

BEGRIFFSDEFINITIONEN

HASHING, ENCODING, ENCRYPTION

Hashalgorithmen (Hashing):

Der Begriff Hashing (Deutsch: zerhacken) bezeichnet die Transformation eines beliebig großen Datensatzes in eine Zeichenkette mit einer festen, kürzeren Länge, die den ursprünglichen Datensatz referenziert. Mittels einer Hashfunktion werden die einzelnen Elemente aus dem Datensatz zunächst einem Schlüssel und dann den Hashwerten zugeordnet, die die originalen Daten auf bestimmte Weise repräsentieren. Der Datensatz kann aus Zeichenfolgen, Listen, Dateien oder anderen Inhalten bestehen; die Schlüssel, die für diese Daten stehen, geben die Position der Elemente im Datensatz an, die mit ihnen durch Hashwerte verknüpft werden. Die Hashfunktion bildet die Elemente des Datensatzes über einen Schlüssel ab und erzeugt Hashwerte. Beim Hashing werden die Daten in kleine Teile zerlegt und in einer Datenstruktur geordnet. Die Hashwerte erlauben es in Datenbanken beispielsweise, bestimmte Elemente weitaus schneller zu finden, weil nur die Datenstruktur, nicht der gesamte Datensatz durchsucht werden muss. Möchte man einzelne Daten finden oder verändern, muss nur die Struktur durchsucht werden – die eigentlichen Daten müssen nicht rekonstruiert werden.

Quelle: <https://bit.ly/38EzB2W>

Kodierung (Encoding):

Bezeichnet eine Transformation, die nicht geheim ist und daher von jedem rückgängig gemacht werden kann. Der Code, den die meisten Computer für Text-Dateien verwenden, ist unter der Bezeichnung ASCII (American Standard Code for Information Interchange) bekannt. ASCII kann alphabetische Zeichen, Ziffern, Satzzeichen und allgemeine Symbole in Groß- und Kleinschreibung darstellen. Andere häufig verwendete Codes sind Unicode, BinHex, Uuencode und MIME. Dabei repräsentieren Binärzahlen (Bits) die Übergänge zwischen hohen und niedrigen logischen Zuständen. In der Webentwicklung beispielsweise gibt es eine Vielzahl von Codierungs- und Decodierungsmethoden. Der älteste von allen bekannten Codes ist der Morse-Code. Die Begriffe Codierung und Decodierung werden häufig für den Prozess der Konvertierung von analog zu digital und umgekehrt verwendet. Codierung sollte dabei nicht mit Verschlüsselung verwechselt werden. Letztere ist ein Prozess, bei dem Daten bewusst verändert werden, um ihren Inhalt zu verbergen. Eine Verschlüsselung kann erfolgen, ohne dass der jeweilige Code, in dem der jeweilige Inhalt vorliegt, geändert wird. Eine Codierung wiederum ist möglich, ohne damit bewusst den Inhalt zu verschleiern.

Quelle: <https://bit.ly/2V1ZRAR>

Verschlüsselung (Encryption):

Ist eine Transformation, die von einem geheimen Schlüssel abhängt und daher nur von bestimmten Zielpersonen rückgängig gemacht werden kann, die im Besitz des Schlüssels sind. Verschlüsselung bedeutet, dass Daten mittels elektronischer bzw. digitaler Codes oder Schlüssel inhaltlich in unlesbare Formen übersetzt werden. Für die Rücktransformation ist ein ganz bestimmter Schlüssel in Form eines Verfahrens oder eines Algorithmus erforderlich. Erst dann stehen dem legitimierten Nutzer die ursprünglichen Daten wieder vollumfänglich zur Verfügung. Diese Schlüssel sind mit einem Geheimcode vergleichbar, mit dessen Hilfe ein Klartext in eine unlesbare Chiffre überführt wird. Wer diesen Schlüssel besitzt, ist in der Lage, den umgekehrten Weg zu gehen, also von der Chiffre zum ursprünglichen Klartext. Man spricht in diesem Zusammenhang auch von Chiffrierung und Dechiffrierung. Dabei kommen klassische und moderne, symmetrische und asymmetrische Verschlüsselungsverfahren zur Anwendung.

Quelle: <https://bit.ly/32730QT>