13. Rückblickübungen

In diesem Unterrichtsblock wollen wir die folgenden, erarbeiten und bereits auch bereits angewendeten Einheiten und Themen, die wir im Modul 114 'Codierungs-, Kompressions- und Verschlüsselungsverfahren einsetzten' repetieren, als auch damit noch mehr festigen.

00 Einleitung für Lehrpersonen und Lernende

Zielsetzung im Modul 114, Voraussetzungen, Überfachliche Kompetenzen, SQL-Umsetzung, Vorschlag zur Organisation des Unterrichts, Sachstruktur

01 Die Zahlensysteme BIN, HEX und DEZ kennenlernen

- Unsere drei Zahlensysteme: Dezimal-, Binär- und Hexadezimalsystem
- Werte vom einen System ins andere umwandeln

02 Arithmetische und logische Grundoperationen binär

- Grundoperationen im Binärsystem: +, -, *, /, AND, OR, XOR, NOT und andere

03 Die Logik und den Prozessor verstehen

- Addieren mit dem Prozessor: Halb- und Volladdierer, Subtraktion, Multiplikation, Division

04 Grosse Zahlen in kleinen Variablen ablegen, wie geht das?

- Integer- und Gleitkomma-Variablen

05 Fehler in der Datenübertragung finden und korrigieren

- Deutlichere Übertragung durch Redundanz: 1-aus-10-Code, 2-aus-5-Code, Hamming-Distanz, Redundanz berechnen
- Prüfziffern
- Fehlererkennung und automatische Korrektur: Paritätsbits, Hamming-Code

06 Speicherplatz als rares Gut – Dateien und ihr Platzbedarf

- Jede Datei ist ein Binärwert: Analyse mit dem HEX-Editor
- Grössen von Dateien: SI-System (Dezimal und Binär)
- Dateiarten
- Codierung für Texte: ASCII- und Uni-Code

07 Speicherplatz als rares Gut – Kompression

- Kompression allgemein
- Ansätze zur verlustfreien Kompression: Huffmann-Code, Faktor und Rate der Kompression

08 Speicherplatz als rares Gut – Reduktion

- Reduktion (Verlustbehaftete Kompression)
- Aufnahme und Reduktion von Audiodateien: Aufnahme, psychoakustische Reduktion
- Aufnahme und Reduktion von Bilddateien: Schwarzweiss-Grafiken, Graufstufen, farbige Bilder

09 Vektorgrafiken – Eine Alternative zu den Pixeln

- Der andere Ansatz
- Vorteile von vektorbasierten Grafiken: Skalierbarkeit, Dateigrösse
- Nachteil von vektorbasierten Grafiken

10 Verschlüsselung – Geschichte und Grundsätzliches

- Ziele beim Schutz von Informationen: Vertraulichkeit, Integrität, Authentizität
- Steganographie
- Geschichte der Verschlüsselung: Monoalphabetische und Caesar- Chiffren, Kryptoanalyse
- Symmetrische und asymmetrische Verschlüsselung mit Hybridem Verfahren

11 Verschlüsselung – Moderne Verfahren

- Das RSA-Verfahren (Vertraulichkeit): Anwendung binärer Schlüssel
- Digitale Signatur (Authentizität)

12 Kryptographie und Steganographie

- Diese beiden Verfahren kennen, unterscheiden und anwenden

13 Rückblickübungen

Mit Rückblickübungen die erarbeiteten und angewendeten M114-Themen repetieren und damit festigen!

Als Unterrichtshilfen dienten uns:

- Die Unterrichtsblöcke auf https://eitswiss.berufscockpit.ch/app/gebaeudeinformatiker-kommunikationmultimedia/
- Arbeits- und Übungsblätter nach 'eitswiss.berufscockpit.ch'
- Vertiefungsübungen und praktische Anwendungen

