Karlsruher Institut für Technologie

Studienkolleg

Schriftliche Feststellungsprüfung
Fach: Informatik
Dauer: 3 Stunden
Hilfsmittel: Taschenrechner (ohne Programmteil)

Aufgabe I. Theoretische Informatik (34P)

I.1. Nun ist es doch geschehen! Die Aliens haben endlich Kontakt mit uns aufgenommen, und eine Nachricht gesendet:

#WIR#LIEBEN#MUCHO#ABBA#UND#ACDC!

a. Wie viel Speicherplatz benötigt diese Nachricht, wenn diese Zeichen (auf der Erde ☺) in *Unicode* gespeichert werden?

_____

b. Berechnen Sie die Redundanz (nach Shannon) in dieser Nachricht (auf Zeichenebene)[1]

_____

c. Die Kanalkapazität eines typischen Ethernet-Übertragungskanals beträgt 100 Mbit/s. Wie viel Zeit würde für die Übertragung dieser Nachricht (s.o.) benötigt, wenn sie in ASCII kodiert wäre?

_____

d. Ein Hund transportiert 10 externe Festplatten (Speicherkapazität: 2 TB pro Festplatte) mit einer Geschwindigkeit von 20 km/h. Wie groß ist die Kanalkapazität des Hundes in MBit/s, wenn er die Festplatten über eine Strecke von 10km transportieren muss?

_____

Voraussetzung der Nachrichtenübertragung ist nach Shannon die Existenz eines *Signals*.
e. Definieren Sie den Begriff *Signal*.

_____

_____

I.2.a. Bilden Sie folgende Zahlen im beschriebenen Zahlensystem ab (Ziffern: 0,1,2,3,4,5,6,7,8,9,A,B,C, ...):

$(101102101102101102)_6$ =>(?)$_{36}$ _____

$(101102101102101102)_{32}$ =>(?)$_{64}$ _____

$(101102101102101102)_4$ =>(?)$_{32}$ _____

[1] Die nach Shannon definierte Redundanz kann berechnet werden, indem man vom theoretischen maximalen Informationsbetrag (= Entropie) den durchschnittlichen Informationsbetrag subtrahiert.

I.2.b. Berechnen Sie:

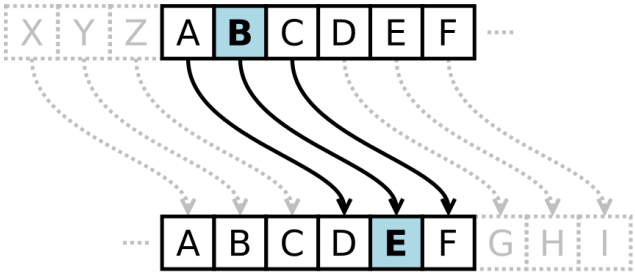
$(4321)_6 + (1234)_6 = (?)_{36}$ _____

$(127)_{10}$ XOR $(31)_{10}$ =>(?)$_{10}$ _____

$(64)_{10}$ NOR $(64)_{10}$ =>(?)$_{10}$ _____

I.3.

Bei der sogenannten Caesar-Verschlüsselung wird jeder Buchstabe des Klartexts auf einen Geheimtextbuchstaben abgebildet, dies wird als monoalphabetische Substitution bezeichnet. **Beispiel (!):**



a. Übersetzen Sie den mittels monoalphabetischer Substitution verschlüsselten Geheimtext in Klartext:

AUZESYAFXG

b. Eine Weiterentwicklung dieser Methode war die polyalphabetische Substitution nach Vigenère[2]. Mit dieser Methode wurde es möglich, Schlüsselwörter zu verwenden.
Übersetzen Sie den nach Vigenère verschlüsselten Geheimtext in Klartext (das Schlüsselwort ist *DIENSTAG*):

IXWPZKILWTMPZAEAWM

c. Aus welchem Grund nennt man die Vigenère-Verschlüsselung eine „symmetrische“ Verschlüsselung?

_____

_____

_____

_____

_____

d. Nennen Sie das Problem (Sicherheit?) bei dieser Methode der Verschlüsselung (Vigenère).. (Tipp: dieses Problem tritt bei der asymmetrischen Verschlüsselung nicht auf):

_____

_____

_____

_____

[2] siehe Vigenère-Tafel im Anhang

e. Als Grundlage der asymmetrischen Verschlüsselung dient eine Kombination sogenannter *Einweg-Funktionen*. Welche Funktionen sind das? Nennen (oder beschreiben) Sie sie:

