Fakultät für Informatik

Technische Hochschule **Rosenheim**

Prüfung **WS 2019/20**
Studiengang: INF-B
Fach: Grundlagen der Informatik
Prüfer: Prof. Dr. J. Schmidt
Prüfung: 4.2.2020

90 Minuten. Hilfsmittel: alle Unterlagen, Taschenrechner, **kein** Laptop, Handy, u.ä.
Es sind insgesamt 90 Punkte zu erreichen. Die Prüfung besteht aus zwei Teilen, die separat bewertet werden. Die Endnote ergibt sich aus dem gewichteten arithmetischen Mittel der beiden Teilnoten.
Die Seiten dürfen nicht getrennt werden. Konzeptpapier muss (mit Namen versehen) mit abgegeben werden.

Name: _____ **Matrikelnr.:**_____

Aufgabe	1	2	3	4	5	ges.
Punkte						

Note Teil 1:

Aufgabe	6	7	8	9	10	11	12	ges.
Punkte								

Note Teil 2:

Gesamtnote:

Teil 1 – Multiple Choice (40 Punkte)

Geben Sie im Folgenden für jede Aussage an, ob sie zutrifft oder nicht zutrifft.
Es gibt **keinen** Punktabzug für falsch gesetzte Kennzeichnungen.

Aufgabe 1: Hardware (4 Punkte)

Beantworten Sie die folgenden Fragen (je 1 Punkt):

	Trifft zu	Trifft nicht zu
Der Datenbus transportiert Daten zwischen RAM und CPU	☐	☐
Die ALU ist ein Teil der CPU	☐	☐
Bei der von-Neumann-Architektur liegen Daten und Programme in getrenntem RAM	☐	☐
Register sind Speicherzellen im Prozessor	☐	☐

Aufgabe 2: Zahlendarstellung (11 Punkte)

Beantworten Sie die folgenden Fragen für die Zahlendarstellung Binärformat (Basis 2) (je 1 Punkt):

	Trifft zu	Trifft nicht zu
Im Einerkomplement gibt es eine positive und eine negative Null	☐	☐
Im Zweierkomplement gibt es eine positive und eine negative Null	☐	☐
Im IEEE-Gleitkommaformat gibt es eine positive und eine negative Null	☐	☐

Beantworten Sie die folgenden Fragen (je 2 Punkte):

	Trifft zu	Trifft nicht zu
$8110_{10} = 11111_{17}$	☐	☐
$10{,}1_{16} = 12{,}04_{8}$	☐	☐

Im Standard IEEE 754-2008 werden neben den in der Vorlesung behandelten binären Gleitkommazahlen mit 32/64 Bit Länge auch welche mit halber Genauigkeit (16 Bit) wie folgt definiert:

- 1 Vorzeichenbit
- 5 Bit Exponent (Bias: 15)
- 10 Bit Mantisse

Gegeben sei die folgende Gleitkommazahl in diesem Format in hexadezimaler Form: C848
Beantworten Sie dazu die folgenden Fragen (je 2 Punkte):

	Trifft zu	Trifft nicht zu
Der „echte“ Exponent (d.h. ohne Bias) ist –3	☐	☐
Es handelt sich um die Dezimalzahl –0,5625	☐	☐

Aufgabe 3: Verschlüsselung (10 Punkte)

Für eine RSA-Verschlüsselung werden die Primzahlen p = 17, q = 23 verwendet.

Beantworten Sie dazu die folgenden Fragen (je 2 Punkte):

	Trifft zu	Trifft nicht zu
Ein möglicher öffentlicher Schlüssel ist (3, 352)	☐	☐
Ein möglicher öffentlicher Schlüssel ist (5, 391)	☐	☐
Unter der Annahme (5, 391) wäre ein korrekter öffentlicher Schlüssel: Dann ist 301 ein passender privater Schlüssel	☐	☐
20 verschlüsselt mit (5, 391) ergibt 56	☐	☐
Für den Austausch der RSA-Schlüssel benötigt man einen sicheren Kanal	☐	☐

Aufgabe 4: Codierung (11 Punkte)

Beantworten Sie die folgenden Fragen (je 1 Punkt):

	Trifft zu	Trifft nicht zu
Ein Code mit Hamming-Distanz 10 kann 2-Bit-Fehler erkennen	☐	☐
(Eindimensionale) Paritätsprüfung hat eine Hamming-Distanz von 2	☐	☐
Mit einer Lauflängencodierung lassen sich 1-Bit-Fehler erkennen	☐	☐
Huffman- und Fano-Codierung erzeugen immer den gleichen Code	☐	☐
Die Redundanz einer ASCII-Codierung ist dann minimal, wenn alle Zeichen die gleiche Auftrittswahrscheinlichkeit haben	☐	☐

Wir betrachten nun einen (15, 11) Hamming-Code. Empfangen wurde das Codewort
010 0101 0000 0011

Beantworten Sie dazu die folgenden Fragen (Nummerierung der Bits von rechts, je 1 Punkt):

	Trifft zu	Trifft nicht zu
Der Code hat eine Hamming-Distanz von 2	☐	☐
Die Paritätsbits befinden sich an den Stellen 1, 2, 4, 8, 16	☐	☐

Außerdem die folgenden Fragen (je 2 Punkte):

	Trifft zu	Trifft nicht zu
Das Codewort wurde fehlerfrei empfangen	☐	☐
Die gesendeten Daten (ohne Paritäten) waren 0100 1010 000	☐	☐

Aufgabe 5: Graphen (4 Punkte)

Gegeben sei die folgende Adjazenzmatrix eines Graphen:

$$\boldsymbol{A} = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

Beantworten Sie dazu die folgenden Fragen (je 1 Punkt):

	Trifft zu	Trifft nicht zu
Die Eingangsgrade der Knoten sind 1, 2, 2, 2	☐	☐
Der Graph ist ein binärer Wurzelbaum	☐	☐
$\boldsymbol{A}^5 \neq \boldsymbol{0}$	☐	☐
$\boldsymbol{S} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$ wäre die Adjazenzmatrix eines Spannbaums	☐	☐

Teil 2 – Schriftliche Aufgaben (50 Punkte)

Bearbeiten Sie die folgenden Aufgaben auf dem separaten Prüfungspapier. Sollten Ihrer Meinung nach Angaben in der Aufgabenbeschreibung fehlen oder falsch sein, machen Sie sinnvolle Annahmen und dokumentieren Sie diese. Der Berechnungsweg muss ersichtlich sein.

