Fragen, Aufgaben im Fragenkatalog notiert.
Peter Rutschmann authored 1 year ago

Name	Last commit	Last update
..		
x_gitressourcen	rename ress folder	2 years ago
Fragenkatalog.md	Fragen, Aufgaben im Fragenkatalog notiert.	1 year ago
README.md	Fixed lasst typos according validation.	1 year ago

README.md

Kompetenzmatrix - Modul 114

Handlungsziele und typische Handlungssituationen

1. Codierungen von Daten situationsbezogen auswählen und einsetzen. Aufzeigen, welche Auswirkung die Codierung auf die Darstellung von Daten hat.

Hans Muster erhält eine Datei, in der einzelne Zeichen nicht korrekt dargestellt sind. Er erkennt als Ursache Probleme bei der Codierung der Zeichen. Er korrigiert die Codierung der Daten in der Datei oder die Interpretation durch die darstellende Applikation.

Auf einer Einladung zu einem Firmenevent müssen zusätzliche Information (z. B. Ort, Datum, Zeit, Webseite, Sitzplatz) in einer maschinenlesbaren Form codiert werden. Hans Muster stellt die Daten zusammen, kreiert eine Codierung und wählt einen geeigneten Barcode, um die Codierung in eine maschinenlesbare Form zu bringen. (Hanok 1.1)

In einer Berechnung in seinem Programm erhält Hans Muster unterwartet ein negatives Ergebnis auf Grund eines Werteüberlaufes. Hans Muster untersucht das Problem und setzt sich dabei mit der Codierung von Zahlen, den sich daraus ergebenden Wertebereichen auseinander. Er wählt einen anderen Datentyp und kann so das Problem lösen. (Hanok 1.4)

2. Kompressionsverfahren gemäss Vorgaben für die Aufbewahrung, Wiederherstellung und Übertragung von Daten auswählen und einsetzen.

In eine neue Webseite sollen Multimediainhalte eingebunden werden. Das Problem dabei sind die recht grossen Datenmengen und die damit verbundenen Ladezeiten, wenn die Seite angezeigt wird. Hans Muster muss die Multimediainhalte (Bilder, Video, Audio) für die Webseite in Bezug auf die Speichergrösse und Qualität optimieren. Er wählt gezielt ein geeignetes verlustbehaftetes oder verlustfreies Kompressionsverfahren aus und wendet es an.

3. Verschlüsselungsverfahren zur Sicherung von Daten gemäss Vorgaben gegen unbefugten Zugriff auf Datenspeicher und Übertragungswegen auswählen und einsetzen.

Für eine Kunden muss Hans Muster Dateien auf einem externen Speichermedium zusammenstellen. Er macht sich Gedanken, wie er die Daten vor fremden Zugriffen zu schützen kann. Hans Muster entschliesst sich die Daten zu verschlüsseln. Er wählt ein geeignetes Verschlüsselungsfahren aus und wendet es auf die Daten an. Die notwendigen Informationen für die Entschlüsselung sendet Hans Muster getrennt vom Speichermedium dem Kunden zu.

4. Gesicherte Übertragungsverfahren für Dateien mit asymmetrischen und symmetrischen Verschlüsselungsverfahren nutzen. Dabei Aspekte wie Public/Private Key, Zertifikate, Protokolle und Standards berücksichtigen.

Die Firma von Hans Muster will Ihren E-Mail-Verkehr sicherer machen. Hans Muster setzt sich mit dem Unterschied von Signieren und Verschlüsseln auseinander. Er weiss nun, dass dankt dem Signieren Veränderungen von Dritter erkannt werden können. Und dass mit Hilfe einer Verschlüsselung Fremden das Lesen von E-Mails verunmöglicht wird. Er konfiguriert sein E-Mail Programm um E-Mail wahlweise signieren und verschlüsseln zu können. Um den Datenaustausch (z. B. E-Mail-Verkehr) abzusichern, wendet Hans Muster das Signieren und Verschlüsseln der Daten nun konsequent an.

Nun wendet sich Hans Muster der Absicherung der Übertragung von Daten zwischen dem Webserver seiner Firma zu den Clients der Kunden auseinander. Er analysiert den Unterschied zwischen HTTP und HTTPS, setzt sich mit Zertifikaten und mit dem Schlüsselaustausch via Diffie-Hellman auseinander.

5. Verschiedene Verschlüsselungstechnologien hinsichtlich Aktualität, Verbreitung und Sicherheit bewerten. Schwachstellen erkennen und Vorschläge für alternative Technologien machen.

