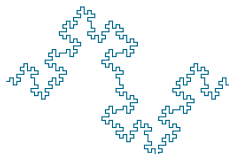


Secure Hash Algorithm

SHA-256

Chi Trung Nguyen
T-Systems



6. Juni 2012

INHALT

EINFÜHRUNG

Was ist ein Hash?

GESCHICHTE

SHA

SHA-0

SHA-1

SHA-2

eig

IMPLEMENTIERUNG

Algorithmus

Pseudocode

ANWENDUNG

Verwendungszweck

Sicherheitslücken

AUSBLICK

SHA-3

WAS IST EIN HASH?

- ▶ deutsch: „zerhacken“, „verstreuen“

WAS IST EIN HASH?

- ▶ deutsch: „zerhacken“, „verstreuen“
- ▶ Hashfunktion oder Streuwertfunktion erstellt aus beliebiger großer Quellmenge eine immer gleich große Zielmenge
 - ▶ $f(x) = f(x')$

WAS IST EIN HASH?

- ▶ deutsch: „zerhacken“, „verstreuen“
- ▶ Hashfunktion oder Streuwertfunktion erstellt aus beliebiger großer Quellmenge eine immer gleich große Zielmenge
 - ▶ $f(x) = f(x')$
- ▶ Item C

SHA ALLGEMEIN

- ▶ Gruppe von kryptologischer Hashfunktionen
- ▶ 1993 vom **National Institute of Standards(NIST)** als ein **U.S. Federal Information Processing Standard (FIPS)** veröffentlicht

SHA ALLGEMEIN

- ▶ Gruppe von kryptologischer Hashfunktionen
- ▶ 1993 vom **National Institute of Standards(NIST)** als ein **U.S. Federal Information Processing Standard (FIPS)** veröffentlicht
 - ▶ Subitem 1
 - ▶ Subtem 2
- ▶ Item C

SHA-0

► Item A

SHA-0

- ▶ Item A
- ▶ Item B
 - ▶ Subitem 1
 - ▶ Subtem 2
- ▶ Item C

SHA-1

SHA-2

EIG

Tabelle : Secure Hash Algorithmus Eigenschaften

| Algorithmus | Message Size(bits) | Block Size(bits) | Word Size(bits) | Message Digest Size(bits) |
|-------------|--------------------|------------------|-----------------|---------------------------|
| SHA-1 | $< 2^{64}$ | 512 | 32 | 160 |
| SHA-224 | $< 2^{64}$ | 512 | 32 | 224 |
| SHA-256 | $< 2^{64}$ | 512 | 32 | 256 |
| SHA-384 | $< 2^{128}$ | 1024 | 64 | 384 |
| SHA-512 | $< 2^{128}$ | 1024 | 64 | 512 |

FUNKTIONEN

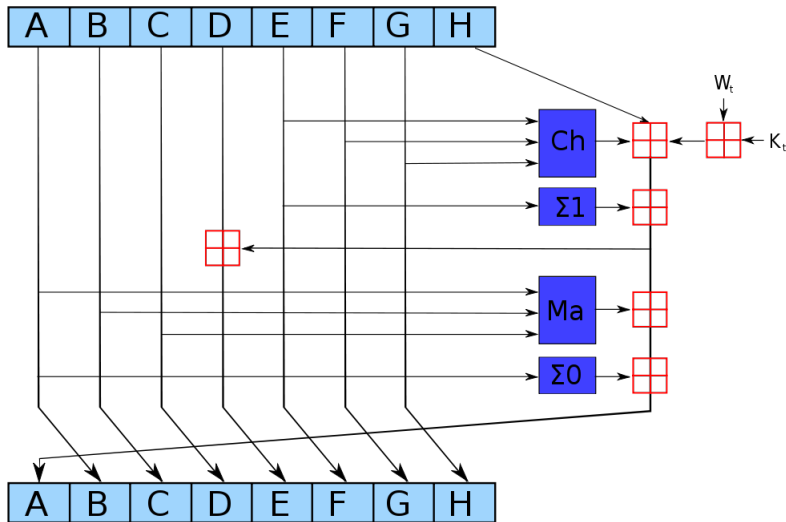
$$Ch(E, F, G) = (E \wedge F) \oplus (\neg E \wedge G)$$

$$Ma(A, B, C) = (A \wedge B) \oplus (A \wedge C) \oplus (B \wedge C)$$

$$\Sigma_0 = (A \ggg 2) \oplus (A \ggg 13) \oplus (A \ggg 22)$$

$$\Sigma_1 = (A \ggg 6) \oplus (A \ggg 11) \oplus (A \ggg 25)$$

DARSTELLUNG DES ALGORITHMUS



PSEUDOCODE

VERWENDUNGSZWECK

SICHERHEITSLÜCKEN

SHA-3