Datenschutz - weitere kryptografische Verfahren

Prüfsumme:

- Daten können mit Prüfsummen überprüft oder fälschungssicher als Signatur übertragen werden.
- bekannte Verfahren: md5, sha, Quersumme
- einfaches Beispiel: (Quersumme der Textzeichen, a=1, b=2 usw. Großbuchstaben + 26)

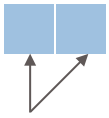
Hallo $\hat{=}$ 34 + 1 + 12 +12 + 15 = 74

Der Text „Hallo“ wird mit der Prüfsumme „74“ übertragen, der Empfänger kann dann überprüfen ob die Übertragung fehlerfrei war.

Steganographie

- (unverschlüsselte) Daten werden unauffällig zum Empfänger transportiert. Z.B. In digitalen Bilddaten im jeweils letzten Bit eines Bildpunktes versteckt. (Strickmuster mit Bedeutung, tätowierte Kopfhaut usw.)
- Problem: Das Verfahren muss geheim gehalten werden!
- Beispiel: Verstecken der Daten 101011… in einem Bild.

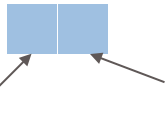
Bildpixel vorher



9FC1E0

9[1111]C[0001]E[0000]

Bildpixel nachher



9EC1E1

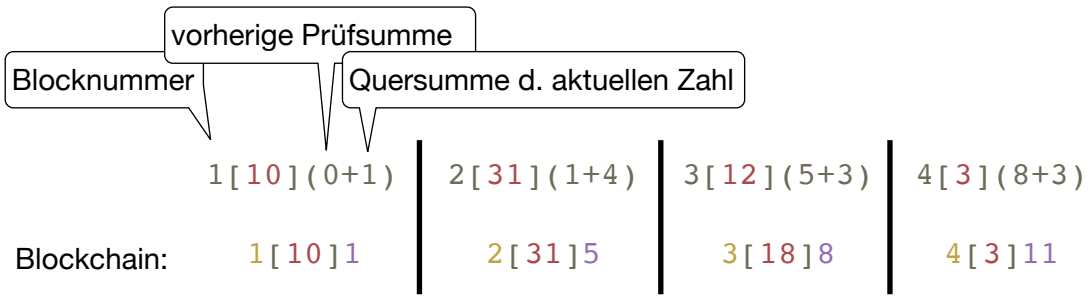
9[1110]C[0001]E[0001]

9FC0E1

9[1111]C[0001]E[0000]

Blockchain

- kontinuierlich erweiterbare Kette von kryptografisch gesicherten Datensätzen, die nachträglich nicht geändert werden kann.
- einfaches Beispiel: Übertragung von mehreren ■ Blöcken mit ■ Zahlen und deren Absicherung über ■ Prüfsummen



Übungen:

Probiere doch einmal das Steganigraphie-Programm StegoShare als Java-Programm auf Windows, Mac und Linux lauffähig.

http://stegoshare.sourceforge.net/download.html

oder Pictograph für iOS