Assignment #1

Due: January 13, 2011, 6:30pm

1. Use the extended Euclidean algorithm to derive $P^{-1}\ mod\ Q$ where $P = 23$ and $Q = 89$. Be sure to show all of your work.
2. Suppose you witness someone a sending single message m encrypted to three different friends under three different RSA keys *all using a public exponent of 3.* Suppose that you know all 3 public keys N_1, N_2, and N_3 and see all 3 encryptions. Describe how to use the information you have to determine the message m.
3. Suppose that you have access to a device (e.g. a smart card) with an embedded RSA public-private key pair. The device is willing to disclose its public key $N = PQ$ and perform RSA decryptions, but it will not disclose its private key. Suppose further that the device uses Chinese remaindering to perform decryption. Show how you can extract the private key if the device returns a result in which it has performed the $mod\ P$ portion of the decryption properly but made an error in the $mod\ Q$ portion of the decryption.
4. Suppose that you are witness to a transaction where Bob receives Alice's certified public key and places an order as follows. Bob encrypts the order details using Alice's public key, encrypts his credit card information – also using Alice's public key, concatenates the two encryptions, and then sends them to Alice. Describe how you can exploit this protocol to order your own goods and have them charged to Bob.
5. Suppose that each of three people has a certified Diffie-Hellman public key: $A = Y^a \bmod N$, $B = Y^b \bmod N$, and $C = Y^c \bmod N$, respectively. Describe the steps that each should take so that all will agree upon a common key.