Homework 6, Introduction to Number Theory, Due Monday, May 11th

1. Suppose that the public encryption key for the RSA algorithm $n = 2537$ and $e = 13$. ($n$ is the modulus and $e$ is the exponent.) Convert your initials to a 4 digit (or 3 digit) number $P$, and find the encryption cipher $C$ of $P$ using the RSA algorithm.

2. Find the decryption key $d$ if $n = 2537$ and $e = 13$.

3. Use the decryption key you found in problem 2 to decrypt the cipher $C$ you made in 1 and verify that you get back your initials.

4. Let $p$ and $q$ be odd primes and $n = pq$. Suppose $p$ and $q$ have been lost, but you know $n$ and $k = \phi(n)$. Show how to recover $p$ and $q$ from $n$ and $k$ by deriving a formula to express $p$ and $q$ explicitly in terms of $n$ and $k$.

5. Prove that if $n$ is a positive composite number then $\phi(n) < n - 1$.

6. Use the result of the previous exercise to help prove the following:

   - Suppose $n > 1$. The number $n$ is prime if and only if there exists a number $b$ such that $(b, n) = 1$ and $b^{n-1} \equiv 1 \pmod{n}$ and $b^{(n-1)/d} \not\equiv 1 \pmod{n}$ for all positive divisors $d$ of $n - 1$ with $d > 1$.

   Hint: Use $h = \exp_n(b)$ in your proof.

7. Extend the result in the previous exercise to prove the following:

   - Suppose $n > 2$. The number $n$ is prime if and only if there exists a number $b$ so that $(b, n) = 1$ and $b^{(n-1)/2} \equiv -1 \pmod{n}$ and $b^{(n-1)/q} \not\equiv 1 \pmod{n}$ for all odd prime divisors $q$ of $n - 1$.

   This is potentially useful for certifying primality of a given number in situations where the prime factors of $n - 1$ are known.