MA/CSSE 473   Day 10 Announcements and Summary

Announcements:

1. HW 5 due Monday night. HW6 Thursday
2. Exam dates: Tuesday Sept 30, Tuesday November 4.   In-class. Still not in the schedule page (soon!).
   - If you are allowed extra time for the exam and plan to use that time, please talk with me soon about timing.
3. In my office hours 6, 7, 9, and probably the last half of 8 today. (meeting prospective student; don't know how long it will take)
4. Monday we will discuss the Donald Knuth interview mentioned in the Day 3
5. Grading of yesterday's Primality testing checkup.:
   - 9 – essentially all of the ingredients
   - 6 – most of the ingredients
   - 3 – At least one of the ingredients, and with some clarity.
   - 0 – Vague stuff about clarity, but no mention of Fermat's theorem by name or by formula.

Main ideas from today:

1. **Cryptography intro.** We focus on how to encode a single integer message m with $0 \leq m < N$.
   e is the encoding key, and d is the decoding key.

2. In *public-key* cryptography, I give you (e, N) so you can send me a message, but I keep d private.

3. **RSA:** Choose two large primes p and q, and let N = pq.

4. Choose any number e that is relatively prime to N' = (p-1)(q-1). Then
   a. the mapping $x \to x^e \bmod N$ is a bijection on $\{0, 1, \ldots, N-1\}$, and
   b. If d is the inverse of e mod N', then for all x in $\{0, 1, \ldots, N-1\}$, $(x^e)^d \equiv x \pmod N$.

5. Example: p=63, q=53 (so N=3233):

6. **Property that is the basis of RSA:** If N=pq for 2 primes p and q, and if e is any number that is relatively prime to N' = (p-1)(q-1), then
   a. the mapping x→xe mod N is a bijection on
      {0, 1, …, N-1}
   b. If d is the inverse of e mod (p-1)(q-1), then for all x in {0, 1, …, N-1}, (xe)d ≡ x (mod N)