ASSIGNMENT 7 ECE 103 (Spring 2009)

Due in tutorial on Monday, July 6.

1. Let $p = 223$, $q = 281$, and $e = 73$. Find the associated RSA public and private keys.
2. Consider the RSA cryptosystem with public key $(e, n) = (25, 16837)$ and private key $(d, n) = (15913, 16837)$. Using the square and multiply algorithm, encrypt the message "HI," represented by the integer $M = 0809$, with the appropriate key.
3. Consider the RSA cryptosystem with public key $(e, n) = (121, 17653)$ and private key $(d, n) = (5317, 17653)$. Note that $p = 139$ is a prime factor of n. Using the Chinese Remainder Theorem, decrypt the ciphertext $C = 10214$ with the appropriate key.
4. What is the private key associated with the RSA public key $(e, n) = (107, 221)$? (In this problem you are *breaking* RSA, which is feasible because n is not too large.)