CIS-481: Introduction to Information Security

InfoSec Chapter Exercise #8

Team: 3
Participants: Marvin Weaver, Sam Steele, Aaron Gordon, Brandon Crosier, Kitrina Justus

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

C O M P U T E R C O M P U T
T H I S I S G R E A T F U N

V V U H C L K I G O F U O G

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)*

Symmetric encryption is a cryptography method where the same algorithm and secret key are used to encode and decode. Asymmetric encryption is a cryptography method that uses a public key and a private key to encode and decode. Whichever key is used to encode a message, the opposite key is used to decode it.

The drawbacks of symmetric encryption are that both parties must know the private key. Also, if an unauthorized individual gets the private key they’d be able to decode every message. The drawbacks of asymmetric encryption are that the company must keep track of many keys, both public and private. They are also not as efficient as symmetric encryption in terms of CPU computations. A hybrid, like Diffie-Hellman, is used to be efficient like symmetric, but secure like asymmetric. A hybrid will use asymmetric encryption to exchange symmetric session keys, allowing the parties to have the security and efficiency desired.

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 must access Bob's public key. Next, Alice must encrypt her message using Bob's public key. As this is public-key encryption, Bob will only be able to decode the message with his private key. This ensures that only Bob will be able to decrypt the message.

To ensure that Bob knows the message had to come from Alice, Alice must incorporate a hash function. A hash function is a mathematical algorithm used to confirm that the sender is who they say they are and the message has not been altered.

⚇ → ⚇ 🔑 → ⚇ 🗝

First, Alice finds Bob's public key

Then, Alice encrypts the message with her hash

Bob checks Alice's identity with the hash function and then decrypts the message