Math 316, RQ 7.2B The RSA Cipher

Name: _____

Finish reading and taking notes on Section 7.2 The RSA Cipher (starting with the subsection "Elementary aspects of security of RSA"). If you are using the first edition of the textbook, please see Blackboard for an updated version.

Reading Questions

1. Explain why the difficulty of factorization makes RSA secure.

2. Why is it important that exponentiation be 'easy' relative to factorization?

3. Why is it important that primality testing is 'easy' relative to factorization?

4. Suppose that I wanted to set up a secure communication network in our class, using one common modulus n (keeping p and q secret) and giving each student different encryption/decryption exponents. (So, for Mitch to send a message to Liam, he would use Liam's public key (n, e_L), and Liam would decrypt the message using his own decryption key (n, d_L). And for Liam to send a message to Mitch, he would use Mitch's public key (n, e_M), and Mitch would decrypt it using his own decryption key (n, d_M).) Why is this a bad set-up?

5. Pick one other attack on the RSA cipher and describe how it can be thwarted.

6. What struck you in this reading? What is still unclear? What remaining questions do you have?