CIS 481 – Intro to Information Security

IN-CLASS EXERCISE # 8

Names of team members: Volodymyr Bestiyanets, Nick Cunningham, Timothy Mahan, and Shawn Nasr.

Logistics

A. Get into your regular team

B. Discuss and complete the assignment <u>together</u>. Don't just assign different problems to each teammate! That defeats the purpose of team-based learning.

C. Choose a recorder to prepare the final copy to submit to instructor in Blackboard.

Problem 1
Using the Vigenère Square on p. 458 and the key COMPUTER, encrypt the following message: (8 pts.)

COMP UT ERCOM PUT
THIS IS GREAT FUN: **VVUH CL KIGO UOG**

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

Hybrid encryption methods, such as the Diffie-Hellman key exchange, integrate symmetric and asymmetric algorithms into cryptosystems. This method uses asymmetric encryption to exchange session keys, which are symmetric keys with limited-use that allow two entities to have temporary, efficient, and secure communications during an online session, based on symmetric encryption. The asymmetric encryption alone is less efficient with key use and CPU computations than symmetric and hybrid methods. The asymmetric encryption method requires involved parties to use an excessive amount of keys to have communications. Symmetric encryption involves getting the key to a receiver, while staying out of bound to avoid interception. The hybrid methods protect data from exposure to third-parties that can occur while exchanging keys out of band, by using asymmetric session keys that expire usually after a few minutes.

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. (10 pts.)

1. Alice goes to the public key registry found within their organization and obtains Bob's public key.
2. Alice and Bob agree upon a hash algorithm that they want to use to create their respective message digests.
3. Alice encrypts the message using Bob's public key.
4. Alice also uses her own private key to create a message digest using the agreed upon hash algorithm.
5. Alice uses a digital signature algorithm as well in order to create her digital signature and then implements this into the message.

6. The message is then transmitted.
7. Bob decrypts the message using his own private key.
8. Bob goes to the public key registry and obtains Alice’s public key.
9. Bob uses the same agreed upon hash algorithm to reveal the message digest that contains Alice’s digital signature.
10. Bob uses Alice’s public key to verify and decrypt the digital signature also contained within the message.