NUMBER THEORY: CLASS 25

1. Exercise

1) Given $N = 26, \quad k = 4, \quad l = 5$ with the public key $(n, e) = (8902171, 574373)$ and the deciphering key $(n, d) = (8902171, 4424621)$. Pair up with your friend in the class to practice sending and receiving message using RSA Cryptosystem.

Download program to help convert letter to numbers and vice versa from my web site.

2) Let n be the product to distinct primes.
Let d and e be positive integers such that $de \equiv 1 \bmod \phi(n)$.

Show that $a^{de} \equiv a \bmod n$ for *any* integer a.

Date: Friday, November 21, 2008.