CIS-481: Introduction to Information Security

Module 10 - Cryptography

Exercise #8

Team:

Participants: Emmett Swann, Yogesh Timshina, Luke Leveque

Logistics

A. Get together with other students on your assigned **Team** in person and/or 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 and may impact your performance on assessments, especially with respect to the essay questions.
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. 389 and the key **CYBERSECURITY**, decrypt the following ciphertext message:

GLDVPHXKIEQLDWL

Result: ENCRYPTIONISFUN

Be sure to show or describe your work decrypting the message.

First you must line up the keyword and message, and align letters together, repeating the keyword as needed to match the length of the message. Then you must use the keyword as the column headers and follow down the rows until you find the matching message letter, and record the letter in the associated row. Continue the process until each associated letter is produced.

C Y B E R S E C U R I T Y C Y
G L D V P H X K I E Q L D W L

Column C, contains G = E
Column Y, contains L = N
Column B, contains D = C
Column E, contains V = R
Column R, contains P = Y
Column S, contains H = P
Column E, contains X = T
Column C, contains K = I
Column U, contains I = O
Column R, contains E = N
Column I, contains Q = I
Column T, contains L = S
Column Y, contains D = F

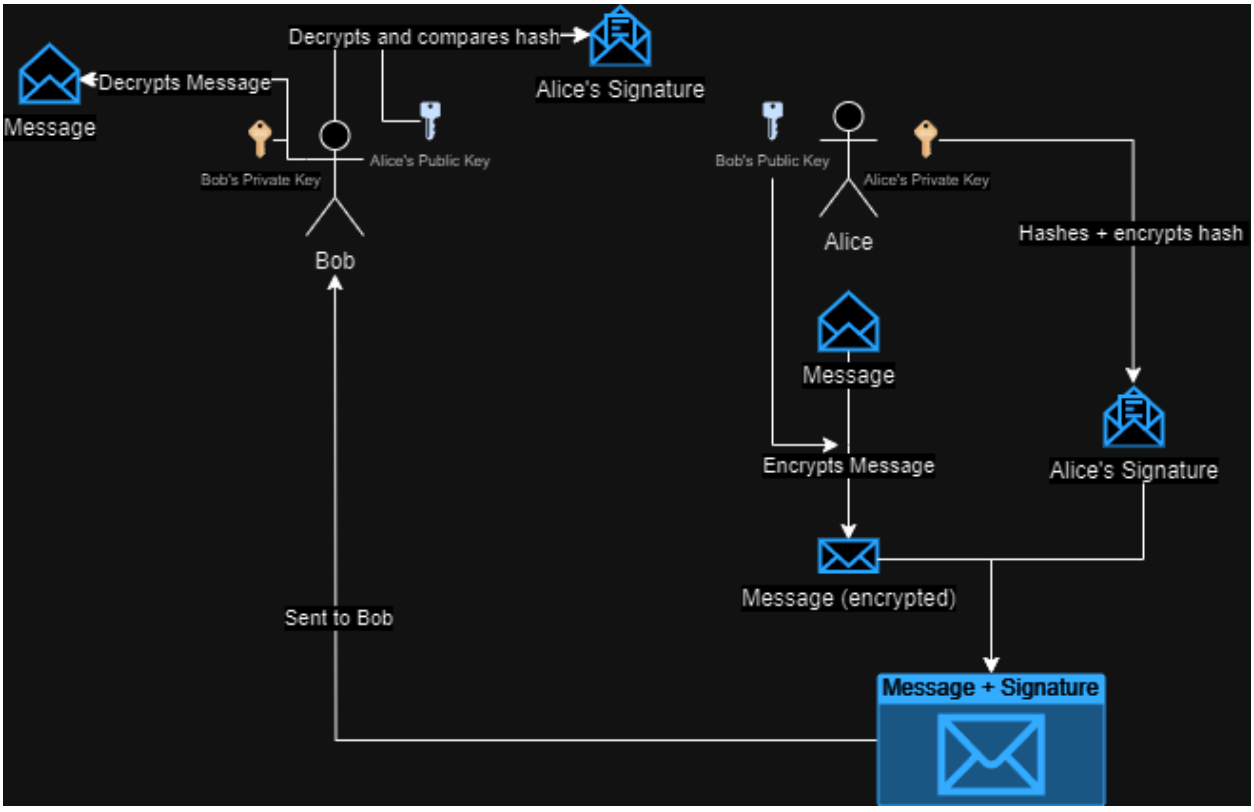
Column C, contains W = U
Column Y, contains L = N

Thus yielding ENCRYPTIONISFUN.

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

Symmetric encryption is where the encoding key and decoding key are the same. This means that in the encrypted message, only one key is created. Asymmetric is different in that mathematic operations generate two different keys. One key is used to encode messages and the other is used to decode the message. The issue with symmetric keys is getting them to the other person, which must be done “out of band” as the book refers, to avoid interception. The problems with asymmetric encryption that is solved is that the asymmetric encryption is only used for the transmitting of the key to be used, which reduces the intensity and heavy computer resources needed.

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*. Use a diagram to explain the process. You may use two rounds of encryption in sequence or explicitly add a digital signature with a hash.



1. Bob creates private and public key.
2. Alice creates private and public key.
3. Alice hashes the message and encrypts the hash with her private key to create a signature.
4. Alice gets Bob's public key.
5. Alice encrypts message and signature with Bob's public key.
6. Sends message and signature to Bob.
7. Bob decrypts the message with his private key.
8. Bob gets Alice's public key.
9. Bob uses Alice's public key to get the message from the signature.
10. Bob hashes the original message and compares it to the hash in the signature.