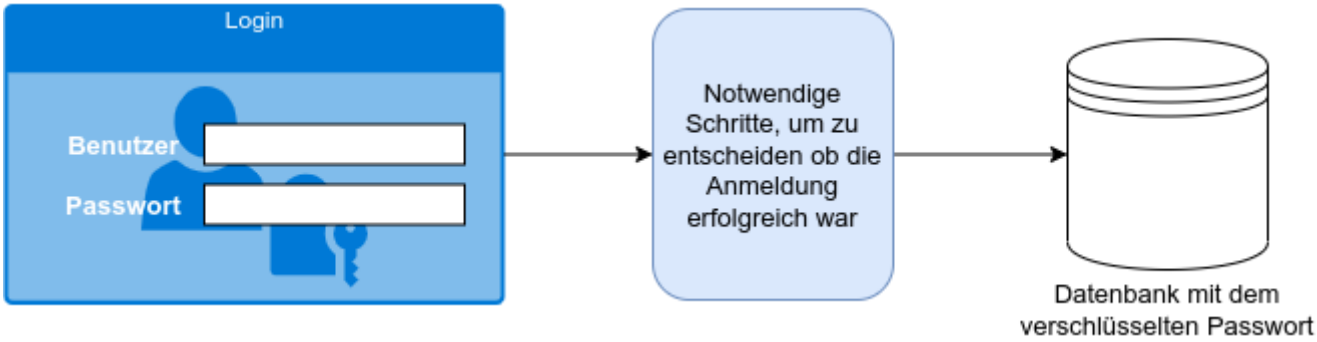
Hashfunktionen

Ein kleines soziales Netz

Passwörter speichern

Für eine Microblogging Plattform möchtest du die Zugangsdaten deiner Nutzer in der einer Datenbank speichern, insbesondere den Benutzernamen und das Passwort, das die Benutzer zur Anmeldung verwenden. weil du in Informatik gut aufgepasst hast, ist dir sofort klar, dass es nicht in Frage kommt, die Passwörter unverschlüsselt in der Datenbank abzulegen.

Dein erster Gedanke ist: Die speichere ich verschlüsselt in der Datenbank ab! Die Situation stellt sich also wie folgt dar:



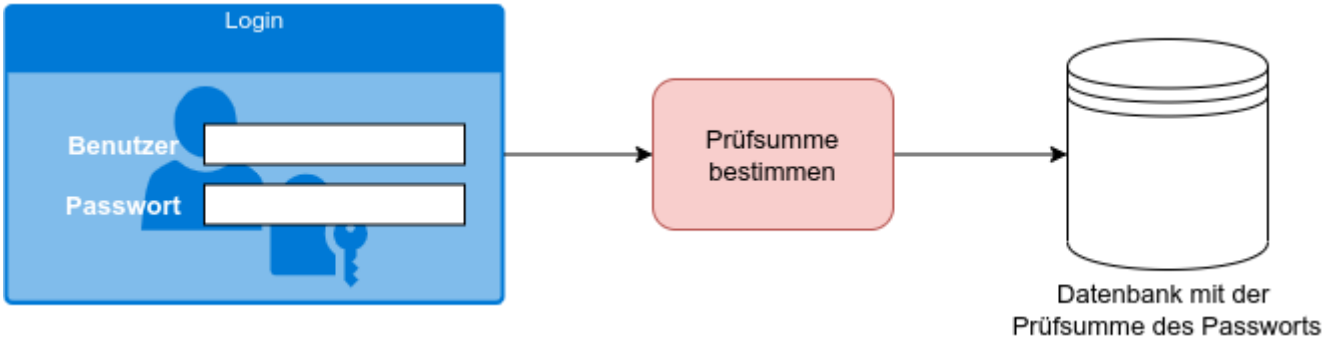
(A1)

Fritz Mayer meldet sich durch Eingabe seines Benutzernamens und seines Klartextpassworts am Login Formular an.

- Überlege dir, wie der Vorgang ablaufen könnte, der dazu führt, den Anmeldeversuch bei Eingabe des richtigen Passworts als "korrekt" zu bewerten.
- Welche Probleme erkennst du, wenn das Passwort verschlüsselt in der Datenbank gespeichert wird?

Die Prüfsummenstrategie

Du überlegst dir, anstatt des verschlüsselten Passworts eine **Prüfsumme** in der Datenbank zu hinterlegen. Jetzt kannst du die Prüfsumme eines eingegebenen Passworts berechnen und mit der gespeicherten Prüfsumme vergleichen:



Dein Entwicklungschef schlägt dir zwei Möglichkeiten vor:

- Die **iterierte Quersumme** ist die Quersumme, die entsteht, wenn man solange immer wieder die Quersumme ausrechnet, bis nur noch eine einzige Ziffer übrig bleibt. Beispiel: Für die Zahl 97 lautet die normale Quersumme 16, berechnet man davon wiederum die Quersumme, so entsteht die iterierte Quersumme: 7.
- Die **alternierende Quersumme** entsteht durch abwechselndes Subtrahieren und Addieren der einzelnen Ziffern. Beispiel: Für die Zahl 1234 ist die alternierende Quersumme 1 - 2 + 3 - 4 = -2).

Um unsere Überlegungen einfach zu halten, lassen wir fürs Erste nur Kennwörter zu, die aus Zahlen bestehen.

Benutzername	Passwort	Iterierte QS	Alternierende QS
martin	12345	1+2+3+4+5 = 15 → 1+5 = 6	1-2+3-4+5 = 3
susi	123456		
franzi	12223345678		
karle	123456789		
eva	1234567890		
kathrin	11111121		
hubertus	123123		

(A2)

- Ergänze die Tabelle für die weiteren Zeilen.
- Entscheide für welche Methode der Passwortspeicherung du dich entscheiden würdest. Begründe deine Entscheidung.
- Welche Eigenschaft würdest du dir von einer optimalen Prüfsumme wünschen? Erläutere, warum diese auf deiner Wunschliste stehen würde.

Bessere "Prüfsummen"-Methoden

Benutzername	Passwort	Methode 1	Methode 2	Methode 3
martin	12345	54321	34567	120
susi	123456	654321	345678	720

Benutzername	Passwort	Methode 1	Methode 2	Methode 3
franzi	1222334567	7654332221	3444556789	60480
karle	4534567	7654354	6756789	50400
eva	657703	307756	879923	4410
kathrin	11111121	12111111	33333343	2
hubertus	123123	321321	345345	36

(A3)

- Finde heraus, welche Methonden zur "Prüfsummenbildung" hier zum Einsatz kommen?
- Wenn du dich für eine dieser drei Methoden enstcheiden müsste - welche wäre dies? Begründe deine Wahl.

From:
https://info-bw.de/ -

Permanent link:
https://info-bw.de/faecher:informatik:oberstufe:kryptographie:hashfunktionen:start?rev=1645634109

Last update: **23.02.2022 16:35**