CIS 481 – Intro to Information Security

CLASS EXERCISE # 6-7

Problem 1
Using the Vigenère Square on p. 458 and the key COMPUTER, encrypt the following message: (8 pts.)

```
COMP UT ERCOM PUT
THIS IS GREAT FUN

Encrypted: VVUHCLKIGOFUOG
```

Problem 2
What drawbacks to symmetric and asymmetric encryption used alone are resolved by using a hybrid method like Diffie-Hellman? (7 pts.)

Symmetric encryption has the major drawback of trying to get the key to the end user. Because the same key that encrypted it has to decrypt it, the use must find a way to securely get the key to the end recipient. The main drawback with asymmetric encryption is that to have a single conversation between two parties, involves four keys. Diffie-Hellman hybrid encryption solves this by making it possible to share private keys via public key encryption. The user can encrypt the private key and the message, and send that back to the owner of the public key who can decrypt the message and the key at the same time.

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 and Bob have digital certificates that are stored in a public key infrastructure
2. Alice retrieves the public key that Bob has made available in a repository of some kind.
3. Alice encrypts her message with her digital certificate.
4. Bob receives the encrypted message that only his private key can decrypt.
5. Bob decrypts the message and sees Alice's digital certificate, to identify who the sender was.

This workflow allows ease of use. Both parties can be identified through a digital certificate and still have a public key available for use. Both parties could have their public keys in a repository, and both parties could access they keys anytime, and could be identified using their digital certificate.