By default, SQLite does not support any form of user account authentication. SQLite is different from other relational databases in this way as an SQLite database is fully contained in a single file. The only way to control access (without additional software or adding an extraneous source code file to your SQLite build) is to set file permissions on the database file.

Another method is to add a specific source code file to the build that activates user authentication logic. Activating this logic enables the use of several different APIs to facilitate user authentication.

The last method involves using separate software to encrypt the SQLite file which password protects the database. Some of this software requires the purchase of a license (Like SEE), but most of this software is open source (Like SQLCipher which is what we’re using in class). The different types of software used for encryption use different methods of encryption to produce the desired result, which can lead to compatibility issues when trying to open a file encrypted by different software.