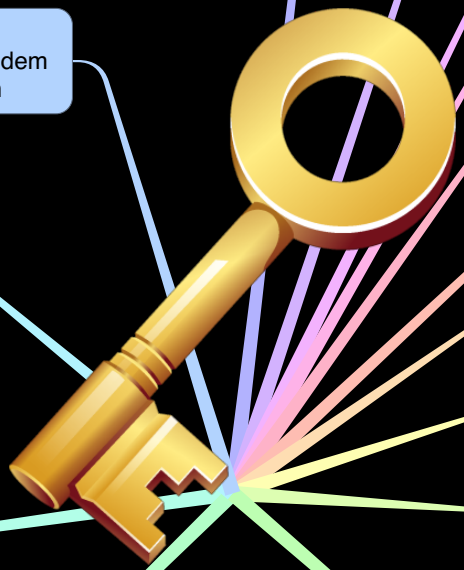
Secure Hash Algorithm



SHA

sicherer Hash-Algorithmus

National Institute of Standards and Technogy (NIST)

zur Berechnung eines Prüfwerts für beliebige digitale Daten (Nachrichten)

Kollisionsresistenz

praktisch unmöglich, zwei verschiedene Nachrichten mit dem gleichen Prüfwert zu erzeugen

Blockverschlüsselung

Blockchiffre — ***block cipher***

ist ein deterministisches Verschlüsselungsverfahren, das einen Klartextblock, d. h. einen Klartextabschnitt fester Länge, auf einen Geheimtext- oder Schlüsseltextblock fester (in der Regel der gleichen) Länge abbildet

Grundlage zur Erstellung einer digitalen Signatur

SHA ist widerstandsfähig gegen Brute-Force-Angriffe zum Auffinden von Kollisionen

standardisierter kryptologischer Hashfunktionen

wird verwendet, um die Integrität einer Nachricht zu sichern

SHA-1 gebrochen

SHA-2

SHA-224, SHA-256, SHA-384 und SHA-512

SHA-512/256 und SHA-512/224

NSA

SHA-3

called *Keccak*

SHA3-224

SHA3-256

SHA3-384

SHA3-512

SHAKE128

SHAKE256

non-NSA designers