Aufgabe 6: Codierung (10 Punkte)

Gegeben sei eine Nachrichtenquelle, die das folgende tabellierte Alphabet mit den Zeichen $\{x_i\}$ und den zugehörigen Auftrittswahrscheinlichkeiten $\{p_i\}$ sendet.

x_i	p_i	I_i	l_i
A	0,5		
B	0,04		
C	0,08		
D	0,21		
E	0,1		
F	0,07		

a) Berechnen Sie die Informationsgehalte I_i für das Alphabet und tragen Sie die Ergebnisse (mit 2 Nachkommastellen) in die oben stehende Tabelle ein. Berechnen Sie daraus die Entropie.

b) Bilden Sie den einen Binärcode für das Alphabet mit Hilfe des Huffman-Verfahrens und tragen Sie die sich ergebenden Wortlängen l_i in die obige Tabelle ein.

c) Berechnen Sie nun die mittlere Wortlänge und die Redundanz für den in (b) ermittelten Code.

d) Geben Sie die Wortlänge des kürzesten Block-Codes für das Alphabet an.
Um wie viel Prozent ist ein mit diesem Block-Code codierter Text länger als einer, der mit dem Huffman-Code codiert wurde?

Aufgabe 7: Rechnerarchitektur (5 Punkte)

Die CPU eines Rechners habe einen Steuerbus der Breite 8 Bit, einen Adressbus der Breite 16 Bit und Datenbus der Breite 32 Bit. Die Busse und CPU seien alle gleich mit 1MHz getaktet.

a) Wie groß ist der Adressraum, d.h. wie viele Speicherzellen sind adressierbar?

b) Wie groß ist die maximal mögliche Größe des RAM in KiB, wenn man davon ausgeht, dass der Speicher nicht byteweise sondern immer nur in 32 Bit Blöcken adressiert werden kann?

c) Wie hoch ist die maximal mögliche Datenrate in MiB/s, wenn man davon ausgeht, dass 10% der Bandbreite durch das Busprotokoll für die Synchronisierung und Sicherung der Datenübertragung benötigt (Overhead) werden?

Aufgabe 8: Zahlendarstellung (4 Punkte)

Gegeben sei der Speicherinhalt einzelner Bytes eines Computers, jedes Byte entspricht einer ganzen Zahl. Geben Sie an, wie die Zahlen in normaler Dezimaldarstellung aussehen, wenn sie im Einer- bzw. Zweierkomplement codiert wurden bzw. wenn eine nicht-vorzeichenbehaftete Darstellung (unsigned) verwendet wurde:

Speicherinhalt	unsigned	Zweierkomplement	Einerkomplement
$F4_{16}$			
22_{16}			

Aufgabe 9: Codierung – CRC-Code (8 Punkte)

Zur Absicherung während der Übertragung sollen Daten mit einem CRC-Code gesichert werden. Verwendet wird folgendes Generatorpolynom:

$x^7 + x^5 + x^4 + x^3 + x + 1$

a) Berechnen Sie den CRC für die zu sendende Nachricht: 1011 1010
Geben Sie dann die komplette Bitfolge an, wie sie nach der Berechnung gesendet werden muss.

b) Lassen sich mit diesem Generator alle k-Bit Fehler erkennen, wenn k die Form $k = 2n + 1, n = 0, 1, 2, 3, 4, \ldots$ hat?

Aufgabe 10: Verschlüsselung – Diffie-Hellman (6 Punkte)

Beim Diffie-Hellman-Schlüsseltausch werden zwei öffentliche Zahlen benötigt: Eine Primzahl p sowie eine ganze Zahl g ∈ {2, 3, …, p – 2}.
Es seien p = 37 und g = 4.

a) Alice wählt nun als geheimen Exponenten die Zahl 2, Bob wählt 4.
   - Welche Zahl wird von Alice an Bob übertragen?
   - Welche Zahl wird von Bob an Alice übertragen?
   - Wie lautet der generierte Schlüssel?

b) Ist p eine sichere Primzahl?
c) Ist g eine primitive Wurzel modulo p?

Aufgabe 11: Verschlüsselung – Elliptische Kurven (12 Punkte)

Gegeben sei folgende Gleichung:

$$y^2 = x^3 + 5x$$

Gerechnet wird im endlichen Körper mit 31 Elementen.

a) Erfüllt diese Gleichung die Anforderungen an eine elliptische Kurve?

b) Liegen die Punkte (0, 0) und (2, 24) auf der Kurve?

c) Bestimmen Sie die Summe S = (0, 0) + (2, 24) nach den Rechenregeln für elliptische Kurven.

Aufgabe 12: Graphen (5 Punkte)

Bestimmen Sie für den folgenden gewichteten Graphen den kürzesten Weg von G nach A mit uniformer Kosten Suche. Bei gleicher Bewertung soll der Zielknoten bevorzugt expandiert werden.

Zeichnen Sie den Suchbaum. Die Reihenfolge der Knotenexpansion und die Bewertung muss ersichtlich sein.