**Things that I will be doing:**

Will be using HMAC SHA-256 to encrypt the files.

Will be using SHA-512 to encrypt the passwords

Will require a key to do this encryption.

Will only need one key and the key can be derived from the password inputted by the user.

**Questions relating to functionality:**

Q. How can Each user can only see their part of the database?

Q. How will I store the user passwords securely?

Hash the passwords using salt and SHA-512, then put into the database.

Q. Where would I store these salt values?

Q. How to derive key from password?

Crypto.Protocol.KDF.PBKDF1 from the Crypto.protocol package.

Q. Where do I store the file sensitivity information?

**Questions to be answered for the report:**

Why am I using HMAC SHA-256 and not normal hashing?

Why am I deriving the key required by HMAC using the passwords?

How did I securely store the passwords?

How did I support more than 1 user?

Why did I use a salt value?