Fakultät für Informatik

Hochschule **Rosenheim**
University of Applied Sciences

Prüfung **WS 2015/16**
Studiengang: INF-B
Fach: Grundlagen der Informatik 1
Prüfer: Prof. Dr. J. Schmidt
Prüfung: 26.1.2016

90 Minuten. Hilfsmittel: alle Unterlagen, Taschenrechner, **kein** Laptop, Handy, u.ä.
Insgesamt sind 90 Punkte zu erreichen. Die Punktzahl gibt damit auch einen Anhaltspunkt für die Bearbeitungszeit.
Sollten Ihrer Meinung nach Angaben in der Aufgabenbeschreibung fehlen, machen Sie sinnvolle Annahmen und dokumentieren Sie diese.
Der Berechnungsweg muss ersichtlich sein.
Die Seiten dürfen nicht getrennt werden.
Konzeptpapier muss (mit Namen versehen) mit abgegeben werden.

Aufgabe	1	2	3	4	5	6	7	8	9	ges.
Punkte										

Note:

Name: _____ **Matrikelnr.:** _____

Aufgabe 1: Codierung (15 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	0,12		
B	0,15		
C	0,25		
D	0,1		
E	0,18		
F	0,06		
G	0,14		

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.
Mit welchem Kompressionsfaktor kann man unter Verwendung des Huffman-Codes die Länge eines mit dem Alphabet formulierten Textes im Vergleich zu dem kürzesten Block-Code verringern?

Aufgabe 2: Zahlendarstellung (13 Punkte)

a) Geben Sie die Zahl 5843_{10} im Stellenwertsystem zur Basis 13 an.

b) Führen Sie die Rechenoperation 12 – 54 in binärer Arithmetik unter Verwendung des Zweierkomplements (mit 8 Stellen) aus.
Geben Sie Ihr Ergebnis (d.h. die Summe im Zweierkomplement interpretiert als vorzeichenlose Binärzahl) in dezimaler, oktaler und hexadezimaler Form an!

c) Gegeben sei die hexadezimale Zahl C7 9C 7D 20. Diese soll als 32-Bit Gleitpunktzahl nach IEEE-Format interpretiert werden.
Geben Sie die Zahl in der üblichen dezimalen Schreibweise an.

d) Wie sieht die Gleitpunktzahl aus der vorhergehenden Teilaufgabe in hexadezimaler Form aus, wenn sie durch zwei dividiert wird?

Aufgabe 3: Verschlüsselung – Diffie-Hellman (7 Punkte)

Beim Diffie-Hellman-Schlüsseltausch werden zwei öffentliche Zahlen benötigt: Eine Primzahl p sowie eine ganze Zahl $g \in \{2, 3, \ldots, p-2\}$.
Es seien $p = 19$ und $g = 3$.

a) Alice wählt nun als geheimen Exponenten die Zahl 3, Bob wählt 2.
   - Welche Zahl wird von Alice an Bob übertragen?
   - Welche Zahl wird von Bob an Alice übertragen?
   - Wie lautet der generierte Schlüssel?

b) Zeigen Sie: p ist keine sichere Primzahl.

c) Zeigen Sie: g ist eine primitive Wurzel modulo p.

d) Der berechnete Schlüssel wurde nun in binärer Form als One-Time-Pad verwendet. Empfangen wurde der Chiffretext 5 (dezimal). Wie lautet die Botschaft im Klartext?
Hinweis: Falls Sie kein Ergebnis für den Schlüssel aus (a) haben, dann verwenden Sie bitte den Schlüssel 6.

Aufgabe 4: Verschlüsselung – RSA (5 Punkte)

Beim RSA-Verfahren wird für jeden Teilnehmer ein öffentlicher Schlüssel im Schlüsselverzeichnis veröffentlicht. Dieser besteht aus einer Zahl n, die das Produkt zweier großer Primzahlen p und q ist, sowie einem Exponenten c. Jeder Teilnehmer erhält ferner einen geheimen Schlüssel d.

a) Es seien p = 7 und q = 13. Berechnen Sie daraus n und den Wert der eulerschen Funktion $\phi(n)$.

b) Zeigen Sie, dass c = 11 als Teil des öffentlichen Schlüssels geeignet ist.

c) Alice verwendet c = 11 als Teil des öffentlichen Schlüssels.
Zeigen Sie, dass d = 59 als geheimer Schlüssel geeignet ist

Aufgabe 5: Kompression (8 Punkte)

Daten bestehend aus Zeichen des Alphabets A = { W, X, Y, Z} sollen mit arithmetischer Codierung komprimiert werden. Die Tabelle mit den Auftrittswahrscheinlichkeiten p_i sieht wie folgt aus:

Zeichen	p_i	Intervall
W	$1/2$	
X	$1/10$	
Y	$1/5$	
Z	$1/5$	

a) Füllen Sie die fehlende Spalte für das dem Zeichen zugeordnete Intervall aus.

b) Kodieren Sie den Text XYXYZ.

