CIS-481: Introduction to Information Security

InfoSec Chapter Exercise #8

Team: 7
Participants: Zach Gonzalez, Quinn Fessler, John Moriarty

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
PANDEM ICPA N DEMI -> Group into fives
= PLEAS EWEAR AMASK
PANDE MICPA NDEMI

ELRDW QEGPR NPEES

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 made up of a pair of two passwords or open and private keys that are used to convert encryption to decryption. Symmetric encryption only uses a single key to decode encoded data. It is a relatively older type of encryption and not as superior as asymmetrical encryption because its password or keys are converted during the data transmission as well. The drawback faced using these encryption methods alone is that wherever the passwords or key(s) are sent all the encrypted data is sent with it. The hybrid method like Diffie-Hellman can resolve this issue by allowing two parties to communicate over a public channel and have a mutual secret without passing it over the internet.

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.

The simplest approach to this issue would be a secret-key algorithm, in which Alice and Bob are confidentially sharing the key to their encryption. Using this method, Alice and Bob can freely

exchange messages and use a key to encrypt *and* decrypt messages. Bob would be certain the message came from Alice *as long as* no external parties have gained access to the key(s). Keys must be communicated across different mediums and can become quite unmanageable after a fair amount of time has passed and more keys become necessary. Hash functions would not be very practical in this scenario, as hashing is a form of one-way encryption and is nearly impossible to revert. Hash encryption is much more practical for database matching rather than interpersonal communications.