**CIS 481 – Intro to Information Security**

**CLASS EXERCISE # 8**

Grading ID: A7386

**Problem 1**

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

(8 pts.)

THIS IS GREAT FUN

VVUHCLKIGOFUOGD

**Problem 2**

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

In symmetric encryption, both parties must possess the same key in order to encrypt or decrypt the data. If a third party is able to get a key, they could decrypt the data without the other parties knowing. Asymmetric encryption requires two distinct but related keys, and while either key can encrypt, only one can decrypt. If key A is used to encrypt, only key B can decrypt. The Diffie-Hellman model combines both models by having both parties create a shared encryption key that is never stored or transmitted, and thus can’t be intercepted, mitigating the risk of symmetric encryption and removing the hassle of asymmetric key limitations.

**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.)

1. Alice starts by choosing two prime numbers and sharing them with Bob.
2. Bob picks secret number a without sharing it with Alice, and computes where g and p are the shared prime numbers. The result is A, it is sent to Alice.
3. Alice chooses her own secret number b without sharing it with B, and computes where g and p are the shared prime numbers. The result is B, it is sent to Bob.
4. Both parties do the same operation, but now with the result that was sent by the other. Alice computes , while Bob computes .
5. = , this is the shared key that is used for communication. Only Alice and Bob can use it because they generated it together, and the key itself was never shared or transmitted, only computed locally. This prevents an unauthorized party from decrypting the data on the channel. Alice can now use this key to encrypt her data, and Bob can use it to decrypt what Alice sends him. (Shout out to Stack Exchange for explaining this in plain English.)