CIS-481: Introduction to Information Security

InfoSec Chapter Exercise #8

Team: 5
Participants: James Hoagland, Ethan Grimes, Holli Grubbs, Gregory Ellis

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

PLEASE WEAR A MASK

ELRDWQEGPRNPAES

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

Asymmetric encryption is a cryptographic method that incorporates mathematical operations that uses both a public key and private key to encipher/decipher a message. Either the public or private key can be used to encrypt a message, but the other key is needed to decrypt it. Asymmetric encryption is also referred to as 'public-key encryption'.

Symmetric encryption is a cryptographic method where the same algorithm and secret key are used both to encipher and decipher the message. It can be programmed into quick computing algorithms and executed quick as well. Symmetric Encryption is also referred to as 'private-key encryption'.

A hybrid method like Diffie-Hellman means that asymmetric encryption is used to exchange session keys. Session keys are limited use symmetric keys. The use of session keys allows for a more efficient and more protected communication based on symmetric encryption which is known to be more efficient than asymmetric encryption.

Using the symmetric encryption method there are drawbacks such as data being potentially exposed because keys are being exchanged out of band; using Diffie-Hellman solves that issue. Also, using Diffie-Hellman instead of asymmetric is more efficient because computational wise it is not as rigorous as asymmetric.

Problem 3 *(10 points)*

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.