Übung Übertragungstechnik I

Aufgabe 11

In einer Kodierung wird die Modulo-2-Addition sowohl zum Kodieren als auch später zum Dekodieren verwendet. Die Addition erfolgt jeweils mit dem selben Schlüssel.

Daten („Klartext“)	1 0 1 1 1 0 0 0 0 0 1 1 0 0 1 1 1 1 0 0 1 0 1 0
Schlüssel	1 0 1 1 0 1 0 0 0 1 0 1 1 1 0 1 1 1 0 0 1 0 0 0

Aufgabe 11.1: Fertigen Sie zu der Aufgabe eine Skizze an.

Aufgabe 11.2: Bitte ermitteln Sie die kodierten Daten.

Aufgabe 11.3: Bitte formen Sie den Klartext und die kodierten Daten jeweils in die hexadezimale Schreibweise um.

Aufgabe 11.4: Bitte dekodieren Sie die kodierten Daten.

Übung Übertragungstechnik I

Aufgabe 12

Ein Programm verwendet Passwörter. Diese werden in einer Datenbank gespeichert. Die Speicherung erfolgt nicht direkt sondern über die MD5-Hashwerte.

Aufgabe 12.1: Ab welcher Passwortlänge sind Kollisionen prinzipiell nicht zu vermeiden? Diskutieren Sie den Zusammenhang?

Aufgabe 12.2: Hängt die Passwortlänge vom Alphabet ab, aus dem die Passworte gebildet werden? Wenn ja, wie? Geben Sie den mathematischen Zusammenhang an.

Übung Übertragungstechnik I

Aufgabe 13

Ein Programm verwendet Passwörter. Diese werden in einer Datenbank gespeichert. Die Speicherung erfolgt nicht direkt sondern über die MD5-Hashwerte.

Die Möglichkeit, mittels eines Brute-force-Angriffes Passwörter im Klartext zu ermitteln, soll durch die vorgeschriebene Länge und das vorgeschriebenes Alphabet der Passwörter minimiert werden. Die Passwörter sollen nicht länger als nötig sein.

Aufgabe 13.1: Wie kann die Länge ermittelt werden? Was für eine Rolle spielt das Alphabet?

Aufgabe 13.2: Ermitteln Sie bitte die Längen, wenn folgende Alphabete verwendet werden:

A: alle großen lateinischen Buchstaben
B: alle großen und kleinen lateinischen Buchstaben
C: alle Ziffern
D: alle großen und kleinen lateinischen Buchstaben und alle Ziffern
E: alle großen und kleinen lateinischen Buchstaben und alle Ziffern und 5Sonderzeichen

Übung Übertragungstechnik I

Aufgabe 14

Eine Quelle sendet Symbole mit unterschiedlicher Wahrscheinlichkeit. Durch eine Expansionssubstitution sollen die unterschiedlichen Wahrscheinlichkeiten verdeckt werden.

Quelle X {A B C D E F} $P(x_i)$ {0,1 0,2 0,05 0,15 0,2 0,3}

Aufgabe 14.1: Ermitteln Sie durch Überlegung, wieviele Symbole das Alphabet der Kodierung besitzen muss, um gleiche Wahrscheinlichkeiten zu ermöglichen.

Aufgabe 14.2: Wie kann das mathematisch ermittelt werden?

Übung Übertragungstechnik I

Aufgabe 15

Im Browser MS-IE oder Seamonkey werden die vorhandenen Zertifikate angezeigt.

IE: Extras – Internetoptionen – Inhalte – Zertifikate

Seamonkey: Bearbeiten – Einstellungen – Datenschutz & Sicherheit – Zertifikate – Zertifikate verwalten

Aufgabe 15.1: Bitte prüfen Sie, ob Zertifikate von Personen vorhanden sind. Wenn ja, untersuchen Sie eines dieser Zertifikate auf den Inhalt. Interpretieren Sie den Inhalt.

Aufgabe 15.2: Bitte untersuchen Sie den Inhalt von einem Zertifikat einer Zertifizierungsstelle (Authority). Nutzen Sie, soweit vorhanden, ein Zertifikat der Deutschen Telekom und eines der FH-Jena.

Aufgabe 15.3: Bitte erklären Sie den Unterschied zwischen dem Zertifikat einer Person und dem einer Zertifizierungsstelle.

Übung Übertragungstechnik I

Aufgabe 16

Gegeben sind zwei Klartexte P1 und P2 und ein Schlüsselstrom KS. Die Verschlüsselung erfolgt durch Px + KS = Mx.

P1: 1 1 1 2 3 3 1 3 1 1 1

P2: 1 3 3 2 1 1 1 2 1 1 3

KS: 1 3 2 1 5 2 3 5 2 1 5

Aufgabe 16.1: Sind augenscheinlich ungleiche statistische Verteilung der Symbole in P zu sehen?

Aufgabe 16.2: Bitte bilden Sie aus jeweils dem Klartext und dem Schlüsselstrom die verschlüsselte Nachrichten M1 und M2. Lassen sich augenscheinlich Rückschlüsse auf die statistische Verteilung der Symbole in P ziehen?

Aufgabe 16.3: Bitte bilden Sie aus den beiden verschlüsselten Nachrichten die Differenz. Lassen sich augenscheinlich Rückschlüsse auf die statistische Verteilung der Symbole in P ziehen?

Übung Übertragungstechnik I

Aufgabe 17

C ist ein binärer Kanalkode. Aus Blöcken der Länge 2 des Eingangsdatenstromes X werden Kodeworte c_i gebildet. Dabei wird die von X stammende Bitfolge 3 mal wiederholt und angefügt. Die beiden originalen Bits und die sechs angefügten Bits ergeben jeweils ein Kodewort.

