CIS-481: Introduction to Information Security

InfoSec Chapter Exercise #8

Team: 1

Participants: Jacob Forcht, Zack Graas, Trevor Hagel

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:

Phrase: PLEASE WEAR A MASK
key : PANDEM ICPA N DEMI
Encrypted: ELRDWQ EGPR N PEES
key : PANDEM ICPA N DEMI
Decrypted: PLEASE WEAR A MASK

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?

The difference between symmetric and asymmetric encryption is that asymmetric encryption uses two different keys, public and private key, to decipher a message. Symmetric encryption uses the same algorithm to decipher the message. A drawback for when sometimes the symmetric keys don't have a lot of use to them since they use one algorithm and asymmetric deals with keys that could not be safe since it uses public keys. What the hybrid method, like Diffie-Hellman, does is it uses asymmetric systems with symmetric's sessions key to decipher messages at an efficient rate.

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.

If Alice wants to send a message to Bob and ensure that both he alone can decrypt it and know it came only from Alice, she could use public-key encryption with PGP. Both Alice and Bob would need to have a private and public encryption key. The public and private keys are connected to each other and allow encryption and decryption of messages through this connection. Bob and Alice should know or have access to each others public encryption key.

To start, Alice would encrypt her plain text message using her private key and Bob's public key. Once she has done this, she can add a "signature" which is encrypted using only her private key. Once Bob receives her message, he can attempt to verify her signature by using her public key to decrypt it. If it is a legitimate signature, the connection of Alice's public and private keys allows for it be verified. Bob can then use Alice's public key and his private key to decrypt the message she sent. Since it was encrypted with her private and his public, it would be able to be decrypted by Bob using the alternate of what it was encrypted with.