Modul 114: Codierungs-, Kompressions- und Verschlüsselungsverfahren einsetzen (IN20_24)

Quick links Deutsch (de)

Modul 114: Codierungs-, Kompressions- und Verschlüsselungsverfahren einsetzen

Semesterplan IN20-24 abc M114 (neu wegen Verschieb. auf Do)

Modulidentifikation M114

LBV M114-6 BZTF

8. Februar - 14. Februar

Heute:
- Modul kennenlernen, LBV, Termine
- Vorwissen-Brainstorming
- Lernen, wie man zwischen Zahlensystemen umrechnet - ohne Taschenrechner!

Lernziele:
- Ich kann von dezimal in ein beliebiges Zahlensystem umrechnen, v.a. dec->bin, dec->hex
- Ich kann von einem beliebigen Zahlensystem nach dezimal umrechnen, v.a. bin->dec, hex->dec
- Ich kann von binär in hexadezimal umrechnen.
- Ich kann von hexadezimal in binär umrechnen.

Hausaufgaben:

Übung 1: Darin enthaltenen Theorieteil lesen und die Aufgaben lösen.

HINWEIS: Ich habe die LB-Termine geändert, damit Sie nicht alle LB's auf einem Haufen haben.

M114 Uebung 01 Zahlensysteme

15. Februar - 21. Februar

Codierung Neg. Zahlen im Binärsystem

Binärcodierung:

BCD-Code

1-aus-n-Code

Exzessdarstellung

Hausaufgaben:

Aufgabe 2 und Aufgabe 4: Theorie durchlesen und Aufgaben lösen.
Hinweis: BCD ohne Rechnen, und ohne Excess-Code

M114 Uebung 02 Zahlencodierung

M114 Uebung 04 Binaercodierung

22. Februar - 28. Februar

Heute:

Hausaufgaben anschauen, rep. neg. Binärzahlen, BCD, 1-aus-n-Code

Exzess-Codierung kennenlernen
Wie werden Gleitkommazahlen im Speicher codiert?
Grey-Code, EAN-Code
ASCII-Code und UNICODE? -> Übung 4-1
Hammingdistanz und das Paritätsbit, Redundanzen berechnen -> Übung 3 und 5A

Hausaufgaben:

Alles rekapitulieren: Gleitkommacodierung, Grey-, EAN-, ASCII-, Unicode, Hammingdistanz, und Aufgabe 5, 2. Te

M114 Uebung 03 Hammingdistanz

M114 Uebung 04 Binaercodierung

M114 Uebung 04-1 ASCII Unicode UTF

Beispiel_Unicode

---

1. März - 7. März

Lernziele für heute:
Sie können die (theoretische) Redundanz eines Zeichensatzes berechnen. Dazu steht die Übung 3, erster Teil, zur Verfügung.
Sie können in der Praxis angewandte Methoden erklären und rechnen, die mittels hinzugefügter Redundanz die Datenübertragung sicherer machen (welche können nur Fehlererkennung, welche können Fehlerkorrektur, und wenn ja, wieviele Bits?):
-> Paritätsbit
-> Hammingcode
-> CRC (ev. nächstes Mal)
Dazu steht die Übung 5 zur Verfügung.

Hausaufgaben:

Redundanz, Paritätsbit, Hammingcode und CRC erklären und rechnen können!
Übungen 3 und 5 (soweit besprochen) fertigmachen.

M114 Uebung 05 Fehlererkennung

---

8. März - 14. März

Heute auf dem Programm:
Wir schauen zusammen die Lernziele für die LB1 an.
CRC-Prüfsumme: Wie erkennt nun der Empfänger allfällige Bitfehler?
Bild- und Toncodierung: wie funktioniert es so ungefähr ->Aufgaben 4.2 & 4.3

Hausaufgaben:

Studieren Sie die Lernziele und bereiten Sie sich vor auf die LB1.

M114 Uebung 04-2 Bildcodierung

M114 Uebung 04-3 Toncodierung

---

15. März - 21. März

Heute findet die LB1 statt!
Unten finden Sie das Dokument mit den Lernzielen.

...und danach werden Sie einen Überblick über die Komprimierungsverfahren erhalten.
Wir werden einige verlustfreie Komprimierungsalgorithmen wie Huffman, LZ77, LZ78 und BWT/RLE kennenlernen.
Nicht alles heute, wir fangen einfach mal an:-)

Hausaufgaben:

Mit Huffman-Baum komprimieren MISSISSIPPIFLUSS, TRITTBRETT

M114 Lernziele LB1

22. März - 28. März

Heute auf dem Programm:
Prüfungsbesprechung LB1 (zuerst Nachprüfung durchführen)
Hausaufgaben anschauen und Huffman-Baum nochmals besprechen.
Anwendungen der verlustfreien Algorithmen zeigen.
Die Algorithmen LZ77, LZ78 und BWT kennenlernen.

