1. Use the square and multiply algorithm to compute the following by hand:

$$(a)\ 5^9 \mod 9 \qquad (b)\ 3^{30} \mod 25$$

2. Let $n = 3953$
   (a) Verify that $n = 59 \cdot 67$. Notice that both 59 and 67 are prime
   (b) Use the Euclidean algorithm to show that $\gcd(17, \phi(n)) = 1$
   (c) Apply the Extended Euclidean algorithm to write $u \cdot 17 + v \cdot \phi(n) = 1$
   (d) Conclude that $2477 \equiv 17^{-1} \mod \phi(n)$
   (e) If Bob were to use $n = 3953$ for RSA, what are some values they could choose for $k_{pub} = (n, e)$ and $k_{pr} = d$?