CS610 – Project #4

Overview:

Creatw a Dropbox®-like client-server application (with a few security enhancements).

Description:

Add functionality to your application so that it supports enhanced security and file sharing among users. Files should only be stored on the server in encrypted form using a key the server does not know. Therefore, if the server is compromised a user's files are not. Note that the files will be stored in unencrypted form on each of the client's computers but never on the server. Also, implement sharing so that a user can specify that a particular file in his or her cloud storage should be shared with other users. For example, Alice might specify that file X should be shared with Bob and Carol and that file Y should be shared with Carol and Dave. Shared files must always be stored encrypted on the server and must be synched with all users who share them. Again, I **strongly** encourage you not to write your own encryption routines but to use existing well-known and trusted cryptographic libraries. Also, **please think very carefully about how you will implement encryption, sharing, and synching before you start coding**. I recommend that you review how OpenPGP (http://www.ietf.org/rfc/rfc4880.txt) handles encrypted messages sent to multiple recipients.

Deliverables:

Submit a design document and a tarred copy of your code using the "Project 4" link under "Assignments" in Canvas.

- Your design document should explain the high-level design of the functionality you added for this project. Do not append this to your design document(s) for previous projects and do not re-explain to me the functionality you implemented previously (assuming it hasn't changed – if your design and implementation has changed significantly then you will need to cover that in your Project 4 design document). Make sure to describe any non-standard libraries you use and how you use them. You don't have to tell me about iostream, fstream, or any other standard programming libraries, but if you use socket, cryptographic, or other "specialized" libraries please describe them.
- Your tarfile should include a file named README that explains how to compile and run your programs, how to use the client, and any known bugs either contains. Leave your server running on stu until your project has been graded.
- I will probably need at least three client accounts in order to test your programs.