**CIS 481 – Intro to Information Security**

**IN-CLASS EXERCISE # 8**

Names of team members: Corey Cooley, Taylor Payne, Will Brown, & John Hopson

Logistics

A. Get into your regular team

B. Discuss and complete the assignment together. Don’t just assign different problems to each teammate! That defeats the purpose of team-based learning.

C. Choose a recorder to prepare the final copy to submit to instructor in Blackboard.

**Problem 1**

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

(8 pts.)

THIS IS GREAT FUN

*VVUH CL KIGOF PUT*

**Problem 2**

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

*The drawback of asymmetric encryption is requiring two keys per party, and with symmetric, the sender and recipient must have the same secret key and if someone else unauthorized got ahold of the key it would render the information integrity and confidentiality breached. Diffie-Hellman allows keys for temporary communication exchanging asymmetric encryption with a symmetric key in order to communicate, fixing the out of band issue.*

*The drawback of asymmetric encryption is the CPU overhead required to maintain encryption during communication due to the need for two keys per party. With symmetric encryption, the problem is the out of band issue, in that a common key must be exchanged between two entities without allowing a potential man-in-the-middle to gain the key as well. The Diffie-Hellman key exchange uses asymmetric encryption to exchange session keys. These are limited-use symmetric keys for temporary communications; they allow two entities to conduct quick, efficient, secure communications based on symmetric encryption, which is less taxing on the CPUs than asymmetric encryption for sending messages.*

**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. (10 pts.)

*First, starting with a plaintext message Alice would encrypt the message with Bob’s public key creating a ciphertext, which ensures only he can decrypt it. In parallel, Alice would run the plaintext message through a hash algorithm Alice and Bob have agreed upon creating a message digest. This hashed digest is then inserted into a digital signature algorithm, which uses Alice’s private key along with a random number to generate the digital signature. The digital signature ensures that Alice and only Alice could have sent the message. Both are sent at the same time to Bob.*

*Bob then uses his private key to decrypt Alice’s message. Bob then uses Alice’s public key to decrypt the digital signature. Then Bob runs Alice’s decrypted plaintext message through the hash algorithm to create his own hashed message digest. Bob can then compare the two hashed messages to see if they match. If they are the same then it couldn’t have been altered in transit.*