Die Fima von Hans Muster setzt seit Jahren ein schon etwas in die Jahre gekommenes Verschlüsselungsprogramm ein, mit dem sensitive Daten verschlüsselt werden. Ist dieses Verfahren noch sicher? Gibt es neuere Verfahren? Was sind die aktuellen Empfehlungen? Hans Muster vergleicht und bewertet verschiedene Verschlüsselungstechnologien und macht einen Vorschlag, welche aktuelle Verschlüsselung eingesetzt werden soll.

Matrix

Kompetenzband:	HZ	Grundlagen	Fortgeschritten	Erweitert
Daten codieren	1	A1G: Ich kann die binäre Interpretation einer Codierung erklären (z. B. Zahlen, Text)	A1F: Ich kann eine Codierung unter Berücksichtigung verschiedener, aufgabenbezogener Faktoren auswählen. (z. B. Zeichenvorrat, Wertebereich, Berechenbarkeit)	A1E: Ich kann eine Codierung in andere transformieren (z. B. Text <--> Zahl)
	1	A1G: Ich kann Unterschiede von Bildformaten (Raster- und Vektorgrafik sowie z. B. JPG, GIF, PNG, SVG) und Farbcodierungen (z.B. RGB, CMYK, YCrCb) erläutern.	A2F: Ich kann unterschiedliche Bildformate passend für den Einsatz des Bildes anwenden und parametrisieren. (z. B. für Logo, Galerien, Thumbnails in Bezug auf Speicherplatz, Transparenz, Skalierbarkeit, Komprimierung ...)	A2E: Ich kann das Format eines Bildes in Bezug auf seine spezifische Anwendung wandeln.
	1	A3G: Ich kann eine zusammengesetzte Codierung erklären. (z. B. alte AHV Nummer, IBAN, EAN)	A3F: Ich kann eine zusammengesetzte Codierung umsetzen. (z. B. Sitzplatz in Stadion)	A3E: Ich kann eine zusammengesetzte Codierung kritisch hinterfragen (z. B. Eindeutigkeit, Auswertbarkeit) und Verbesserungen vorschlagen.
Daten komprimieren	2	B1G: Ich kenne den Unterschied (Vorteile/Nachteile) zwischen verlustloser und verlustbehafteter Komprimierung und kann die typischen Einsatzgebiete erläutern.	B1F: Ich kann ein gängiges, verlustloses Kompressionsverfahren wie z.B. VLC/Huffman, RLC, BWT, LZW und ein gängiges, verlustbehaftetes Kompressionsverfahren wie z. B. DCT bei JPG anwenden.	B1E: Ich kann - abhängig vom zu komprimierenden Medium - ein geeignetes Verfahren begründet auswählen.
Daten verschlüsseln	3	C1G: Ich kann den Zweck und das Prinzip der Verschlüsselung (chiffrieren und dechiffrieren) erklären.	C1F: Ich kann Daten mit Hilfe einer Software verschlüsseln (chiffrieren und dechiffrieren) .	C1E: Ich kann verschiedene Verschlüsselungs-verfahren analysieren und vergleichen. (Vor- , Nachteile)
gesicherte Übertragungen	4	D1G: Ich kann den Zweck und das Prinzip der gesicherten Datenübertragung erklären. (z. B. Public/Private Key, Zertifikate, Protokolle und Standards)	D1F: Ich kann Daten gesichert übertragen (Senden und Empfangen) (z. B. Email).	D1E: Ich kann Verfahren für eine gesicherte Datenübertragung vergleichen und begründet auswählen.
Verschlüsselungs-technologien bewerten	5	E1G: Ich kann verschiedene Verschlüsselungs-technologien unterscheiden.	E1F: Ich kann Unterschiede der verschiedenen Verschlüsselungstechnologien aufzeigen.	E1E: Ich kann Schwachstellen von Verschlüsselungs-technologien erkennen und Alternativen vorschlagen.

Kompetenzstufen

Grundlagen | Stufe 1

Diese Stufe ist als Einstieg ins Thema gedacht. Der Fokus liegt hier auf dem Verstehen von Begriffen und Zusammenhängen.

Als Richtungshinweis: Wer alle Kompetenzen in dieser Stufe erfüllt, hat die Noten 3.0.

Fortgeschritten | Stufe 2

Diese Stufe definiert den Pflichtstoff, den alle Lernenden am Ende des Moduls möglichst beherrschen sollen.

Als Richtungshinweis: Wer alle Kompetenzen in dieser Stufe erfüllt, hat die Noten 4.5

Erweitert | Stufe 3

Diese Lerninhalte für Lernende gedacht, die schneller vorankommen und einen zusätzlichen Lernanreiz erhalten sollen.

Als Richtungshinweis: Wer alle Kompetenzen in dieser Stufe erfüllt, hat die Noten 6

Fragekatalog

Link zum Fragekatalog