T-79.4501 Cryptography and Data Security
2006 / Homework 4
Mon 13.2 and Wed 15.2

1. Assume that an HMAC are using SHA-1 as the underlying hash function. Given a fixed key, what kind of message independent pre-computations can be performed to speed up the computations?

2. Compute 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 $\phi(n)$ smallest (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

$$\begin{aligned} x &\equiv 2\,(\mathrm{mod}3) \\ x &\equiv 3\,(\mathrm{mod}5) \\ x &\equiv 2\,(\mathrm{mod}7) \end{aligned}$$

   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 prime p is about twice as large as q, approximately how large $\phi(n)$ is compared to n?