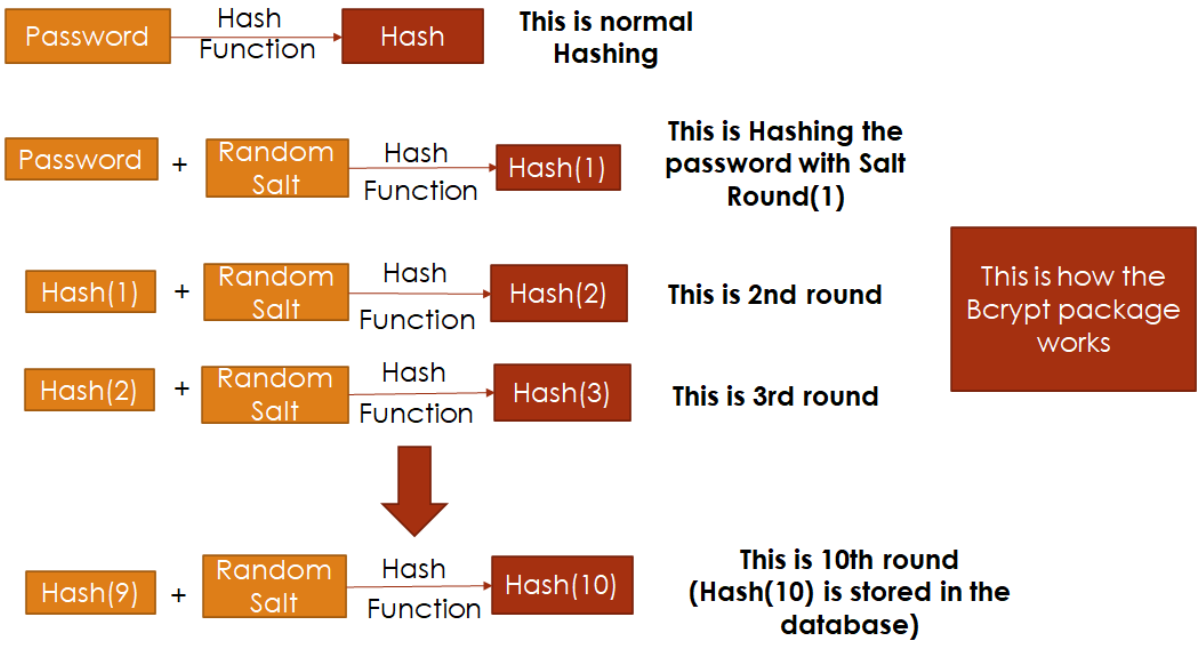
Authentication and Encryption

Authentication

- The main idea of this project is to simulate the authentication and encryption of a user's password.
- Authentication is the process of recognizing a user’s identity. It is the mechanism of associating an incoming request with a set of identifying credentials.
- The credentials provided are compared to those on a file in a database of the authorized user’s information on a local operating system or within an authentication server.
- The registered users are the only ones who can access the resources which are present in the website.
- The second main part of this project is, the website won’t save the user’s plain password in the database. It stores the encrypted password in the database.
- In this way, we are enhancing the security of the user's password.

Encryption

- In this project, we are encrypting the user’s password using a built in npm package called Bcrypt.
- This package encrypts the user’s password by using Hashing & Salting methods.
- Normally a hash is generated whenever we pass a password into a hash function.
- But here to make the password even more secure, we are salting the password and passing into a hash function to generate a hash.
- In this package, we have one more parameter called salt Rounds. Basically if the value of this salt Rounds is 10. That means the algorithm runs for ten(10) rounds.
- By doing this, we are making this algorithm even stronger.
- That’s why it is very difficult to crack this encrypted password.



Workflow

The general workflow for account registration and authentication in a hash-based account system is as follows:

1. The user creates an account.
2. Their password is hashed and stored in the database. At no point is the plain-text (unencrypted) password ever written to the hard drive.
3. When the user attempts to login, the hash of the password they entered is checked against the hash of their real password (retrieved from the database).
4. If the hashes match, the user is granted access. If not, the user is told they entered invalid login credentials.
5. Steps 3 and 4 repeat every time someone tries to login to their account.