Crypto and Comm Security	**Homework 7**
CS 6750 Fall 2009 (Pucella)	**Due: Nov 19, 2009**

Note on integrity: You may discuss problems with fellow students, but all written work must be entirely your own, and should not be from any other course, present or past. If you use a solution from another source, including someone who helps you, you must cite it.

Questions

(1) In general, the Diffie-Hellman protocol allows two parties to share a common key (hence the name, two-party Diffie-Hellman key agreement). The following natural extension of the two-party Diffie-Hellman protocol allows n parties to share a common key. It is called a group key agreement protocol.

Consider the following protocol to share a common key for three members:

1. A generates a random number $n_1 \in \mathbb{Z}_p^*$ and sends $g^{n_1} \mod p$ to B.
2. B generates a random number $n_2 \in \mathbb{Z}_p^*$ and sends $(g^{n_1} \mod p, g^{n_2} \mod p, g^{n_1 n_2} \mod p)$ to C.
3. C generates a random number $n_3 \in \mathbb{Z}_p^*$ and sends $(g^{n_1 n_3} \mod p, g^{n_2 n_3} \mod p)$ to A, B.

What is the common key? Show how A, B, and C can compute that key based on the information they have received.

(2) Consider the following variant of the Diffie-Hellman key agreement protocol. As in the Diffie-Hellman protocol, let p be a sufficiently large prime such that it is intractable to compute discrete logarithms in $\mathbb{Z}_p^*$. Let α be an element of $\mathbb{Z}_p^*$ of order n. Both p and α are publicly known. Alice has a secret key x_A and a public key $y_A = \alpha^{x_A}$. Bob has a secret key x_B and a public key α^{x_B}. Alice and Bob establish a secret shared key by executing the following protocol:

1. Alice chooses a at random, $0 \leq a \leq p-2$, sets $c = \alpha^a$, and sends c to Bob.
2. Bob chooses b at random, $0 \leq b \leq p-2$, sets $d = \alpha^b$, and sends d to Alice.
3. Alice computes the shared key $k = d^{x_A} y_B^a = \alpha^{b x_A + a x_B}$.
4. Bob computes the shared key $k = c^{x_B} y_A^b = \alpha^{a x_B + b x_A}$.

Does this protocol provide mutual authentication, that is, does the protocol ensure that when Alice completes her interaction, she is guaranteed to have been exchanging messages with Bob, and vice versa, and in particular, that they both share a key with each other, as opposed to sharing one with an adversary? If yes, argue why. If no, show an attack.