CIS-481: Introduction to Information Security

InfoSec Chapter Exercise #8

Team: Seven
Participants: Jackson Dillingham, Matthew Jackson, Hilton Siaffa, Tabor Payne, Emily Wantland

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 **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
- VVUHC LKIGO FUOG

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

- Asymmetric encryption uses a pair of keys, the public and private key. As the name suggests, the public key is accessible by the public whereas a private key is held by a singular owner, is private, and only known to the owner.
- Symmetric encryption uses a pair of keys that are identical between the receiver and the sender. Both keys are only supposed to be known between the sender/receiver, which is why transmitting the key between secure lines before message transmission is a must if symmetrical encryption is to be used.
- Using a hybrid method such as the Diffie-Hellman algorithm allows asymmetrical encryption to be used to verify the identity of the sender/receiver, by means of a digital signature, whereby once the identity is verified symmetrical encryption is used to encrypt the actual message. This method substantially decreases the amount of computing power that is needed to encrypt entire messages asymmetrically. In addition, the number of keys that are needed decreases and it is much easier to manage.

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)*

- In order for Alice to be sure that ONLY Bob could read the message, she would need to encrypt the message using Bob's public key. When he receives the message, only he will be

able to decrypt the message using his private key. In order for Bob to make sure that the message came from Alice, she would include a digital signature, which is a version of Alice's private key. If Bob can decrypt the digital signature, then the message had to have come from Alice.