RSA Project

Math 242
due Friday, March 22

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 functions necessary for RSA encryption, as discussed in class. Copy all of these functions into a single Mathematica notebook. This includes everything from `modPow2` to the functions that convert text to numbers and back.

Choose your own secret primes p and q (of at least 30 digits), compute your encryption key (e, n) and publish this in the RSA Forum on Moodle. Test that your encryption and decryption 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 two other people.
- Reply to at least one encrypted message from two other people.

In your Mathematica notebook, demonstrate that your communication worked by including two 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 16 points. The following rubric gives characteristics of notebooks that will merit sample point totals. (Interpolate the following for point totals that are not divisible by 4.)

16 points. Problems and goals are clearly stated, including relevant definitions or parameters. Computations are complete; code runs and is clearly explained. Conclusions are clearly stated and backed up by sufficient computational evidence. Limitations of the methodology, extensions for future work, and conjectures are discussed. Notebook is well-formatted and easy to read.

12 points. Problems and goals are stated well, though relevant definitions or parameters may be missing. Computations are mostly complete; code runs, but explanation is weak. Conclusions are unclear or not well justified. Insufficient discussion of limitations, extensions, and conjectures.

8 points. Statement of problem or goal is unclear. Computations are incomplete; explanation is ambiguous. Code may produce errors when run. Conclusions are possibly correct, but not justified. Little or no discussion of limitations, extensions, or conjectures. Notebook is difficult to read.

4 points. 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, or conjectures. Notebook is difficult to read.

0 points. Notebook is not turned in.