Aufgabe 17.1: Bilden Sie die Kodebeschreibung nach dem Muster **C** (n, k, d).

Aufgabe 17.2: Bilden Sie alle Kodewort c_i in aufsteigender Reihenfolge von x_i.

Aufgabe 17.3: Ermitteln Sie die Hamming-Gewichte.

Aufgabe 17.4: Ermitteln Sie die Hamming-Distanzen für das dritte Kodewort (x_i in aufsteigender Reihenfolge) zu allen anderen Kodeworten.

Aufgabe 17.5: Ermitteln Sie die Gewichtsverteilung.

Aufgabe 17.6: Ermitteln Sie die Distanzverteilung und vergleichen Sie diese mit der Gewichtsverteilung.

Aufgabe 17.7: Ermitteln Sie das minimale Gewicht.

Aufgabe 17.8: Ermitteln Sie die Mindestdistanz.

Aufgabe 17.9: Wie viele Bitfehler in r sind sicher erkennbar?

Aufgabe 17.10: Wie viele Bitfehler in r sind sicher korrigierbar?

Aufgabe 17.11: Stellen Sie die Formel für die Hamming-Schranke mit diesen Werten auf und rechnen Sie diese durch.

Aufgabe 17.12: Handelt es sich um einen perfekten Kode?.

Aufgabe 17.13: Ermitteln Sie die Prüfmatrix.

Aufgabe 17.14: Führen Sie für zwei korrekte r die Multiplikation mit der Prüfmatrix aus.

Aufgabe 17.15: Ermitteln Sie für zwei fehlerhafte r die Syndrome.

Übung Übertragungstechnik I

Aufgabe 18

C ist ein binärer Kanalkode. Aus einzelnen Bits des Eingangsdatenstromes X werden Kodeworte c_i gebildet. Dabei wird das von X stammend Bit 3 mal wiederholt und angefügt. Das originale Bit und die drei angefügten Bits ergeben jeweils ein Kodewort.

Aufgabe 18.1: Bilden Sie die Kodebeschreibung nach dem Muster **C** (n, k, d).

Aufgabe 18.2: Bilden Sie alle Kodewort c_i in aufsteigender Reihenfolge von x_i.

Aufgabe 18.3: Ermitteln Sie die Hamming-Gewichte.

Aufgabe 18.4: Ermitteln Sie die Hamming-Distanzen.

Aufgabe 18.5: Ermitteln Sie die Gewichtsverteilung.

Aufgabe 18.6: Ermitteln Sie die Distanzverteilung und vergleichen Sie diese mit der Gewichtsverteilung.

Aufgabe 18.7: Ermitteln Sie das minimale Gewicht.

Aufgabe 18.8: Ermitteln Sie die Mindestdistanz.

Aufgabe 18.9: Wieviele Bitfehler in r sind sicher erkennbar?

Aufgabe 18.10: Wieviele Bitfehler in r sind sicher korrigierbar?

Aufgabe 18.11: Stellen Sie die Formel für die Hamming-Schranke mit diesen Werten auf und rechnen Sie diese durch.

Aufgabe 18.12: Handelt es sich um einen perfekten Kode?.

Aufgabe 18.13: Ermitteln Sie die Prüfmatrix.

Aufgabe 18.14: Führen Sie für zwei korrekte r die Multiplikation mit der Prüfmatrix aus.

Aufgabe 18.15: Ermitteln Sie für zwei fehlerhafte r die Syndrome.

Aufgabe 18.16: Vergleichen Sie die Ergebnisse dieser Aufgabe mit den Ergebnissen der vorherigen Aufgabe. Diskutieren Sie Gemeinsamkeiten und Unterschiede.

Übung Übertragungstechnik I

Aufgabe 19

Das folgende Polynom steht für einen Körper.

$$x^N + 1 \qquad N = 7$$

Aufgabe 19.1: Überprüfen Sie, ob die folgenden Polynome Teiler des oben stehenden Polynoms sind (Teilung ohne Rest). (Wenn ja, und wenn das jeweilige Polynom nicht selber faktorisiert werden kann, dann steht das jeweilige Polynom für einen Unterkörper.)

$$x + 1$$

$$x^2 + 1$$

$$x^3 + x^2 + 1$$

$$x^3 + x^2 + x + 1$$

$$x^3 + x + 1$$

Übung Übertragungstechnik I

Aufgabe 20

Das folgende Polynom ist ein Generatorpolynom für einen zyklischen (7,4)-Blockkode.

$$x^3 + x^2 + 1$$

Aufgabe 20.1: Ermitteln Sie die Generatormatrix G in systematischer Form.

Aufgabe 20.2: Ermitteln Sie aus G alle möglichen Elemente von **C** und schreiben Sie diese in aufsteigender Reihenfolge auf.

Aufgabe 20.3: Ermitteln Sie die minimale Hamming-Distanz.

Aufgabe 20.4: Überprüfen Sie anhand des Ergebnisses aus 20.2, ob jedes Codewort der bitweisen Verschiebung eines Kodewortes entspricht.

Aufgabe 20.5: Überprüfen Sie für wenigstens drei Kodeworte, ob sie ganze Vielfache von g(x) sind.

Aufgabe 20.6: Ermitteln Sie das Blockschaltbild für die Implementierung des Kodierers unter Verwendung von Schieberegistern und XOR-Gliedern.

Aufgabe 20.7: Simulieren Sie die Bildung der Kodeworte in der ermittelten Schaltung. Verwenden Sie alle möglichen Eingangsdatenworte. Schreiben Sie das Ergebnis in einer zur Aufgabe 20.2 vergleichbaren Form auf.

Aufgabe 20.8: Vergleichen Sie die Ergebnisse von 20.2 und 20.7.