Linux-Übung: Kryptologie

1 Hash-Funktionen

- Welche Hash-Funktionen gibt es unter Linux?
- Erstellen Sie Hash-Werte von Textdateien mit verschiedenen Hash-Funktionen und vergleichen Sie diese.
- Erstellen Sie Hash-Werte einer leeren Textdatei mit verschiedenen Hash-Funktionen und vergleichen Sie diese mit den Angaben in Wikipedia.

2 Symmetrische Verschlüsselung

- Welche Linux-Software kann symmetrisch ver- und entschlüsseln?
- Verschlüsseln Sie eine Textdatei.
- Löschen Sie das Original.
- Entschlüsseln Sie die Datei wieder.

3 Asymmetrische Verschlüsselung

- Welche Linux-Software kann asymmetrisch ver- und entschlüsseln?
- Erstellen Sie einen Private-Key.
- Erstellen Sie aus dem Private-Key den zugehörigen Public-Key.
- Schauen Sie sich die Schlüssel mit einem Textviewer an.
- Verschlüsseln Sie eine Datei mit dem Public-Key.
- Entschlüsseln Sie die Datei wieder mit dem Private-Key.

4 Signatur eines Dokuments

- Erstellen Sie eine Textdatei.
- Erstellen Sie eine Signatur der Datei mit einer Hashfunktion und Ihrem Private-Key.
- Verifizieren Sie die Integrität und Authentizität der Datei mit dem Public-Key.