SHA

Rubrik: IT-Sicherheit

SHA steht für Secure Hash Algorithm und bezeichnet eine Familie kryptografischer Hashfunktionen.

SHA steht für Secure Hash Algorithm und bezeichnet eine Familie kryptografischer Hashfunktionen. Sie berechnen aus Daten Prüfsummen fester Länge, ohne die ursprünglichen Daten zu verschlüsseln. Zur Familie gehören unter anderem SHA-1, SHA-2 und SHA-3. Für neue sicherheitsrelevante Anwendungen sollten zeitgemäße Varianten statt des veralteten SHA-1 verwendet werden.