



Modulidentifikation

Modulnummer	114
Titel	Codierungs-, Kompressions- und Verschlüsselungsverfahren einsetzen

Kompetenz	Codierungs-, Kompressions- und Verschlüsselungsverfahren einsetzen
-----------	--

Handlungsziele

- 1 Codierungen von Daten situationsbezogen auswählen und einsetzen. Aufzeigen, welche Auswirkung die Codierung auf die Darstellung von Daten hat.
- 2 Kompressionsverfahren gemäss Vorgaben für die Aufbewahrung, Wiederherstellung und Übertragung von Daten auswählen und einsetzen.
- 3 Verschlüsselungsverfahren zur Sicherung von Daten gemäss Vorgaben gegen unbefugten Zugriff auf Datenspeicher und Übertragungswegen auswählen und einsetzen.
- 4 Gesicherte Übertragungsverfahren für Dateien mit asymmetrischen und symmetrischen Verschlüsselungsverfahren nutzen. Dabei Aspekte wie Public/Private Key, Zertifikate, Protokolle und Standards berücksichtigen.

Kompetenzfeld	IT Sicherheit
Objekt	Zu speichernde und zu übertragende Daten.
Niveau	2
Voraussetzungen	keine
Anzahl Lektionen	40
Anerkennung	Eidg. Fähigkeitszeugnis

Modulversion	3.00
--------------	------



Handlungsnotwendige Kenntnisse

Modulnummer	114
Titel	Codierungs-, Kompressions- und Verschlüsselungsverfahren einsetzen

Kompetenz	Codierungs-, Kompressions- und Verschlüsselungsverfahren einsetzen
-----------	--

Handlungsnotwendige Kenntnisse

- 1.1 Kennt die wichtigsten Typen von Binärcodes (z.B. ASCII, ANSI-, BCD-, EAN-, 1-aus -n-, UTF, Uni-Code) und kann anhand ihrer Merkmale (Zeichenvorrat, Redundanz) aufzeigen, wie sich diese hinsichtlich der Bewertbarkeit, Fehlererkennbarkeit und Rechenfähigkeit unterscheiden.
- 1.2 Kennt die wichtigsten Eigenschaften von Bildern (S/W-Strichzeichnung, Farbfoto, bewegte/nicht bewegte Bilder, vektorisiert/pixelorientiert usw.) und kann erläutern, wie damit die Bildqualität (Auflösung, Farbtiefe), der Bildaufbau und der Speicherbedarf beeinflusst werden kann.
- 1.3 Kennt binäre, oktale und hexadezimale Zahlensysteme. Kennt logische Operationen (OR, AND, NOT) und kennt die Verfahren zur Umrechnung in das jeweils andere Zahlensystem.
- 1.4 Kennt Verfahren zur binären Kodierung von Zahlen (z.B. negative Zahlen/Zweierkomplement, Gleitkommazahlen).
- 1.5 Kennt Verfahren zur Repräsentation von Farben (z.B. RGB, CMYK).
- 2.1 Kennt Merkmale (Kompressionsrate, Qualitätsverlust) für gängige verlustlose und verlustbehaftete Kompressionsverfahren.
- 2.2 Kennt ausgewählte Normen und Standards (z.B. JPEG, PNG, MPEG, H261/263, Huffman-Verfahren) und kennt typische Anwendungsbereiche wo diese eingesetzt werden.
- 3.1 Kennt das grundsätzliche Prinzip der Verschlüsselung von Informationen (Kryptografie/Steganografie) und kann anhand eines einfachen Verschlüsselungskonzepts aufzeigen, wie damit Informationen chiffriert und dechiffriert werden können.
- 4.1 Kennt die prinzipiellen Unterschiede zwischen einer symmetrischen und asymmetrischen Verschlüsselung (Passwörter, private und öffentliche Schlüssel) und kann erläutern, wie sich diese auf den Grad der Datensicherheit auswirken.
- 4.2 Kennt das Prinzip elektronischer Signatursysteme und kann anhand von Beispielen aufzeigen, wie damit die Sicherheit (Authentizität, Integrität) der Übermittlung gewährleistet werden kann.



- 4.3 Kennt den Zweck digitaler Zertifikate und kann an Beispielen erläutern, wie damit das Vertrauen zwischen Anbieter und Bezüger (einer Leistung, eines Produktes) sichergestellt werden kann.

Kompetenzfeld	IT Sicherheit
Objekt	Zu speichernde und zu übertragende Daten.
Niveau	2
Voraussetzungen	keine
Anzahl Lektionen	40
Anerkennung	Eidg. Fähigkeitszeugnis

Modulversion	3.00
--------------	------