Hausaufgaben:

1. Huffmanbäume für MISSISSIPPIFLUSS und TRITTBRETT vom letzten Mal zeigen können. Ich werde ein paar Lernende präsentieren lassen!
2. Den LZ77 nochmals anhand der Beispiele durchdenken.

29. März - 4. April

Frühlingsferien

Frühlingsferien

19. April - 25. April

Heute beginnen wir mit dem Thema Verschlüsselung.

Lernziele:
- Sie kennen die zwei grundsätzlichen Verschlüsselungsarten und deren Unterschiede.
- Sie lernen das Cryptool kennen und implementieren die Caesar- und Vigenère-Chiffre.
- Sie kennen zudem die Vernam-Chiffre und wissen, was die Enigma bzw. Rotorchiffre war.

Hausaufgaben:
-> Die Funktionsweise der symmetrischen, asymmetrischen und hybriden Verschlüsselung nochmals durchdenken erklären können.

M114 Uebung 10 Symmetrische Verschl-2

26. April - 2. Mai

Heute auf dem Programm:
1. Kurzrepetition Caesar-, Vigenère- und Vernamchiffre -> für Prüfungsvorbereitung Aufg. 10
2. Übersichtstabelle zu Verschlüsselungsalgorithmen
3. Symmetrische Verschlüsselung: Wie funktioniert der AES? Video und Besprechung.
4. Verwaltung für symmetrische Schlüssel: Passwortverwaltung KEEPASS
5. Asymmetrische Verschlüsselung: Wie funktioniert RSA? Video und Besprechung, siehe auch Doku.

Lernziele
- Sie kennen die Namen und Abkürzungen der heutigen und früheren Verschlüsselungsalgorithmen.
- Sie verstehen die ungefähre Funktionsweise von AES und RSA.
- Sie kennen eine mögliche Passwortverwaltung.

Hausaufgaben:
- Das Dokument zur RSA-Verschlüsselung studieren und das Beispiel darin nachvollziehen. Sie sollten den Algorithmus erk können.
- Die Funktionsweise des AES-Algorithmus repetieren.
- Die Aufgabe 10 lösen zum Thema Caesar, Vigenère, Vernam.

M114 Doku Asymm Verschluess

Video AES-Verschlüsselung

Video RSA-Verschlüsselung

Download-Link KEEPASS

---

3. Mai - 9. Mai

Heute wollen wir die Grundlagen der PKI kennenlernen, insbesondere:
Wie funktioniert die digitale Unterschrift?
Was sind Hash-Funktionen?
Wie läuft in der PKI ab beim Aufruf einer https-Webseite? -> Video "SSL in 3:29 Minuten"
Was sind CA?
...und wir werden OpenSSL installieren und als Erstes einen Hash von einer Zeichenkette generieren.

Lernziele:
- Ich habe den Mechanismus der PKI verstanden.
- Ich habe OpenSSL installiert und einen Hash einer Zeichenkette generiert.

Hausaufgaben:
über die Ferien keine.

Downloadlink für OpenSSL

Anleitung zum Definieren der Umgebungsvariablen für OpenSSL in Windows 10

Pfingstferien

Nicht verfügbar

Pfingstferien

Nicht verfügbar

---

24. Mai - 30. Mai

OpenSSL

Bearbeiten Sie von der folgenden Übung zuerst das letzte Kapitel: Experimentieren mit OpenSSL. Die vorherigen 1 freiwillig und für die, die Interesse haben.

Es geht um Folgendes:
-> Mit OpenSSL ein Zertifikat zu generieren und selber zu unterschreiben
-> Eine Nachricht mit dem öffentlichen Schlüssel zu verschlüsseln und mit dem privaten zu entschlüsseln
-> Den Aufbau der Schlüsseldateien zu studieren (v.a. welcher Schlüssel ist in welchem enthalten)

Hausaufgaben:

Ihr selbst erstelltes und selbst signiertes Zertifikat auf Moodle hochladen. Ihr eigener Name natürlich drin sein!

M114 Uebung 11A -> Gehen Sie auf S.7 Experimentieren mit OpenSSL

Link: Digitale Signaturen mit OpenSSL erstellen

10 PrivateKeys für Nachricht1: Tun Sie, was in der Nachricht steht!

nachricht1

Mein Zertifikat: Wer bin ich, wo und bei welcher Firma arbeite ich?

Abgabelink für Ihr Zertifikat!

