Math 4440 Michael Soltys Test 3 Spring 2008

Name ______________________ Student No. ______________________

No aids allowed. Answer all questions on test paper. Use backs of sheets for scratch work.
Show all your work; there will be no credit for answers without a justification.

Total Marks 100: four questions, each worth 25.

1. Present the Rabin-Miller algorithm for primality testing.

   SOLUTION:

   On input $(n)_b$:
   1. If $n = 2$, accept; if n is even and $n > 2$, reject.
   2. Choose at random a positive a in $\mathbb{Z}_n$.
   3. If $a^{(n-1)} \neq 1 \pmod{n}$, reject.
   4. Find s, h such that s is odd and $n - 1 = s2^h$.
   5. Compute the sequence $a^{s\cdot 2^0}, a^{s\cdot 2^1}, a^{s\cdot 2^2}, \ldots, a^{s\cdot 2^h} \pmod{n}$.
   6. If all elements in the sequence are 1, accept.
   7. If the last element different from 1 is -1, accept. Otherwise, reject.

2. Let $n > 1$ be any natural number; if $a^{(n-1)} \neq 1 \pmod{n}$, then a is called a *witness* of compositness of n. Show that if at least one witness exists in $\mathbb{Z}_n^*$, then at least half of the elements of $\mathbb{Z}_n$ are witnesses.

   SOLUTION: First note that $S := \{a \in \mathbb{Z}_n | a^{(n-1)} = 1 \pmod{n}\}$ is a subgroup of $\mathbb{Z}_n^*$. You should show this ($1 \in S$, if $a, b \in S$ then $ab \in S$, and if $a \in S$, then so is a^{-1}). By Lagrange's theorem, $|S|$ must divide $|\mathbb{Z}_n^*|$; so if a witness exists, we know that $|S| \neq |\mathbb{Z}_n^*|$, so the next best thing S can be is half of $\mathbb{Z}_n^*$, and so at most half of $\mathbb{Z}_n^*$ can be non-witnesses, and since $\mathbb{Z}_n^*$ is contained in $\mathbb{Z}_n$, and all elements of $\mathbb{Z}_n - \mathbb{Z}_n^*$ are witnesses (because if $a \in \mathbb{Z}_n - \mathbb{Z}_n^*$, then $\gcd(a, n) \neq 1$, so a does *not* have an inverse in $\mathbb{Z}_n$, and so a cannot be in S), the claim follows.

3. Present the RSA public-key cryptosystem.

   SOLUTION: Choose two odd primes p, q, and set $n = pq$. Choose $k \in \mathbb{Z}^*_{\phi(n)}$, $k > 1$. Advertise f, where $f(m) = m^k \pmod{n}$. Compute $l = k^{-1}$ (inverse of k in $\mathbb{Z}^*_{\phi(n)}$). Now $\langle n, k \rangle$ are public, and the key l is secret, and so is the function g, where $g(C) = C^l \pmod{n}$. (Note that $g(f(m)) = m^{kl} \pmod{n} = m$.)

4. Let $n = pq$, where $p < q$ are distinct odd primes, and let $0 < m < p$. Suppose that $kl = 1 \pmod{\phi(n)}$; show that $m^{kl} = m \pmod{n}$.

SOLUTION: Note that $m^{kl} =_n m^{1+x\phi(n)} =_n m \cdot (m^{\phi(n)})^x$, for some x. Now we show that $m^{\phi(n)} =_n 1$. By Fermat's little theorem, we know that $m^{(p-1)} =_p 1$ and $m^{(q-1)} =_q 1$, so $m^{(p-1)(q-1)} =_p 1$ and $m^{(q-1)(p-1)} =_q 1$, thus $m^{\phi(n)} =_p 1$ and $m^{\phi(n)} =_q 1$. This means that $p|(m^{\phi(n)} - 1)$ and $q|(m^{\phi(n)} - 1)$, so, since p, q are distinct primes, it follows that $\phi(n) = (pq)|(m^{\phi(n)} - 1)$, and so $m^{\phi(n)} =_n 1$.