4. **Challenge**: Look at the (public) encoded message that was sent to another group. Using that group's public key, try to break the code. (3.5.10)

There is no formal lab report associated with this lab activity. You will be evaluated based on your participation. Have fun!