CIS-481: Introduction to Information Security

In-Class Exercise #8

IQ Team: 4
Names of team members: Daniel Kearl, Mohammed Al Madhi, Yuxuan Chen, Joseph Baxter

Logistics

A. Get together with other students on your assigned team in person and virtually.
B. Discuss and complete this assignment in a collaborative manner. Don't just assign different problems to each teammate as that defeats the purpose of team-based learning.
C. Choose a scribe to prepare a final document to submit via Blackboard for grading, changing the file name provided to denote the number of your assigned **IQ Team**.

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

THIS IS GREAT FUN

THISISGREATFUN
COMPUTERCOMPUT
VVUHCLKIGOFUOG

VVUHCLKIGOFUOG is the encrypted message.

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

Asymmetric encryption is slower and less efficient than symmetric encryption, but symmetric encryption is easier to break and less secure than asymmetric encryption. Diffie-Hellman encryption uses asymmetric keys in order to create a channel through which the sender and receiver can then communicate with symmetric encryption. The session itself is secured with the more secure asymmetric encryption allowing for the messages to be exchanged quickly with symmetric encryption.

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 points)*

First, Alice encrypts her message using Bob's **public** key, which ensures that only Bob's **private** key can open it (which Bob hopefully has kept secret). This message can now only be decrypted by Bob.

Second, Alice then encrypts the message again using her own **private** key that only she has access to. This ensures that the message came from Alice, because only Alice has access to her own private key.

When Bob receives the encrypted message, he would then decrypt it using Alice's **public** key, revealing the next layer of encryption. Next, he would use his own **private** key to unencrypt and read the message from Alice.