Developer Tips

Ron Fybish

Easy Steps

HOW ARE PASSWORD STORED?

Developer Tips

Ron Fybish

Do you want to know how to keep a user password safe?

Let's explore!

Developer Tips

Ron Fybish

The **primary** security mechanism when storing passwords **Is not**

❌ **Encryption**

But rather

✅ **Hashing**

Here's the reason why

Developer Tips

Ron Fybish

Encryption

Encrypting a text means that it is possible to get the text back by decrypting it

An authorized person can know the user's password by decrypting it if they know the key

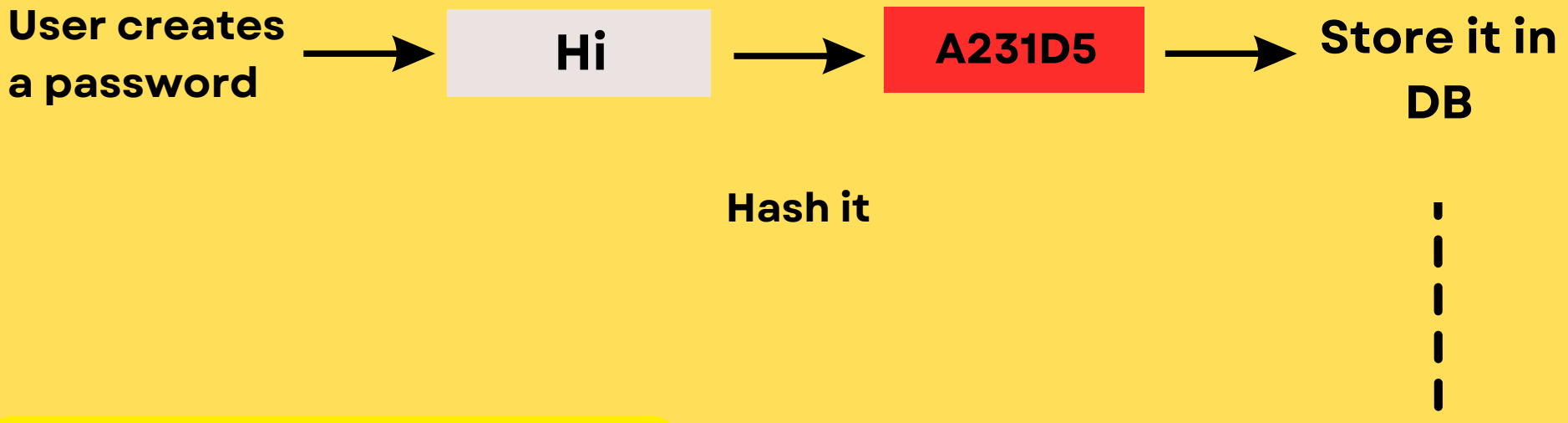
Developer Tips

Ron Fybish

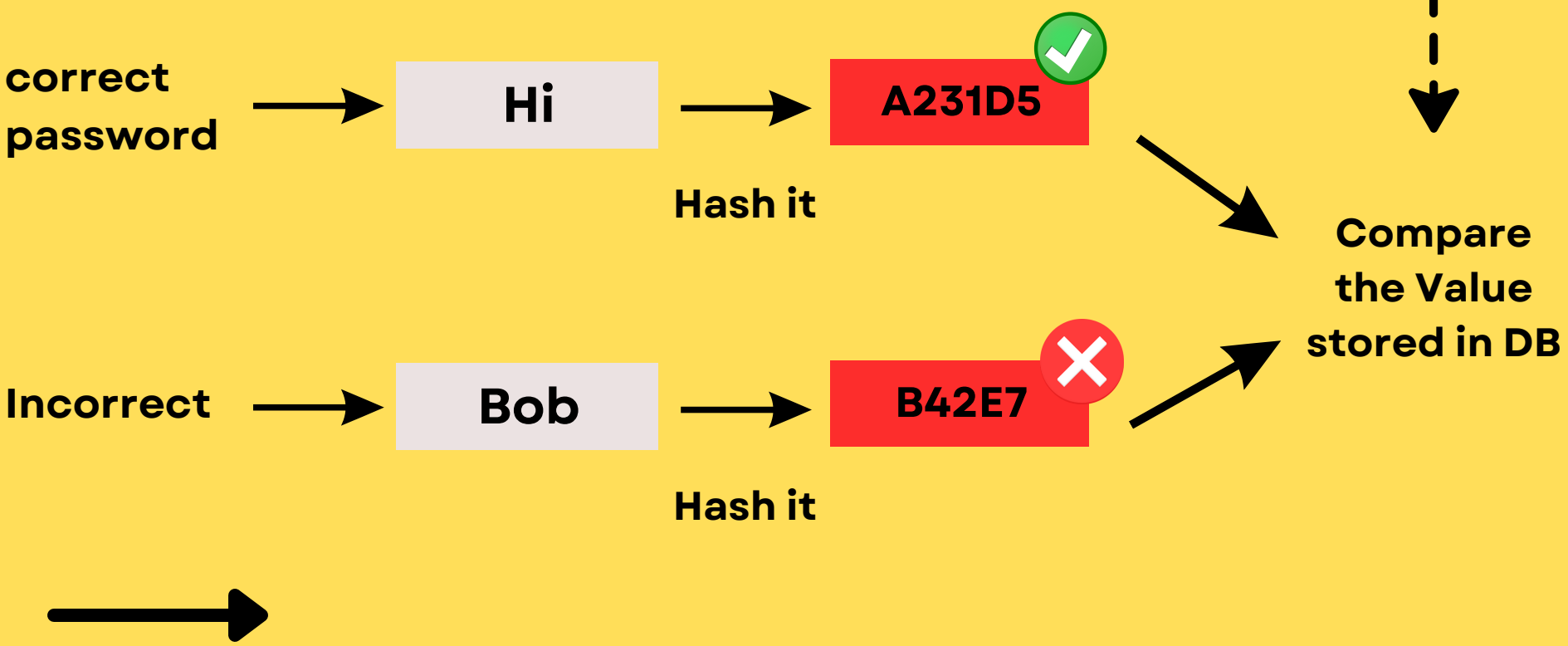
Hashing

Hashing is a way to encrypt text. When we hash something, it produces a digest. But you cannot decrypt the text from the digest.

When a user creates an account:



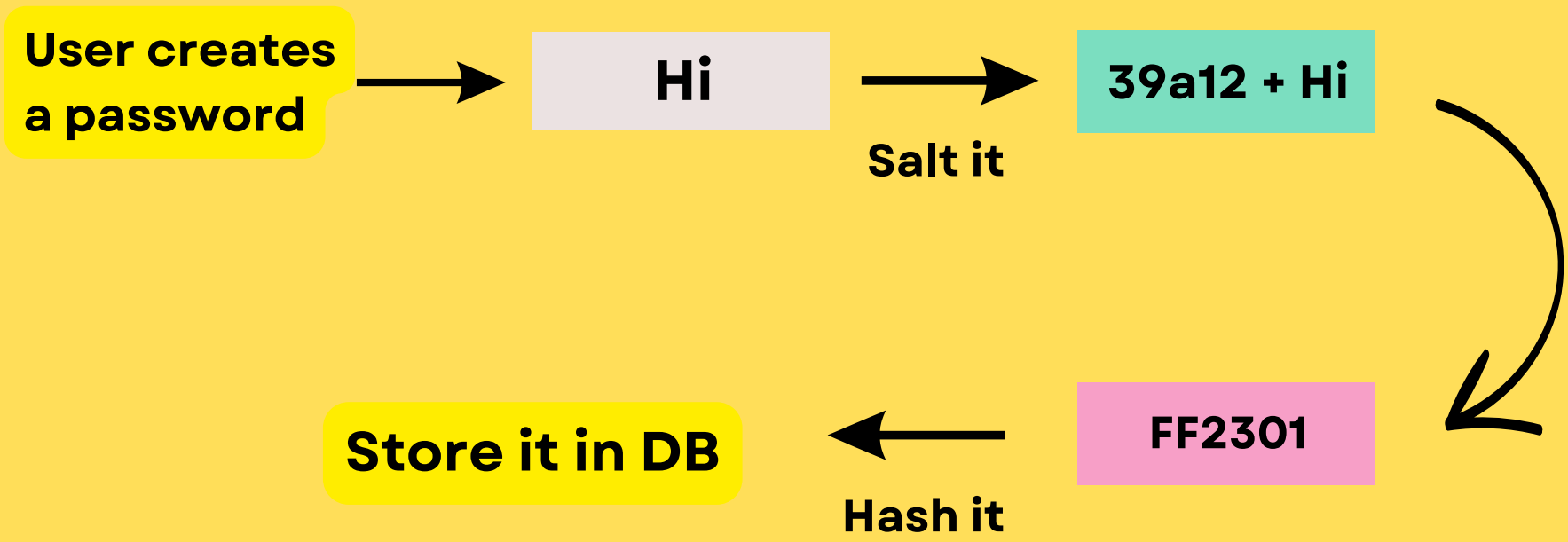
When user logs in:



Developer Tips

Ron Fybish

In addition to Hashing the password, you can also Salt it.



