#flo #inclass #atomic

---

1 | **Password Storage**

passwords. how do we store them?

- dumbest solution:
  - stores all passwords in cleartext on the db.
    - this may be the dumbest, but it's also the easiest! so it actually happens.

why is this dumb? we should expect that our data will be breached. and, all of our employees can see the passwords.

- next best thing
  - encrypt the passwords, with a hash!
  - hash should not have collisions, and should not be reversible.

```
title: non-collision
bijective. every input leads to a different output.
```

if you get a large amount of hashes, you can use the common passwords and hash them, then compare the hashes. this precomputed table of hashes is called a **rainbow table**

```
title: salt
random unencryted string
add this, public and available salt to the password, then hash that.
```

this helps against rainbow table. because the password in the rainbow table won't be precomputed with with salt.