Due: January 26, beginning of tutorial.

This assignment is worth 10% of final grade

1. Recall (or recompute) your 7 or 8 digit ID from assignment 1. Now consider the BBS (Blum Blum Shub) pseudo random generator:
   $x_{i+1} = x_i^2 \ mod \ M$ where $M = p * q$ with p and q primes.
   (There are other technical conditions for p and q that can be found in the Wikipedia entry for the BBS generator.) Set $p = 7$ and $q = 11$ and $x_0 = ID \ mod \ 77$. Let $b_i =$ parity of 1's in the binary representation of x_i. Generate the sequences $x_0, x_1, x_2, \ldots$ and $b_0, b_1, b_2, \ldots$. For what index m does you sequence repeat itself? That is, what is the smallest m such that $x_m = x_i$ for some $i < m$? For this m, consider the binary sequence $b_0, b_1, \ldots, b_m$. Describe how hard it is for you to memorize this binary sequence so that you can repeat it without notes (after not seeing it for one hour).

2. This question relates to the RSA public key system.

   - Explain informally (without using the fact that $\phi(x \cdot y) = \phi(x) \cdot \phi(y)$) why $\phi(p \cdot q) = (p-1)(q-1)$ when p and q are primes. Here $\phi(x)$ is the Euler function discussed in class.
   - Use the Euclidean algorithm to compute $gcd(49, 60)$.
   - Using $n = 77 = 7 \cdot 11$, send me (by email) an RSA "digital signature" of your $ID \ mod \ 77$. You should send me public instructions on how to read you signature.