CIS-481: Introduction to Information Security

InfoSec Chapter Exercise #8

Team: Project Team 11
Participants: Sohal Patel, Erika Maglasang, Nathan Moran, Gabriel Rolink, and Tyler Samuelson

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

The key Computer and the encrypted version of statement is as: VVUHCLKIGOFUOG

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)*

- The only difference between asymmetric and symmetric encryption is that asymmetric encryption is actually comprised up of a pair of two passwords or keys open and private keys, that are used to converted the encoded data (encryption) to decoded (decryption) whereas the symmetric encryption only uses a single key to make forth the conversion of encrypted data into decrypted one.
- Symmetric way of encryption is relatively older than that of asymmetric encryption. Whereas, the asymmetric encryption is better than that of symmetric encryption because the passwords or keys are converted during the transmission of data. The drawback of symmetric and asymmetric encryption is that whenever the open or private key of asymmetric encryption and the single key of symmetric encryption is sent; the encrypted data is sent along with its key using which; when any hacker accesses the encrypted data the key is most probably in the messages or email addresses by the use of which hackers can easily decrypt it, the hybrid model like Deffie-Hellman devises various method to provide solution to this problem.

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)*

Answer: If Alice has to send confidential or private data of any type or intensity to Bob, then there is a possibility where a public and private key can be used as a whole, the points to be initiated lead to what could actually be the possible solution for this question.

1. As per the given scenario the public key could be accessed by everyone.
2. Open key encryption, as a technique for encoding information of Alice with two distinct keys and making one of the keys, the open key, accessible for BOB to utilize. The other key is known as the private key. Information scrambled with the open key must be decoded with the private key, and information encoded with the private key must be unscrambled with the open key. Open key encryption is otherwise called deviated encryption used by Bob.
3. Open key Encryption is significant in light of the fact that it is infeasible to decide the decoding or decryption key used by Bob given just the information on the cryptographic calculation and encryption key.