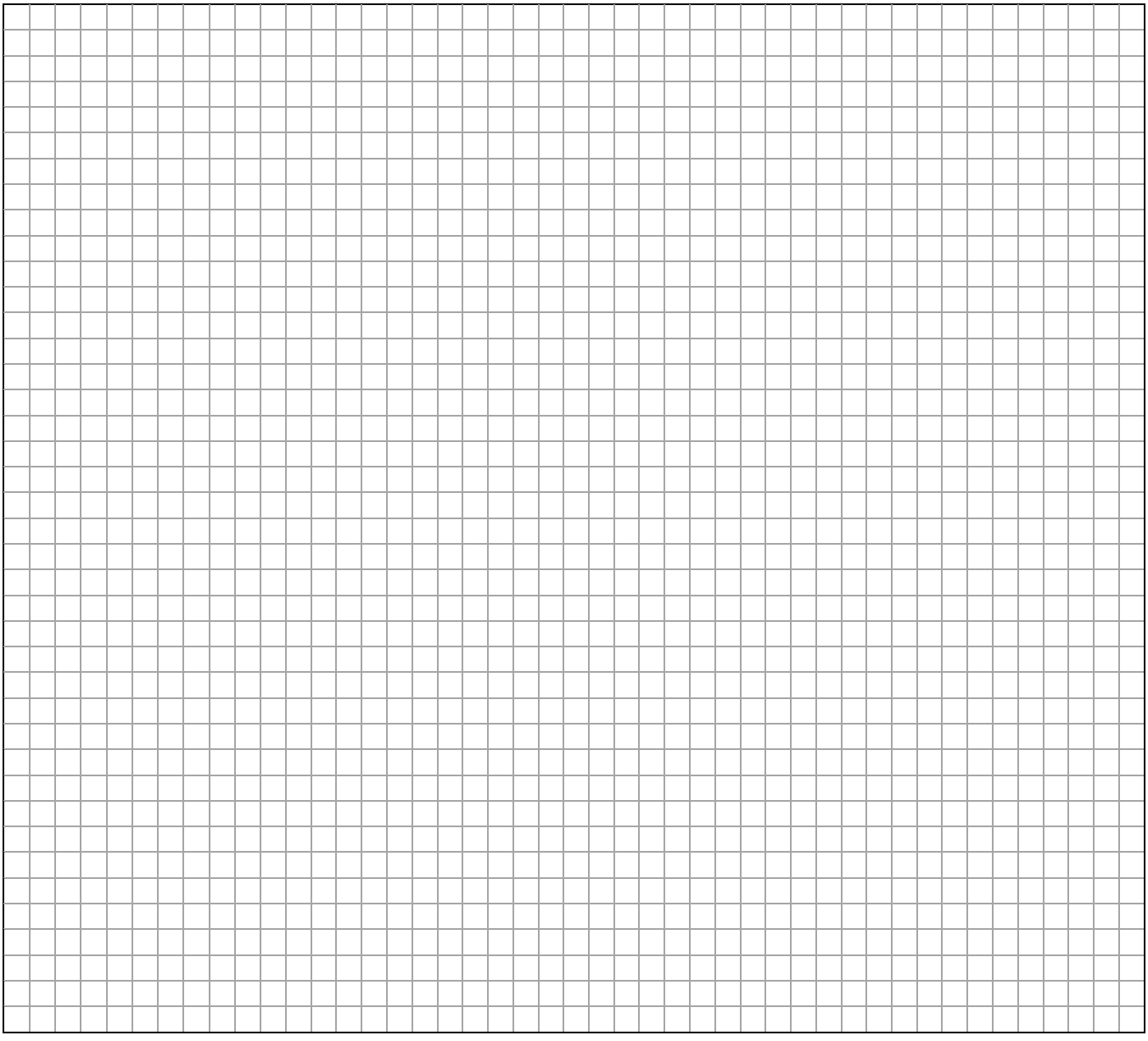
Rückblickübungen

Lösen Sie alle Rückblickübungen wie gewohnt und zu Ihrem Vorteil vollständig und klar. Schreiben Sie zudem Ihre Lösungen alle in ein pdf-File, welches Sie schlussendlich dann auch auf TEAMS abgeben werden!

