Password Authentication

Server has to store some information about your password.

What if the server stores it exactly?

Could easily steal all the passwords if server is compromised.

(Same passwords might be used in multiple places... x_x)

Anyone know about hash functions?

hash functions are hard to invert:

if $h: X \to Y$, then for

$y \in Y$, it is hard for any efficient procedure (computer program) to find any $x \in X$ s.t. $h(x) = y$. ←

So, we could store h(password) instead of the password itself.

Prime test as a "fold":

$$\left.\begin{array}{ll} x_1 & n \% 2 \neq 0 \\ x_2 & n \% 3 \neq 0 \\ \vdots & \quad \vdots \\ & n \% (n-1) \neq 0 \end{array}\right\} \text{AND.}$$

Just need to fold over &&