RSA Project

Math 242

due Friday, March 20

The purpose of this project is to implement RSA encryption/decryption and use it to send secure messages via a public forum. This project requires you to have a working implementation and understanding of RSA encrpytion, but it isn't *experimental* like most other projects in this course.

Finish implementing 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 30 digits), compute your encryption key (e, n), and publish your encryption key 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 an encrypted messages to two other people.
- Reply to encrypted messages from two other people.

In your Mathematica notebook, demonstrate that your communication worked by including two messages in both encrypted and plaintext form.

Aditionally, answer the following questions in your Mathematica notebook:

1. If a message is encrypted using your public key and posted online, why can no one else decrypt the message?
2. Why can you quickly decrypt messages that have been encrypted using your public key?
3. How might quantum computers break RSA encryption?

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. Goals of the project are clearly stated, including relevant definitions or parameters. Computations are complete; code runs and is well documented. Notebook demonstrates that you understand what you are doing and contains thorough answers to the questions above. Limitations of the methodology and possible extensions for future work are discussed. Notebook is well-formatted and easy to read.

12 points. Goals of the project are stated well, though relevant definitions or parameters may be missing. Computations are mostly complete; code runs, with some documentation. The notebook might not make it clear that you understand what you are doing, or answers to the questions above are not thorough. Insufficient discussion of limitations and possible extensions.

8 points. Statement of goals is unclear. Computations are incomplete, documentation is lacking, and code may produce errors when run. Notebook contains little evidence that you understand what you are doing or minimal answers to the questions above. Little or no discussion of limitations or extensions. Notebook is difficult to read.

4 points. Serious misunderstanding of the goals of this project. Computation is inadequate for the task at hand. Work is not clearly explained. Notebook does not contain answers to the questions above. No discussion of limitations or extensions. Notebook is difficult to read.

0 points. Notebook is not turned in.