1. Bei Aufgabe 11.1 wendeten wir bereits binäre Ver- und Entschlüsselung mit der XOR-Verknüpfung kennen, die wir nochmals durchführen und dokumentieren, als auch damit vertiefen wollen.
Verwandeln Sie im Folgenden die ASCII-Codewerte der Buchstaben in Binärzahlen:
Verschlüsseln Sie die Buchstaben des Wortes „SEMESTERENDE“ mit dem Schlüssel „KLASSE“ durch eine XOR-Operation. Übertragen Sie dann die erhaltene, binäre Lösung mit einem E-Mail an eine Ihrer Klassenkollegsperson. Diese entschlüsselt dann mit dem zuvor mitgeteilten Schlüssel "KLASSE" diesen erhaltene XOR-Binärcode und sollte dann das ursprüngliche Wort "SEMSTERENDE" wieder erhalten. Dokumentieren Sie diese Entschlüsselungsprüfung.

2. Bei der Aufgabe 11.2 und 11.3 wendeten Sie bereits die RSA-Verschlüsselung an. Die Personen: Rivest, Shamir udn Adleman definierten dieses Verschlüsselungsverfahren, welches wir mit dieser Übungen wieder anwenden und vertiefen wollen!
Bei der Aufgabe 11.2 lernten Sie mit dem Dokument „Funktionsweise RSA-Verschlüsselung“ dieses Verfahren und spielten dann mit dem Beispiel das folgenden Zahlenwerten mit p = 17; q = 3; e = 5 und m = 11 durch. Dann wendeten Sie dieses RSA-Verfahren mit der Aufgabe 11.3 an. Lösen Sie diese beiden Aufgaben nochmals und dokumentieren Sie Ihre Lösungen vollständig und klar. Bei der Aufgabe 11.3 installieren Sie bekanntlich bereits die Software 'Gpg4win' inklusive der Optionen 'Kleopatra' und 'GpgEX' auf Ihrem BYOD. Die folgenden Übungen erledigen Sie nun eben nochmals vollständig und klar:

- Erstellen Sie ein neues Schlüsselpaar (IET-Mailadresse verwenden). Exportieren Sie nun Ihren öffentlichen Schlüssel in eine Datei. Deponieren Sie diese wiederum in den Ordner «Keys» auf dem Klassenshare.
- Importieren Sie den öffentlichen Schlüssel Ihres Nachbarn.
- Verschlüsseln Sie nun eine Datei (Kontextmenu im Explorer) mit dem öffentlichen Schlüssel Ihres Nachbarn und senden Sie ihm diese per Mail zu.
- Kann Ihr Nachbar die Datei entschlüsseln?



3. Bei der Zusatzaufgabe prüften Sie bereits die korrekte Übertragung von Ethernet-Frames und vielen anderen Dateien, welche Sie mit der CRC-Prüfsumme dann garantieren konnten. Übertragen Sie die Buchstaben 'E', 'N' und 'D' mit der CRC-Prüfsumme mit einem z.B. E-Mail mit einer 33 langen Bitfolge an einen Ihrer Klassenkollegsperson, welche dann die Übertragung kontrolliert und diese 3 Buchstaben wieder dechiffriert.

4. Erstellen Sie für den Text 'bigmad mag gabi' einen Huffmann-Codebaum und teilen Sie diesen einer Klassenkollegsperson mit. Senden Sie dann diesen Text 'bigmad mag gabi' mit einem E-Mail Ihrer Klassenkollegsperson, welche dann diesen Huffmanncodierten Text dechiffriert und damit diesen Text auch wieder erhalten sollte!

5. Verschlüsseln Sie den Text 'LETZTETAGESAUFGABE' in eine Templer-Chiffre-Nachricht und senden Sie diese mit einem E-Mail an einen Ihrer Klassenkollegsperson, welche dann diesen chiffrierten wieder deschiffriert. Die Adresse der entsprechenden Webside finden Sie in Ihren M114-Unterlagen!
6. Welche Redundanz und welchen Hamming-Abstand hat der Code 'Binary Coded Decimals', für was genau dient dieser Code und wie ist dieser aufgebaut? Vergessen Sie dabei nicht, dass Sie die Herleitung Ihrer Resultate vollständig, normgerecht und klar darstellen und erklären müssen!
7. Die Zahl 'Reelling' ist in einem C-Programm eine Variable vom Datentyp 'float'.
   Nun wir im Programm dieser Variablen 'Reelling' die Zahl 456 zugewiesen.
   Beschreiben Sie klar und deutlich, wie diese Zahl im Speicher aussieht!