CS 173, Spring 2013
Honors Homework 1

This homework is due at Monday, March 5th at 5pm.

Honors homework must be formatted using LaTex. See the CS 173 web page for help getting started with LaTex. Exception: you should not try to format supporting materials such as program source code, screenshots, and figures.

Please turn in your a hardcopy of your LaTex output (not the input) in the CS 173 honors dropbox in the basement of Siebel. 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.

Notice that you'll need to use the same character encoding as in Liebeck (A=01, B=02, 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.

Problem 1

Suppose you know that $pq = 39917$ and $(p-1)(q-1) = 39516$. 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 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 examples numbers at the top of Liebeck p. 134. Identify which of Liebeck's calculations is wrong.

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 the message CORNFIELDS using the public key $(N, e) = (493, 143)$.

(b) Figure out what d must be and decipher the following message. What character code did the author of this message use for a blank space?

$$1, 452, 415, 107, 1, 453, 64, 415, 409, 369, 64, 387, 225, 1, 247$$

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 $(N, d) = (9523, 137)$. She was on vacation for his latest mission and delegated the job to Q, who confused the decoding and encoding keys. In other words, 137 was really e.

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

$$3099, 9271, 4393, 8201, 5919, 7656, 2950, 5704$$