T-79.159 Cryptography and Data Security
2005 / Homework 4
Tue 12.4 and Fri 15.4

1. Use the Extended Euclidean Algorithm to compute the multiplicative inverse $357^{-1} \bmod 1234$.

2. Determine the following: $\phi(41)$, $\phi(27)$, and $\phi(231)$.

3. (a) For what type of number n is $\phi(n)$ largest (relative to n)?

   (b) For what type of number n is $\phi(n)$ largest (relative to n)?

   (c) Is it possible for $\phi(n)$ to be bigger than n?

4. The example used by Sun-Tse to illustrate the Chinese Remainder Theorem was

$$x \equiv 2 \,(\mathrm{mod}\,3)$$
$$x \equiv 3 \,(\mathrm{mod}\,5)$$
$$x \equiv 2 \,(\mathrm{mod}\,7)$$

Solve for x.

5. Perform encryption and decryption using the RSA algorithm for the following:

   (a) $p = 3$, $q = 11$, $e = 7$, for $M = 5$;

   (b) $p = 17$, $q = 13$, $e = 7$, for $M = 2$.

6. In RSA,

   (a) is it possible for more than one d to work with a given e, p, and q?

   (b) given that the primes p and q are approximately the same size, approximately how big is $\phi(n)$ compared to n?

7. Using the prime number theorem estimate how many 512-bit primes exist.