_____

_____

_____

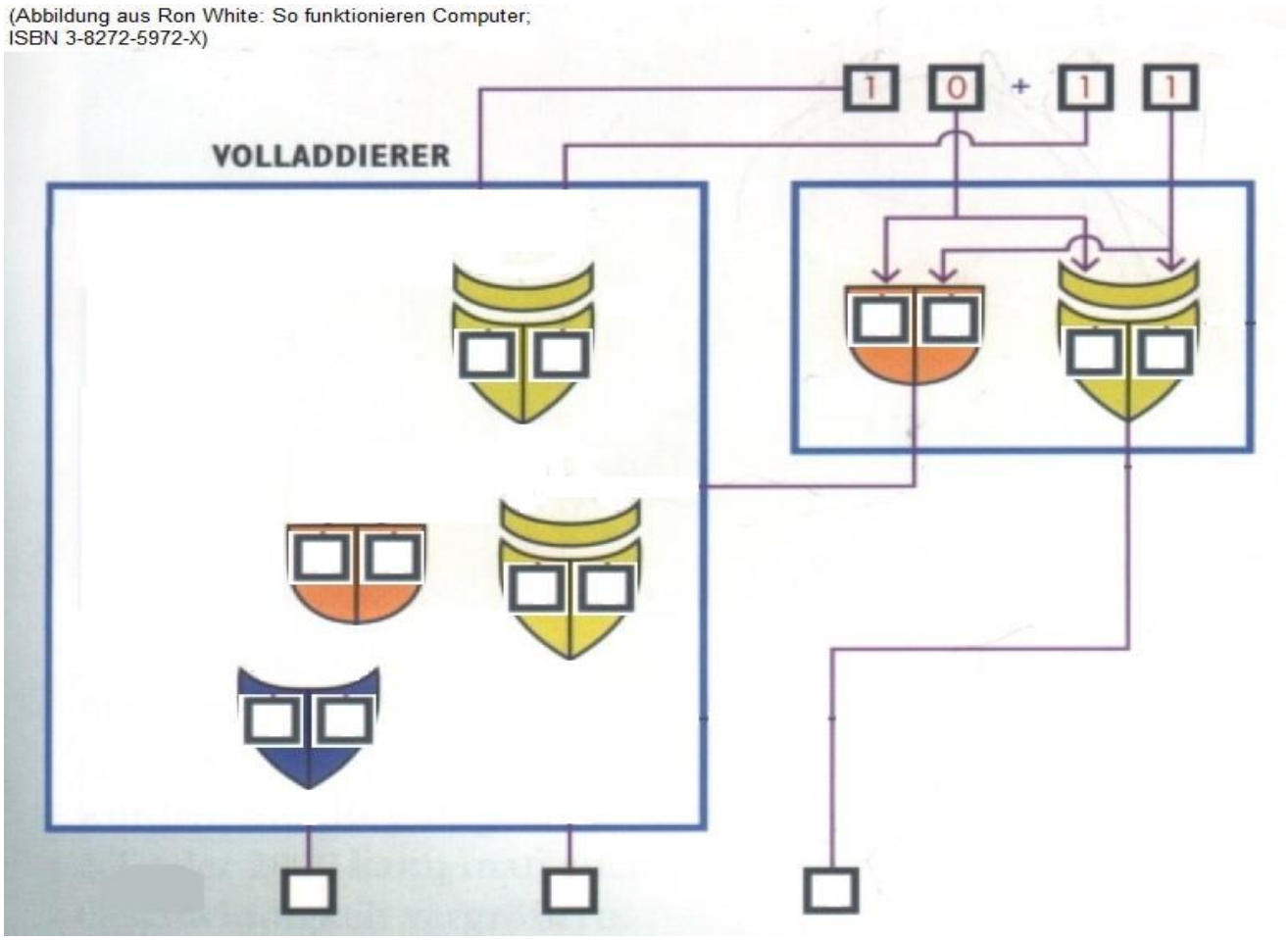
_____

f. In folgender Tabelle sind die Schritte einer asymmetrischen Verschlüsselung dargestellt, wenn Alice an Bob eine geheime Nachricht senden will. Bringen Sie sie durch Angabe von Zahlen/Nummern in die richtige Reihenfolge, und schreiben Sie „f“ oder „falsch“ bei falschen Aktionen.

Aktion/Schritt	**Zahl/Nummer oder „f“ für falsch?**
Bob sendet seinen private key an Alice.	
Alice verschlüsselt ihre Nachricht an Bob mit ihrem public key	
Bob verschlüsselt seinen public key mit Alices private key	
Bob entschlüsselt Alices Nachricht mit seinem private key.	
Alice verschlüsselt ihre Nachricht mit Bobs private key.	
Bob sendet seinen public key an Alice.	
Alice sendet die verschlüsselte Nachricht an Bob.	
Alice verschlüsselt ihre Nachricht an Bob mit Bobs public key.	

