# L2\_2.4 Exkurs: Kennwort speichern

**Informationsmaterial:**

* Dokument „L2\_2.4 Exkurs: Kennwort speichern“

**Aufgabe:**

1. SHA-2 (von englisch *secure hash algorithm*, sicherer Hash-Algorithmus) ist der Oberbegriff für die kryptologischen Hashfunktionen SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 und SHA-512/256, die vom US-amerikanischen National Institute of Standards and Technology (NIST) als Nachfolger von SHA-1 standardisiert wurden. (Wikipedia, <https://de.wikipedia.org/wiki/SHA-2>).   
     
   Suchen Sie im Internet einen Dienst, welcher für einen Nachricht einen mittels **SHA-256** ermittelten Hashwert erzeugt. Bestimmen Sie den Hashwert für die Nachricht/das Kennwort „Hase“.   
     
   (z.B. https://hashgenerator.de/)
2. Besuchen Sie die Seite <https://crackstation.net/>. Geben Sie den Hashwert ein und interpretieren Sie das Ergebnis. Erläutern Sie, warum das Kennwort dennoch bestimmt werden kann.
3. Führen Sie die Schritte 1 und 2 erneut aus, ergänzen Sie die Nachricht/das Kennwort um einen Salt „X\_“. Interpretieren Sie das Ergebnis.
4. Ergänzen Sie die Tabelle „login“ um eine weitere Spalte namens „kennwort2“ vom Typ „varchar(256)“. Informieren Sie sich über die DB-Funktion „sha2(…)“ (<https://dev.mysql.com/doc/refman/8.0/en/encryption-functions.html#function_sha2>) und formulieren Sie eine SQL-Anweisung, welche die Hashwerte der unverschlüsselten Kennwörter in der neuen Spalte „kennwort2“ ablegt. Nutzen Sie eine Hashlänge von 256. Führen Sie die Anweisung aus und prüfen Sie das Ergebnis durch Sichtung der Datenbank.
5. Modifizieren Sie das Beispiel im Dokument „L2\_2.3 Daten lesen und auswerten mit PreparedStatements“ so, dass die Authentifizierung nun unter Verwendung des Hashwertes stattfindet.
6. **Für die Profis:** Ergänzen Sie die Tabelle „login“ um eine vierte Spalte namens „kennwort3“ vom Typ „varchar(256)“. Formulieren Sie eine SQL-Anweisung, welche die Hashwerte der unverschlüsselten Kennwörter in der neuen Spalte „kennwort3“ ablegt und dabei den „salt“ **X\_**  verwendet. Nutzen Sie eine Hashlänge von 256. Führen Sie die Anweisung aus und prüfen Sie das Ergebnis durch Sichtung der Datenbank. Modifizieren Sie die PHP-Seite so, dass die Authentifizierung über die Spalte „kennwort3“ erfolgt.