Hashfunktion und Hashwert

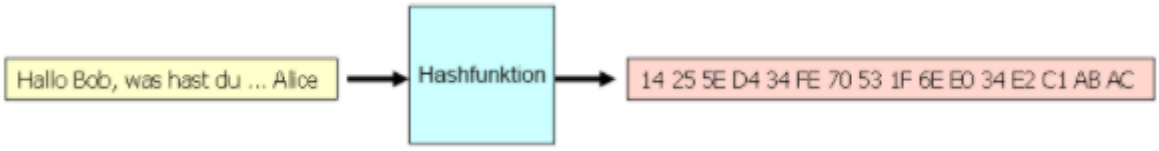
In der IT-Sicherheit ist oft die Rede von Hash-Werten und Hash-Funktionen. Diese spielen bei der Verschlüsselung eine wichtige Rolle. Aber grundsätzlich gilt: ein **Hash ist keine Verschlüsselung**, da die **Hash-Funktion nicht invertierbar** ist. Deshalb dürfen die Begriffe nicht miteinander verwechselt werden.

Begriffsbestimmung

Eine **Hash-Funktion (Algorithmus)** erzeugt aus einem Datensatz, das als Urbild bezeichnet wird, eine duale Zahl. Diese erstellte Zahl (Ergebnis), die meistens in hexadezimaler Schreibweise dargestellt wird, nennt man **Hash-Wert** bzw. **Hash**. Die Algorithmen (z.B. MDA, SHA usw.) der Hash-Funktionen sind immer gleich und fast alle sind „öffentlich“ verfügbar.

Funktionsweise und Anforderungen

Die Funktionsweise einer Hash-Funktion basiert auf einer **Einwegfunktion**, die sich **sehr einfach rechnen** lässt, aber deren **Umkehrung** (vom Hash zum Urbild) dagegen **unmöglich** ist.



Urbild **Hash bzw. Hashwert**

Anforderungen:

- Es sollte nicht möglich sein, den berechneten Hash-Wert wieder in den Ursprungswert zurückzurechnen (~~Reversibilität~~ Irreversibilität).
- Im Umkehrschluss sollte jedoch die Eingabe des gleichen Urbilds immer den gleichen Hash-Wert ergeben (Eindeutigkeit).
- Außerdem soll verhindert werden, dass unterschiedliche Urbilder den gleichen Hash-Wert erzeugen (Kollisionsresistenz).

Anwendungsgebiete

Hashfunktionen werden häufig verwendet, um sensible Daten zu schützen. So sind zum Beispiel die Passwörter für den Zugang zu Systemen / Anwendungen standardmäßig nur als Hashwert und nicht im Klartext in der Passwortdatei gespeichert. Dabei handelt es sich aber nicht um eine Verschlüsselung, denn beim Passworthash ist das Zurückrechnen nicht gewollt und auch nicht notwendig. Die korrekte Passworteingabe kann einfach durch den Vergleich des daraus berechneten mit dem gespeicherten Hashwert verifiziert werden. Weitere Anwendungsgebiete sind die digitale Signatur sowie die Prüfsummen (elektronischer Fingerabdruck).

Fragen zum Informationstext

Beschreiben Sie den Unterschied zwischen Hash-Funktion und Hash-Wert!

Hash-Funktion ist ein Algorithmus die aus einer Datei einen Hash-Wert erzeugt, der nicht zurück konvertiert werden kann

Erläutern Sie warum das Erzeugen eines Hash keine Verschlüsselung ist?

Weil es nicht möglich ist diesen Wert wieder zu entschlüsseln

Nennen Sie drei Anforderungen an die Hash-Funktion?

Irreversibilität

Eindeutigkeit

Kollisionsresistenz

In welchen Anwendungsfeldern werden Hashfunktionen angwendet?

Daten schützen, Passwörter, Integritätsprüfungen