**CIS 481 – Intro to Information Security**

**CLASS EXERCISE # 8**

Grading ID: N1243

**Problem 1**

Using the Vigenère Square on p. 458 and the key COMPUTER, encrypt the following message:

(8 pts.)

COMPUTERCOMPUT

THISISGREATFUN

VVUHCLKIGOFUOG

**Problem 2**

What drawbacks to symmetric and asymmetric encryption used alone are resolved by using a hybrid method like Diffie-Hellman? (7 pts.)

By using a hybrid method, the message senders can avoid several issues with using symmetric and asymmetric encryption alone. First, if the senders only used symmetric encryption, they would have to ensure the keys are kept save since only one of them needs to be obtained for the message to be decrypted. A hybrid encryption decreases this chance since there are different keys that must be used to encrypt and decrypt the data. Second, the hybrid encryption fixes the drawback of asymmetric since it uses a digital signature which eliminates the drawback of having to know the receiver of the message is really who they say they are.

**Problem 3**

If Alice wants to send a message to Bob such that Bob would know that the message *had to come from Alice* **AND** Alice could be certain that *only Bob could decrypt* it, show the necessary steps and keys to use with *public key encryption*. Explain your choices and/or draw a diagram. You may use two rounds of encryption in sequence or explicitly add a digital signature with a hash. (10 pts.)

If Alice wants to send a message to Bob, the first thing she must do is encrypt the message with Bob’s public key. The public key will also be digitally signed in the hash function so that Bob knows for sure it is Alice. The reason for using Bob’s public key is so that Alice can encrypt the message so that only Bob using his private key can decrypt the message. By doing it this way, Bob knows the message has come from Alice and that only Bob can decrypt the message since he has to use his own private key.