CS 173, Spring 2016
Honors Homework 3

This homework is due Wednesday, December 7th.

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

When you convert strings of characters into strings of digits, you should normalize all letters to their uppercase versions, then use Liebeck's 2-digit code for each alphabetic character. That is, A=01, B=02, etc. The digits 0-9 should be converted to their ASCII codes, i.e. 0 encodes as 48, 1 encodes as 49, etc. Characters other than letters and digits should be coded as 27.

- A file containing all your functions. Include enough comments that I can easily understand what you did.
- A file showing sample inputs and outputs for your functions, as well as answers to the encoding/decoding questions. Find inputs and outputs that clearly illustrate that the code is working right.

Problem 1

Write a function that converts an input string to a list of digits, using the encoding described above. It may help to look back at homework 2.

Write the inverse function, which converts a list of digits to a string. Or, not exactly the inverse, because it can't undo the fact that all letters have become uppercase and all miscellaneous characters have been converted to space.

Problem 2

Write an equation expressing b^{2n} in terms of b^n. Write a similar equation expressing b^{2n+1} in terms of b^n.

Using those equations, write a simple recursive function that takes three inputs (b, n, k) and computes $b^n \pmod{k}$. You'll want to have separate cases, depending on whether n is odd or even. To keep intermediate values small, reduce the output mod k at each main step (e.g. each recursive class).

Hint: look at the racket cheat sheet under "arithmetic" for functions like (integer) quotient).

Problem 3

For this problem and the next, you'll probably want to do some steps by hand and some steps using the Racket functions you built above.

(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.

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

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.

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

Notice the discussion midway through p. 132 of Liebeck about dividing up blocks of digits. (This is the part that seemed too painful to implement in Racket right now.)