# *Topics in Cryptography: Homework 3*

Submit by March 14, 2008. **Solve three of the following questions.**
**Note:** If you cannot solve an item which is part of a question, you can still solve other items in this question assuming that the first 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 $q$.
   b. State and prove a similar claim for multiplication.
   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 $p$.
   d. State and prove a claim (similar to (a) and (b)) for division modulo $n$.

2. Let $n=pq$. Define $\lambda(n)=\mathrm{lcm}(p-1,q-1)$, i.e., $\lambda(n)$ is the least common multiplier of $p-1$ and $q-1$. (If $p=11,q=19$, then $\lambda(n)=90$.)
   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.)
   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 $\phi(n)$.)

3. Consider the following public-key encryption scheme. The public key is $(G,q,g,h)$ and the private key is $x=\log_g h$, generated exactly as in the El Gamal scheme. In order to encrypt a bit $b$ the sender does the following:
   a. If $b=0$ it chooses a random $y \in Z_q$ and computes $C_1=g^y$ and $C_2=h^y$. The ciphertext is $(C_1,C_2)$.
   b. If $b=1$ it chooses independent random $y,z \in Z_q$ and computes $C_1=g^y$ and $C_2=g^z$. The ciphertext is $(C_1,C_2)$.

   Show that it is possible to decrypt efficiently given knowledge of the private key $x$.

   Prove that this encryption scheme is secure against chosen plaintext attacks if the Decisional Diffie-Hellman (DDH) assumption is hard in $Z_q$.