Passwörter

Zum Schutz vor unbefugtem Betreten eines Gebäudes oder eines Raumes gibt es Schlösser und Schlüssel, zum Schutz vor unbefugter Benutzung eines elektronischen Gerätes werden häufig Passwörter benutzt.

Ein Schloß "kennt" die passenden Schlüssel, durch eine genaue Untersuchung eines Schlosses könnte man einen passenden Schlüssel anfertigen.

Ist das bei passwortgeschützten Geräten ähnlich? Kann z.B. Beispiel jemand, der vollständigen Zugriff auf den Schulserver hat, die Passwörter aller Benutzer auslesen?

Einwegcodierung

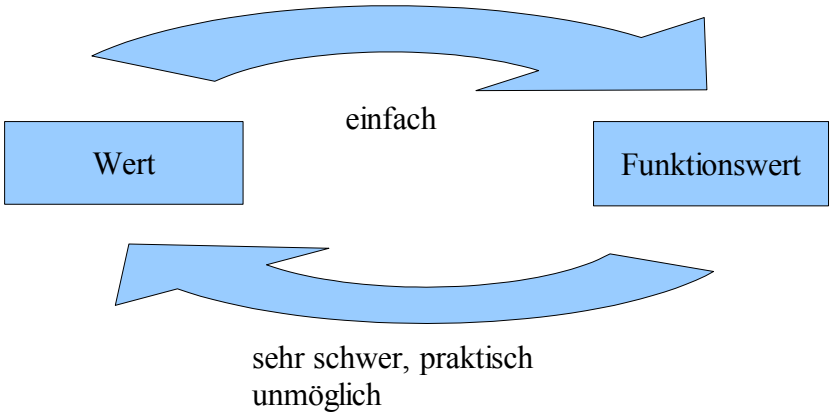
Es gibt Vorgänge, die einfach zu realisieren sind, z.B. einen Tropfen Tinte in einem Glas Wasser aufzulösen. Aber es gibt auch sehr schwierige Vorgänge, z.B. die Tintenmoleküle wieder von den Wassermolekülen zu trennen.

Erfreulicherweise gibt es ähnliche Effekte auch in der Mathematik!

Es ist recht einfach $x^4+x^3+x^2+x$ zu berechnen, wenn x = 7 ist. Man erhält 2794.

Aber es ist relativ schwer, auszurechnen, für welches x gilt: $x^4+x^3+x^2+x=16104$

Einwegfunktonen



Zweck von Einwegfunktionen

Angenommen wir hätten eine Einwegfunktion für Passwörter. Nun wird auf dem Schulserver nicht mehr mein Passwort im Klartext gespeichert, sondern nur der Funktionswert des Passwortes.

Anmelden:
1. Ich gebe meinen Benutzernamen und mein Passwort im Klartext ein.
2. Aus dem Passwort wird der Funktionswert mit Hilfe der Einwegfunktion berechnet.
3. In der Benutzerliste wird geprüft, ob zu meinem Benutzernamen auch genau dieser Funktionswert gespeichert ist. Nur bei Übereinstimmung ist die Anmeldung erfolgreich.

Schutz:
Jemand, der meinen Benutzernamen und den Funktionswert meines Passwortes kennt (z.B. von der Festplatte ausliest), kann sich dennoch nicht unter meinem Namen anmelden! Er kann aus dem Funktionswert nicht mein Passwort rekonstruieren.