**README**

**How does the program works:**

For this second version of the program, I have used bcrypt to hash the passwords. Indeed, I haven’t been able to install Tink, so I decided to use bcrypt which is a well known librarie for cryptography. This library provides us the bcrypt hashing function which is a strong hashing function based on the blowfish cipher. This function is great for hashing password, because it is slow to compute and also a One-Way function. The bcrypt library allows us to hash password with a different hash for each password and give us a function to check password.

To encrypt the password with AES-SIV mode I used the minscreant library.

To store the data, instead of using a txt or a csv file, I choose to use an SQL database, which is much more practical than a txt file. Indeed, with a SQL database, I have been able to store byte variable directly as TINYBLOB instead of converting them into strings before writing them on a txt file.

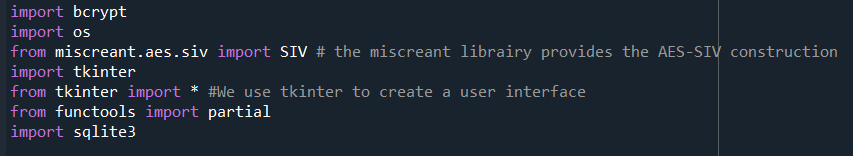
My problem in the last version was that I wasn’t able to catch the data from the txt file and convert them from str to byte as they were before storage. Now with the SQL database, I can catch data directly as byte.

I use a way of writing the data on the SQL database ( with an ? ) which is resistant to SQL injection attack.

**How does the program works:**

I have tried to make the whole program automated. You may have to install some libraries, because I chossed to use tkinter to make a user interface to add users in the database and check if a password is correct for a choosen username.

Here is the list of libraries I have used:



When you will launch the program, a window pop up, were you will enter a username and a password and they will be stored automatically on the database when you click the Add User button.

Then a second window should pop up and you will have to enter a user name and it’s password and when you will close this window a third window open and tells you if the password is correct or not.

Because I am using SQL, the datas or visible with DB browser for SQlite, but if you don’t want to download this tool you will find the datas on a txt file wich is here just to visualize the database, but is not actually usefull.

Some Users are already on the database and all have their password equals to their username (ex : username : guillaume and password : guillaume or username : admin and password : admin ), so you can also try to check password with those users.

The program is separated in different part, so you can also try each function separetly or use the print after each function.