Feb 04

EE 5453 – Assignment #2

Due date: Feb 11, 11:59 PM

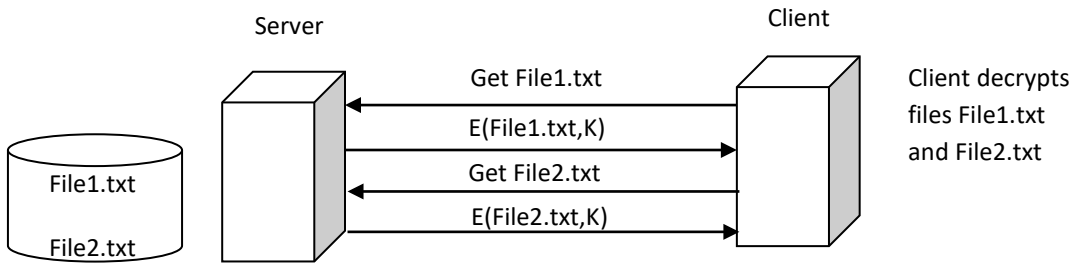
--

<u>This is a group assignment. Work with your group. One submission per group is sufficient.</u>

Problem #1

Build a file server from which a client can request files. Pick a programming language and investigate how to use its networking libraries. Conduct some research on network or socket programming in the language you choose. I recommend C++, Java or Python.

Build on the above so as to provide confidentiality of the files transmitted by the server to the client. Use a symmetric key crypto algorithm such as AES in CBC mode. Generate a key on the server side. Export this key into a file. Using a "secure/private" channel, copy this file (key) to the client computer.



Consult the crypto libraries for the programming language you chose. For example, for Java, do an Internet search on "Java Crypto library" or "Java encryption example". You can find crypto libs for C++ and Python as well. The goal is to learn how to use the crypto APIs for symmetric key encryption and decryption, key generation and for exporting the key so it can be shared between the client and the server.

Submit the following to Blackboard by the deadline as single zip file with the file name <LastNameFirstName>.zip.

(a) A one to two page report detailing the team composition, each member's task(s), minutes from each meeting among the teammates, and the overall approach that was taken to solve this problem.
(b) The source code.