Salt Discussion

Salt is user specific component joined to an encrypted password to distinguish identical passwords. The brute force way of finding out the password usually involved a rainbow attack. A rainbow table with millions of password and their hashes already computed by matching that table against the database the password can be recovered, thus we salt the password. This means adding a random text to the password before calculating the hash. Salts are usually long strings. Usually users do not select long passwords so a rainbow table with hashes of smaller passwords is feasible. When a salt is used the rainbow table must accommodate for the salt also this makes is difficult to computationally this is preferred to add a salt to a password before computing their hash value.