**CIS 481 – Intro to Information Security**

**IN-CLASS EXERCISE # 8**

Names of team members: **Trisia Baltazar, Adrian Boone, Savanah Kennedy, Ryan Smith**

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.)

Plaintext: THIS IS GREAT FUN

Ciphertext: VVUHCLKIGOFUOG

* **Take key and replicate as much as necessary**
* **Go to row for C, column for T, intersection is the ciphertext**
  + **“V” in this example**

**Problem 2**

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

**When symmetric encryption is used, an out-of-band technique needs to be used, or the key might get intercepted and the message might get decrypted by someone who the message was not intended for. A message and key should not be sent the same way, but instead separately or out of band. Another problem with symmetric encryption is dealing with all the keys involved when lots of people in a group that are trying to carry on conversations. If 4 people are in a group and each pair has to have a key, 6 keys need to be generated. This number gets exponentially larger, when more people are in the group, like 1,000 people.**

**When asymmetric encryption is used, it can be computationally difficult. There might not be enough CPU to do it successfully.**

**All of these drawbacks are resolved with a hybrid method, like Diffie-Hellman.**

**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.)

-Message integrity

-Source authentication

Step 1 - Encrypt the message using the recipients public key. Alice would encrypt her message using Bob's public key. Bob’s private key is the only key that can decrypt this message. This guarantees that only Bob can decrypt it.

Step 2 - Adding the digital signature. A hash algorithm is used which is the put into the digital signature algorithm along with a random number to generate the digital signature. The digital signature relies on the sender’s (Alice’s) private key. The encrypted message contains the digital signature which can be verified by using the sender’s (Alice’s) public key. This guarantees the message had to come from Alice because no one else could have created the digital signature, because it requires Alice’s private key. Bob can verify the signature by using Alice’s public key.