Hinweis bei Fehlermeldung:

Falls beim Erstellen des Zertifikats ein Fehler erscheint, dass die openssl.cfg nicht gefunden wird, muss man noch die Umgebungsvariable setzen. Gehen Sie folgendermassen vor:

1. Suchen Sie die Datei openssl.**cfg** oder openssl.**cng** in einem der zwei Verzeichnissen Programme oder Programme (x8
Bei mir ist der Pfad C:\Program Files\Common Files\SSL\openssl.cng, bei Ihnen lautet er vielleicht anders.

2. Kopieren Sie den Pfad zu dieser Datei.

3. Gehen Sie in die Shell und setzen Sie die Umgebungsvariable:

```
set openssl_conf=C:\[Ihr Pfad]\openssl.cfg (oder .cng)
```

Jetzt sollte das Zertifikat ohne Fehlermeldung erstellt werden können.

---

31. Mai - 6. Juni

Heute wollen wir Emails verschlüsseln und dazu Gpg4win kennenlernen.

Lernziele:
- Sie kennen die zwei Varianten, um Email zu verschlüsseln und deren grundlegenden Vertrauenskonzepte.
- Sie haben Gpg4win installiert und können Emails verschlüsseln und/oder unterschreiben.

Die folgende Aufgabe zeigt Ihnen, wie es geht.

**Hinweis: Die Aufgaben auf heute (Zertifikat erstellen) müssen Sie abgeben. Termin heute 07.30 Uhr. Sie können di
Aufgabe heute bis 22.00 Uhr verspätet abgeben.**

M114 Uebung 12 Emailverschuesselung

GPG Kompendium

---

7. Juni - 13. Juni

Heute findet die LB2 statt.

Die Lernziele und weiteren Infos finden Sie im Dokument unten. Ich wünsche Ihnen viel Erfolg und stehe für Fragen gerne Verfügung.

Des weiteren wollen wir heute das Thema Steganografie kennenlernen.

LERNZIELE:
- Sie wissen, was analoge und digitale Steganografie ist.
- Sie können Steganografie mittels BMP-Bildern anwenden und wissen über das Grundprinzip Bescheid.

Modul 114 Lernziele LB2

SteganoG

BMP-Bilder

water stegano

---

14. Juni - 20. Juni

Heute haben wir vier Programmpunkte:
1. Persönliche Durchsicht der korrigierten LB2.
2. Installation eines verschlüsselten Laufwerks auf Ihrem Rechner, z.B. mit Veracrypt. Es gibt dazu eine Demo.
3. Installation eines verschlüsselten Laufwerks in der Cloud, z.B. mit Boxcryptor. Es gibt dazu eine Demo.
4. Installation einer Passwortverwaltung und Wechsel zu sicheren Passwörtern, z.B. mit Keepass. Auch dazu gibt es eine De

Falls Sie einige dieser oder ähnlicher Tools schon verwenden, könnten sie folgendes durchführen:
- Die Punkte realisieren, die Sie noch nicht haben.
- Ein ganzes Laufwerk (anstatt einem Container) verschlüsseln.
- Weitere Sicherheitstools finden und ausprobieren, da lerne ich auch gerne dazu!

Lernziele:
1. Sie haben ein verschlüsseltes Laufwerk auf Ihrem Rechner.
2. Sie haben Ihre Clouddaten verschlüsselt (falls Sie wollen).
3. Sie haben eine Passwortverwaltung in place und allfällige unsichere Passwörter durch sichere ersetzt.
Backup der Passwortdatei nicht vergessen!

Ausblick:
Danach haben wir noch drei Mal. Wenn Sie wollen, können Sie mir Ihre Wünsche angeben. Idealerweise hat es etwas mit k
Komprimierung oder Verschlüsselung zu tun, können aber auch IT-Sicherheit etc. betreffen. Kennt sich jemand in einem G
besonders gut aus und würde uns etwas zeigen? Es kann auch Richtung Hacking, Kali Linux, Honeypots etc. gehen...

---

21. Juni - 27. Juni

Ihre Wünsche, die ich von Ihnen erhalten habe, sind:

Knacken und Hacking

Wir werden heute einwenig hineinschauen:-)

Kali Linux Download-Link

---

28. Juni - 4. Juli

Heute werden wir...
Passwörter knacken, und
kennenlernen, wie man das Passwort für ein WLAN herausfindet.
Sie erhalten von mir einen Hash und sollen mir das Passwort sowie den verwendeten Hashalgorithmus sagen.

Video Passwörter knacken

Hash:

aface255190f27beb8e8cb228e20c849

---

5. Juli - 11. Juli

Nicht verfügbar

Français (fr)

BZT Frauenfeld

https://www.bztf.ch
info@bztf.ch
Tel. +41 58 345 65 00