RSA Project

Math 242

due Friday, March 23

The purpose of this assignment is to implement RSA encryption/decryption and use it to send secure messages via a public forum.

Implement all of the steps in the RSA Project notebook. After you have chosen primes p and q (of at least 30 digits), compute your encryption key (e, n) and publish this in the RSA Forum on Moodle. Then implement the functions necessary to encrypt and decrypt text string. Test that your functions work using your own public and private keys.

Then use the RSA Forum to do the following:

- Send at least one encrypted message to another student.
- Reply to at least one encrypted message from another student.
- Send at least one encrypted message to the professor.
- Reply to at least one encrypted message from the professor.

In your Mathematica notebook, include your messages in both encrypted and plaintext form.

As usual, submit code that runs and explain what your code does; make it clear that you know how your implementation works. Your goal should be to communicate your work to another person (e.g., another student at your level who is not in this course).

Your notebook will be graded on a scale of 0 to 4, according to the following rubric.

4. Problems and goals are clearly stated, including relevant definitions or parameters. Computations are complete; code runs and is clearly explained. RSA encryption has been used to communicate securely with at least one other student and with the professor. Limitations of the methodology, extensions for future work, and/or conjectures are discussed. Notebook is well-formatted and easy to read.

3. Problems and goals are stated well, though relevant definitions or parameters may be missing. Secure communication with at least one other student and with the professor is not demonstrated. Conclusions are unclear or not well justified. Insufficient discussion of limitations, extensions, and/or conjectures.

2. Statement of problem or goal is unclear. Computations are incomplete; explanation is ambiguous. Code may produce errors when run. Secure communication with at least one other student and with the professor is not demonstrated. Little or no discussion of limitations, extensions, and/or conjectures. Notebook is difficult to read.

1. Serious misunderstanding of the problem or goal. Computation is inadequate for the task at hand. Work is not clearly explained. No discussion of limitations, extensions, and/or conjectures. Notebook is difficult to read.

0. Notebook is not turned in.