CS 173, Spring 2014
Honors Homework 1

This homework is due at Friday, March 14th at 5pm.

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. This will be posted on moodle: look for the honors section 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 $pq = 33233$ and $(p-1)(q-1) = 32868$. 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 $(N, e) = (697, 63)$.

(b) Figure out what d must be, showing key steps in your work. Then decipher the following message to find the person who invented a very important piece of electrical equipment. What character code did the author of this message use for a blank space?

$$465, 389, 1, 256, 486, 330, 111, 284, 64, 1, 486, 546, 155, 330, 486$$

Problem 4

Since James Bond travels first class and doesn't like regular airplane food, so he pre-orders a special dish. Moneypenny has a standing arrangement with British Airways that they can decode these orders using the decoding key $(N, d) = (3431, 203)$. She was on vacation for his latest mission and delegated the job to Q, who confused the decoding and encoding keys. In other words, 203 was really e rather than d.

Figure out the true decoding key d and decrypt the message.

$$3192, 65, 1652, 1196, 2609, 2400$$