**Georgia Gwinnett College**

**School of Science and Technology**

**ITEC 3300: Information Security**

**Homework Assignment 3**

You hold the secret code to unlock a hidden treasure that is to be shared by three people. You are to send them the code but need to ensure that no one else can discover the code, and the three open the code *together* so that *no individual or no two* of the three can uncover the code and run away with the treasure.

**Problem 1 [50 Points]**

Suppose that you have *already* *shared a private* **AES** *key with each of the three people*. Devise a method to encrypt the code so that

1. *Only* the three people can open the code.
2. The three can open the code *only when they are all present*. That is, the code will remain secret if just one of the three is absent.

Explain why your method satisfies the above criteria and describe how the three would open the code when they are all present.

**The code/message would need to be encrypted three separate times, once with each of the private AES keys, and then, when all three members are present, the encrypted code would need to be decrypted with each key in the same order that the code was encrypted.**

**Problem 2 [50 Points]**

In this problem, you will implement your method from Problem 1 using **OpenSSL** commands, following the steps below.

1. Connect to vpn.ggc.edu using the Cisco AnyConnect Secure Mobile Client and log in to 172.20.1.106 by SSH, as you did in OpenSSL Lab 1.
2. Create a directory named **hw3** and change directory to **hw3**.
3. ![A close up of text on a black background

   Description automatically generated]()Create a new file, make up a secret code (like “Open Sesame”), type the code in the file, then save and name the file as **code.txt**. View the content of the file to be sure that it contains the code. *Take a screen shot of your commands and the content of* **code.txt***. Include the image here*.
4. ![A close up of text on a black background

   Description automatically generated]()Using proper OpenSSL commands, randomly generate *three 256-bit keys* for **AES** and write the keys to files named **key1.bin**, **key2.bin** and **key3.bin** respectively, pretending that they are the private keys shared with the three people. *Take a screen shot of your commands and include the image here*.
5. ![A close up of a black background

   Description automatically generated]()Using proper OpenSSL commands, encrypt **code.txt** following your method from Problem 1 and name the final ciphertext **cipher.bin**. This is the ciphertext to give to the three people. *Take a screen shot of your commands and include the image here*.
6. Now all the three people are present in front of the hidden treasure and ready to open the code to unlock the treasure. Using proper OpenSSL commands, decrypt **cipher.bin** following your method from Problem 1 and name the plaintext **plain.txt**. View the content of **plain.txt** to make sure that **plain.txt** and **code.txt** are identical. *Take a screen* ![A close up of text on a black background

   Description automatically generated]()*shot of your commands and the content of* **plain.txt***. Include the image here*.