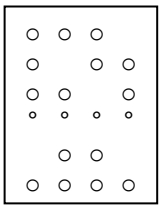
I.4. Unten sehen Sie die unvollständige (!) Abbildung einer logischen Schaltung. Verändern/Ergänzen Sie sie, so dass ein *Volladdierer* daraus wird.

(Abbildung aus Ron White: So funktionieren Computer; ISBN 3-8272-5972-X)



Aufgabe II. Technische Informatik (26P)

II.1. Am 17. Juni 1874 wurde Emile Baudot ein Patent mit dem Titel „System zur schnellen Telegrafie“ erteilt. Seine Erfindung kodierte Zeichen für Telegramme in einem (senkrecht) bitorientierten Lochstreifen mit 5 Zeilen pro Spalte:



<== 1cm==>

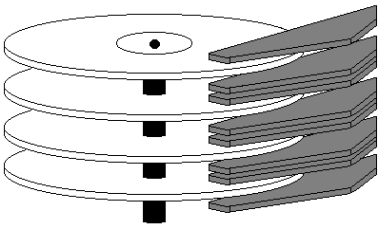
a. Wie viele unterschiedliche Zeichen konnte Baudot damit kodieren/darstellen?

_____

b. Wie lange müsste ein Lochstreifen nach Baudot sein, um 5 MB zu speichern?

_____

II.2. Heutiges Standardspeichermedium ist die sogenannte *Festplatte*.



a. Die nach dem C/H/S-System berechnete Kapazität einer Festplatte ist 72 GB. Sie ist angegeben mit 24 Köpfen und 192 geometrischen Sektoren.
Wie viele Zylinder besitzt sie?

_____

b. Wie viel Speicherplatz ist bei einer Festplatte mit einer Speicherkapazität von 2 TB **nicht** nutzbar, wenn sie mit dem Dateisystem FAT-16 und einer Clustergröße von 64 Sektoren formatiert wird?

_____

c. Wie viel Speicherplatz geht auf dieser Festplatte durch interne Fragmentierung verloren, wenn auf dieser Festplatte ausschließlich Dateien mit einer Größe von 16 KB gespeichert werden, und der (formatierte) Speicherplatz komplett genutzt wird (bis die Festplatte „voll“ ist)?

_____

II.3. Zur Speicherung von Daten auf Festplatten werden verschiedene magnetische Aufzeichnungsverfahren verwendet.
a. Es wird die RLL 2,7-Bitfolge[3] *1001001000000100* gelesen.
(oder *FNNFNNFNNNNNNFNN*, wobei F = Flusswechsel, N = kein Flusswechsel).
Welche Datenbitfolge kann daraus ermittelt werden?

_____

b. Welche Bitfolge würde aus der *Datenbitfolge aus a.)* kodiert nach dem FM-Verfahren entstehen?

_____

c. Wie viele Flusswechsel ergeben sich aus der *Datenbitfolge aus a.)* kodiert nach dem MFM-Verfahren?

_____

[3] siehe RLL-Tabelle im Anhang

d. Was ist ein „Run“?

e. Moderne Festplatten arbeiten nach dem PRML[4]-Aufzeichnungsverfahren. Sie sehen hier die Datenwerte einer Signalfolge (Dreifach-Impuls) des PRML-Verfahrens:

Tabelle 3.7 Datenwerte eines Tri–Impulses.

T		−2	−1	0	1	2	3	4	5
S1		0	0	1	1	0	0	0	0
S2	+	0	0	0	−1	−1	0	0	0
S3	+	0	0	0	0	1	1	0	0
S_T	=	0	0	1	0	0	1	0	0

Welches wäre die Resultierende (*Sr*) eines Vierfach-Impulses?

II.4. Zur Übertragung von Datenpaketen im Internet werden sogenannte IP-Adressen verwendet. Die IPv4-Adressen sind in Klassen (A, B, C …) eingeteilt, und werden in Punktnotation (durch Punkte getrennte Dezimalzahlen) dargestellt.
Wie lautet die *Netzwerkadresse* bei folgenden IP-Adressen:

a. 130.130.130.130

b. 210.210.210.210

c. 120.120.120.120

d. Eine andere Einteilung der IPv4-Adressen kann durch CIDR[5] erreicht werden.
Wie lautet die korrekte Schreibweise des Netzwerks nach CIDR, wenn ein Rechner die IP-Adresse 192.168.0.1 besitzt, und das Netzwerk 64 mögliche Hosts erlaubt?

CIDR:

e. Wie lautet die Subnetzmaske des *Netzwerks aus d.* (in Punktnotation)?

Subnetzmaske:

[4]Partial Response Maximum Likelihood
[5]Classless Inter-Domain Routing

ANHANG:

Vigenère-Tafel zur polyalphabetischen Substitution

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Tabelle RLL 2,7:

Daten	RLL-Code
10	0100
11	1000
011	001000
010	100100
000	000100
0010	00100100
0011	00001000