Introduction to Cryptography: Homework 3

Submit by January 21, 2013.
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 $n=pq$. Define $\lambda(n)=\mathrm{lcm}(p-1,q-1)$, i.e., $\lambda(n)$ is the least common multiple of $p-1$ and $q-1$. (If $p=11,q=19$, then $\lambda(n)=90$.)
    a. Show that if $a=1 \bmod \lambda(n)$ then for all $m \in Z_n^*$ it holds that $m^a \equiv m \bmod n$. (Hint: use the CRT.)
    b. Show that in the RSA cryptosystem one can choose e,d to satisfy $ed=1 \bmod \lambda(n)$. (Instead of satisfying $ed=1 \bmod \phi(n)$.)

2. 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. (g is a generator of a subgroup of order q of G.) 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, by showing a reduction, that if the Decisional Diffie-Hellman (DDH) assumption is hard in the subgroup generated by g, then this encryption scheme is secure against chosen plaintext attacks. Include in your answer an analysis of the error probability of the algorithm which is described in the reduction.