Salt is a unique piece of data for each user and is added to the password before it is hashed. This will also ensure that no two passwords have the same hash.

Ron Fybish

Libraries

The most popular password-hashing algorithms are:

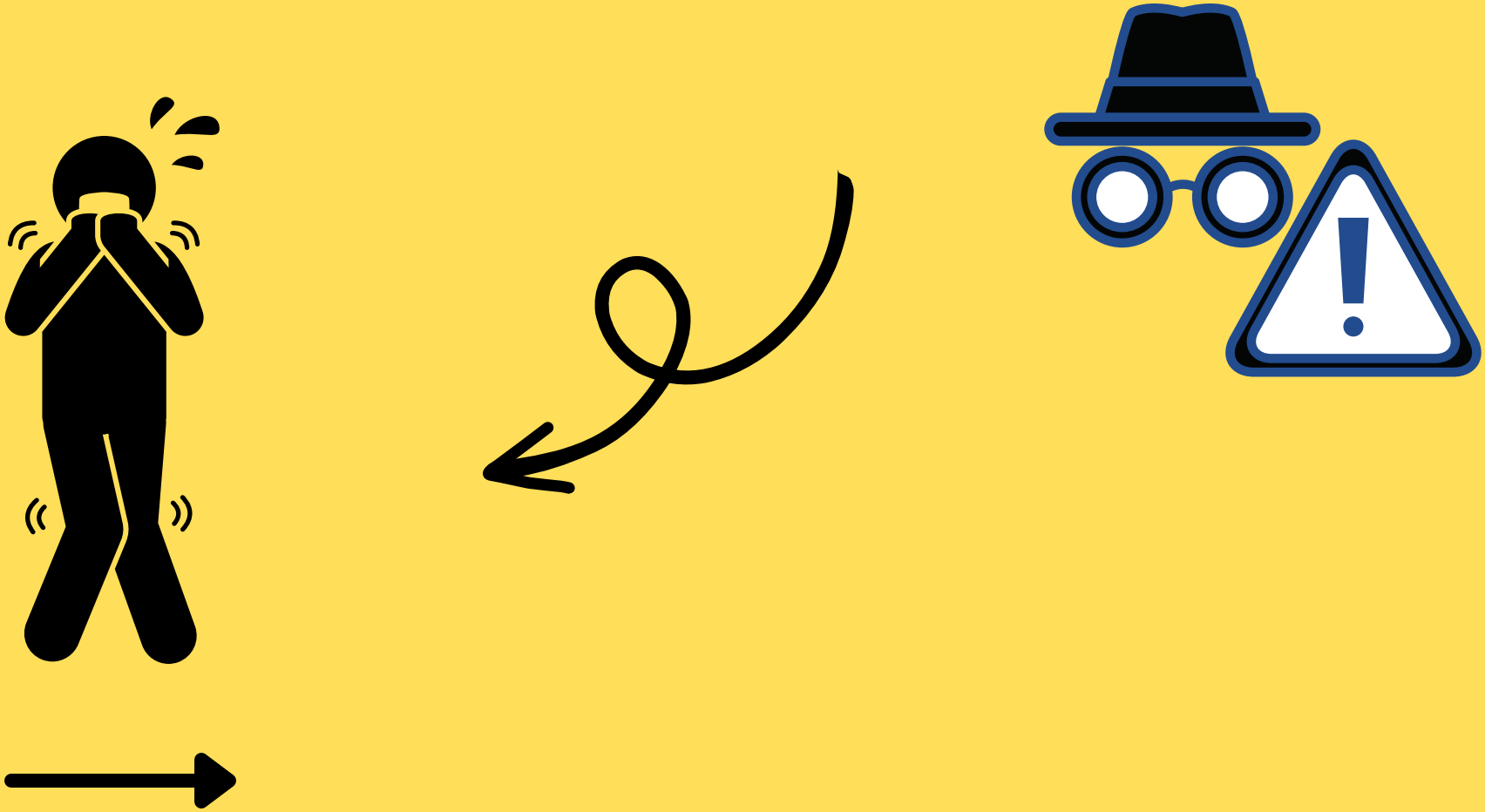
- **PBKDF2**
- **bcrypt**

They are suitable for password hashing and have a built-in salting mechanism.

Developer Tips

Ron Fybish

Using a library for hashing passwords is always recommended instead of trying to implement your own



Ron Fybish
Developer Advocate

What do You Think About This Post?

I hope this helps! Comment below
to let me know what else you like to learn.
Follow @ronfybish to get updated :)