Introduction to Cryptography

Homework 3

Submit by January 22, 2006, *before class*.

Solve 3 of the following 4 questions.

Note: If you cannot solve an item which is part of a question (for example, item (b) in question 2), you can still solve the rest of the question (e.g. items (c) and (d) of question 2) assuming that this item holds.

1. Let p,q be prime numbers, and $n=pq$. *For a number* $m \in [0,1,2,\ldots,n-1]$ we can use the representation $[a,b]$, where $a=m$ mod p, and $b=m$ mod q.
    a. Show that for $m_1,m_2,m \in [0,1,2,\ldots,n-1]$, if the representation of m_1 is $[a_1,b_1]$ and the representation of m_2 is $[a_2,b_2]$, then the representation of $m= m_1+m_2$ is $[a,b]$, where $a=a_1+a_2$ mod p, and $b=b_1+b_2$ mod q. (8 points)
    b. State and prove a similar claim for multiplication. (8 points)
    c. For $x,y \in [0,1,2,\ldots,p-1]$, how is it possible to *efficiently* compute $z=x/y$ mod p? I.e., compute a number $z \in [0,1,2,\ldots,p-1]$ that satisfies $yz=x$ mod p. (9 points)
    d. State and prove a claim (similar to (a) and (b)) for division modulo n. (8 points)

2. Let $n=pq$. Define $\lambda(n)=\text{lcm}(p-1,q-1)$, i.e., $\lambda(n)$ is the least common multiplier of $p-1$ and $q-1$.
    a. Show that if $a=1$ mod $\lambda(n)$ then for all $m \in Z_n^*$ it holds that $m^a = m$ mod n. (Hint: use the CRT.) (18 points)
    b. Show that in the RSA cryptosystem one can choose e,d to satisfy $ed=1$ mod $\lambda(n)$. (Instead of satisfying $ed=1$ mod $\phi(n)$.) (15 points)

3. This question shows that the El Gamal signature scheme is insecure if the signer does not use a new k for every signature.
    - If the same value of k is used for signing m_1 and m_2, then $s_1 = (m_1 - ar)k^{-1}$ mod $p-1$, and $s_2 = (m_2 - ar)k^{-1}$ mod $p-1$.
    - Then, $(s_1 - s_2)k = (m_1 - m_2)$ mod $p-1$.

    a. Show that if $s_1 - s_2 \neq 0$ mod $p-1$, then k can be easily found. (18 points) (Note that gcd($s_1 - s_2$, $p-1$) might be different from 1. You will get a 5 point bonus for handling this case.)

    b. Show that if k is known, then the secret key can be easily found. (15 points)

4. This question shows that the El Gamal signature scheme is insecure if the verifier does not check that $r < p$.

   Let (r, s) be a signature on a message m.
   The adversary can compute a signature on an arbitrary message m' as follows:
   - Set $u = m' \cdot m^{-1} \bmod p-1$.
   - Set $s' = s \cdot u \bmod p-1$.
   - Compute r' satisfying
     - $r' = r \cdot u \bmod p-1$.
     - $r' = r \bmod p$.

   The signature of m' is (r', s').

   a. How is r' computed and what is the range of its possible values? (18 points)
   b. Show that (r', s') is a valid signature of m'. (15 points)