Aufgabe 6: CRC (5 Punkte)

Zur Absicherung während der Übertragung sollen Daten mit einem CRC-Code versehen werden.
Als Generatorpolynom wird $x^6 + x + 1$ verwendet.
Es wurde folgende binäre Nachricht empfangen: 11 0011 1001 1101

a) Prüfen Sie, ob während der Übertragung Fehler aufgetreten sind.

b) Wie lautet die zu empfangene Nachricht ohne den angehängten CRC-Code?

Aufgabe 7: Verschiedenes (9 Punkte)

Welche der folgenden Aussagen sind richtig bzw. falsch? Kreuzen Sie das entsprechende Feld an. Falsche Antworten geben Punktabzug (wird nicht auf andere Aufgaben übertragen).

Aussage	richtig	falsch
Es gibt Hamming-Codes mit Hamming-Distanz 2		
Die Breite des Datenbusses einer CPU legt fest, wie viele Bits parallel ins RAM übertragen werden können		
Die Zahl $0{,}2_{10}$ ist als binäre Gleitkommazahl exakt darstellbar		
Damit ein Code Fehler korrigieren kann, muss er mindestens Hamming-Distanz 1 haben		
AES ist ein fehlerkorrigierender Code		
Die Adjazenzmatrix eines Graphen definiert diesen vollständig		
Die Zahl $0{,}2_{10}$ ist als BCD-Zahl exakt darstellbar		
Der LZW-Kompressionsalgorithmus kann die Codetabelle bei der Dekompression erzeugen – sie muss nicht mit übertragen werden		
Bei Verwendung der Lauflängen-Kodierung kann eine Datei nach der Kompression größer sein als vorher		

Aufgabe 8: Reed-Solomon Code (13 Punkte)

Zur Reed-Solomon Codierung in dieser Aufgabe wird ein endlicher Körper mit 3 Elementen verwendet, die Länge der (uncodierten) Nachricht sei 2, die Codewortlänge 3.

a) Kodieren Sie die Nachricht (3, 2).

b) Empfangen wurde das Codewort (2, ε, 0), wobei ε ein Ausfall ist.
Wie lautet die ursprüngliche (decodierte) Nachricht?

Aufgabe 9: Graphsuche (15 Punkte)

In dieser Aufgabe wird ein Schiebepuzzle bestehend aus einem 3x3 Feld betrachtet, auf dem sich 8 Spielsteine und ein leeres Feld befinden. Die Spielsteine sind mit den Ziffern 1 – 9 beschriftet und können jeweils senkrecht bzw. waagrecht in das angrenzende leere Feld geschoben werden. Ziel des Spiels ist es, die Steine in die folgende Anordnung zu bekommen:

1	2	3
4	5	6
7	8	

Gegeben ist folgende **Start**anordnung:

1		3
4	2	6
7	5	8

Es soll mit Hilfe des A*-Algorithmus die kürzeste Zugfolge gefunden werden, die die Start- in die Zielkonfiguration überführt. Als Bewertungsfunktion soll verwendet werden:

- für die bisherigen Kosten vom Start: Anzahl der Züge
- als heuristische Funktion: Entfernungssumme der Spielsteine

Die Entfernungssumme der Spielsteine ist die Summe der Entfernungen aller Spielsteine von ihrer Zielposition, wobei die Lücke nicht mit aufsummiert wird. Die Entfernung eines einzelnen Spielsteins von seiner Zielposition wird als Summe der Abstände in horizontaler und in vertikaler Richtung berechnet. **Beispiel**:

Beispielkonfiguration

1	5	7
2	8	4
3		6

Entfernungen der Spielsteine

0	1	4
2	1	2
4		1

Entfernungssumme: 15

Erstellen Sie den sich ergebenden A*-Suchbaum ausgehend von der oben stehenden Startanordnung. Beachten Sie dabei:

- es muss für jeden Knoten die Berechnung der Bewertungsfunktion erkennbar sein
- nummerieren Sie die entstehenden Knoten so, dass die Reihenfolge der Expansion erkennbar ist
- Sie können das leere Feld durch eine 0 darstellen