# how to store a password

Storing passwords in plaintext is bad, to protect the passwords we hash them, that way even if a hacker sees the hashed passwords, he wont be able to use them.

But hackers can use lookup tables to try and guess the original password from the hashed one! To combat that we add a salt to every password as we generate its hash, assuring that each hash is random, that makes the job of guessing the password even harder.

We can store the salt without encryption, the hacker cant use the salt to guess the original password.

In other words, rainbow tables are only effective when you are trying to break many passwords that were all digested the same way, using the same digest algorithm. Throwing in different salt for each password means that the passwords are not all digested the same way.