

Kryptosysteme, Keymanagement (KSK3) für CMS
7. Übungsblatt für den 28. November 2006

24. Berechne (mit Hilfe einer speziellen Software) den SHA-1 Hashwert der Zeichenkette „Hallo“.
25. (*Recherche*) Welche Hash-Algorithmen sind im aktuellsten *Secure Hash Standard* spezifiziert? Worin unterschieden sich die verschiedenen Algorithmen?
26. (*Recherche*) In welchen Bereichen wird/wurde die MD5 Hashfunktion verwendet? Warum sollte man diese Funktion nicht mehr verwenden?