CS 173, Spring 2016
Honors Homework 2

This homework is due Friday, April 15th.

Honors homework must be formatted using the LaTeX document formatting package. (Not just the equation mode found in Piazza and Moodle.) See the CS 173 honors web page for help getting started with LaTeX. Exception: you do not need to format supporting materials such as program source code, screenshots, and figures.

Your homework should be submitted as hardcopy in the CS 173 honors dropbox in the basement of Siebel. Please submit a hardcopy of your LaTeX document **both source code and formatted output** and hardcopies of any supporting materials.

The dropboxes are located just east of the lounge area with the big windows. If you get to the candy/soda machines, you've gone too far east.

To do this homework, you'll need to read our handout on RSA and pp. 131-134 from Liebeck, *A Concise Introduction to Pure Mathematics*, 2nd edition, Chapman and Hall, 2006. These are posted on moodle: look for the honors section at the bottom after the last week of classes.

When you convert strings of characters into strings of digits, you'll need to use Liebeck's 2-digit encoding of each character. That is, A=01, B=02, etc. The digits 0-9 will be encoded using their ASCII codes, i.e. 0 encodes as 48, 1 encodes as 49, etc. Also notice (e.g. see p. 132 of Liebeck) that when you divide your numberical string into blocks of digits for encoding, each block should have one fewer digits than N has. For example, if N has 6 digits, then each block (except perhaps the last one) should have 5 digits.

Problem 1

Suppose you know that $pq = 35209$ and $(p-1)(q-1) = 34816$.. Find the primes p and q using the method at the bottom of p. 134 of Liebeck. Show your work.

Problem 2

Use your favorite programming language to write a short program to compute $x^n \pmod{k}$ by repeated squaring. We need to be able to understand how your code works and to verify that it does use the repeated squaring method. So keep your code simple and comment it well.

You should submit source code for your program and also a sample run of your program showing it computing values for the following inputs:

$$5^2 \pmod 7$$
$$234^{1029} \pmod{121}$$
$$377^{901} \pmod{57}$$

Test your code against the example numbers at the top of Liebeck p. 134. Identify which of Liebeck's calculations contains a typo.

Problem 3

For this problem, show the main steps in your work, including the details of using the Euclidean algorithm to find d.

(a) Encode your netID using the public key $(N, e) = (851, 251)$

(b) Figure out what d must be and decipher the following message. What character code is used for a blank space in this message?

$$167, 178, 631, 381, 126, 35, 35, 819, 35, 381, 432, 819, 35, 126, 381, 657, 178, 279, 192, 126, 657$$

Problem 4

A Canadian friend has asked James Bond to play bagpipes at his wedding. The friend emailed him the name of one special piece, so he could practice ahead during his current mission in Zimbabwe. So that his cover would not be broken if anyone were to hear him playing the piece, it was encoded as:

$$5180, 146, 4227, 1533, 2361, 1759, 4097, 4026$$

Moneypenny supposedly sent the decoding key via diplomatic pouch: $(N, d) = (5293, 233)$. However, she had recently been hit in the head by an experimental device of Q's and what she sent was actually the encoding key.

Figure out the decoding key and decrypt the message: