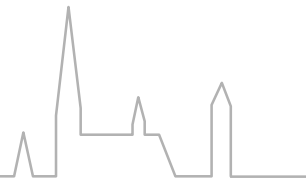


Einwegfunktion



Funktion $f(x)$

x gegeben, $f(x)$ einfach zu berechnen
 $f(x)$ gegeben, x schwer zu berechnen

- Mathematisch kein Beweis für Existenz von Einwegfunktionen
- Kein Hinweis auf Konstruierbarkeit

Beispiele

- x^2 einfach zu berechnen, $x^{1/2}$ nicht
- Keramik
- Vorhängeschloss
- Schokolade





Caesar Cipher

- Zeichen ersetzen durch x . Zeichen nach rechts, modulo 26.
- Z.B. $x=3$: $a \Rightarrow d$; $f \Rightarrow h$; $x \Rightarrow a$
- Spezialfall: $x=13$. ROT13
- $P = \text{ROT13}(\text{ROT13}(P))$

Demos im Web: <http://codebrkr.infopages.net/fcodes.htm>



Symmetrisch, asymmetrisch



Symmetrisch (Kiste mit Schloss)

- gleicher Schlüssel für Ver- und Entschlüsselung
- hohe Geschwindigkeit
- Bekannter Algorithmus: DES

Asymmetrisch (Kiste mit offenem Vorhängeschloss, Wahlurne)

- getrennte Schlüssel für Ver- und Entschlüsselung
- Anwendung für digitale Signatur
- geringe Geschwindigkeit \Rightarrow hybride Verfahren
- Bekannter Algorithmus: RSA

AOF-Demos: <http://www.viror.de/viror.lehrangebot.19990200-jendricke-krypto>

