Kryptographische Prüfsummen mit Betriebssystem-Bordmitteln bilden

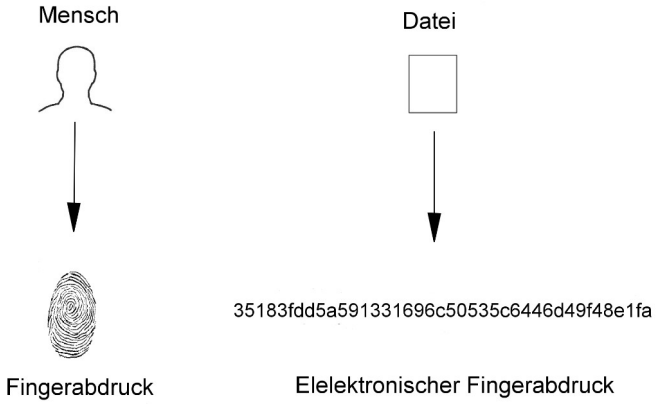
Für MS-Windows, MacOS, GNU/Linux und BSD/Unix

Menschen sind komplexe Lebewesen. Für ihre schnelle und unkomplizierte Identifizierung werden oftmals Fingerabdrücke erstellt. Nach demselben Prinzip können Computerdateien identifiziert werden: Durch Erzeugung eines "elektronischen Fingerabdrucks", der so genannten kryptographischen Prüfsumme, einer stets gleichbleibenden Zahl. Mittels standardisierter Verfahren kann so eine schnelle Integritäts- und Echtheitskontrolle von Dateien jedweder Art vorgenommen werden. Menschliche Fingerabdrücke werden mit Stempelkissen erstellt, elektronische mit einem Prüfsummenprogramm.

Kryptographische Prüfsummen basieren auf Streuwert- bzw. Hashfunktionen, die zu einer beliebigen Datei Streu- bzw. Hashwerte als Ergebnis liefern. Dieser Wert wird auch Hashcode bzw. Hash genannt.

Eine Datei sowie identische Kopien von ihr weist stets dieselbe Hashwert-Prüfsumme auf. Ändert sich jedoch auch nur ein einziges Bit oder Zeichen durch Beschädigung oder Manipulation, sollte ein gänzlich anderer Hashcode entstehen.

Das Ändern des Dateinamens ändert nicht die kryptographische Prüfsumme.



MS-Windows: PowerShell

Ausprobierbeispiel: Plazieren Sie auf Ihrem Desktop ein beliebiges Dateidokument, beispielsweise eine Bilddatei oder ein Textdokument wie z.B. Brief.txt. Geben Sie unten links im Windows-Suchfeld ein: *PowerShell*. Klicken Sie auf den ersten erscheinenden Eintrag, auf "Windows PowerShell App" Es öffnet sich das bordeigene Befehlszeilenfenster. 1. Schreiben Sie, hier immer ohne Anführungszeichen, "*cd Desktop*" und drücken die Eingabetaste (Returntaste). 2. Schreiben Sie nun "*ls*" und drücken die Eingabetaste, woraufhin alle Ihre Ordner und Dateien aufgelistet werden, die sich im Verzeichnis "Desktop" befinden, darunter auch Ihre Beispieldatei. 3. Jetzt bilden Sie die Prüfsumme zu Ihrer Datei, mit dem Befehl *Get-FileHash [Dateiname]*, hier im Beispiel: *Get-FileHash Brief.txt*. Es erscheinen der voreingestellt verwendete Algorithmus, die kryptographische Prüfsumme sowie der Dateipfad.

```
PS C:\Users\chef\Desktop> Get-FileHash Brief.txt
```

GNU/Linux und BSD/Unix sowie MacOS: Shasum

Unter unixartigen Betriebssystemen öffnen Sie ebenfalls eine Befehlszeilenumgebung und verwenden eines der fast immer schon vorinstallierten shasum-Programme, beispielsweise sha256, sha256sum oder sha512 bzw. sha512sum u.a. Beispiel: sha256sum gefolgt vom Dateinamen: *sha256sum Brief.txt*.

Impressum

Peter Jockisch, Habsburgerstraße 11, D-79104 Freiburg. Stand der Kurzartikelversion: 10. Januar 2021. Ausführlicher Originalartikel, "Praktische Anwendung kryptographischer Prüfsummen" erhältlich unter www.peterjockisch.de bzw. unter www.study-of-languages-with-computer-and-internet.com.