

Systeme II

- Probeklausur -



Albert-Ludwigs-Universität Freiburg
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

Arne Vater
Sommersemester 2006
02.08.2006



1. Probeklausur

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelbauer

1. Probeklausur

Systeme II

vom

20.07.2006

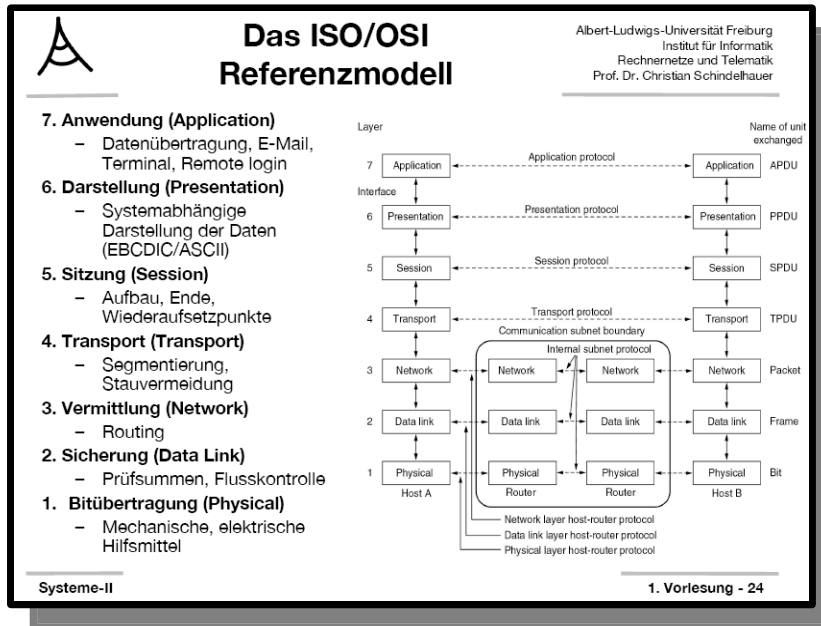


Aufgabe 1

➤ vgl. 1. Vorlesung, Folie 24

Aufgabe 1

Tragen Sie die Bezeichnung der Schichten des ISO/OSI-Modells in die untenstehende Tabelle ein und erläutern Sie in Stichworten deren Aufgaben!



1:	
2:	
3:	
4:	
5:	
6:	
7:	

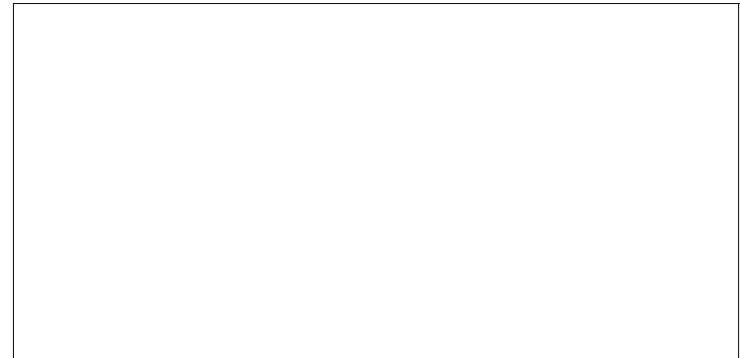


Aufgabe 2

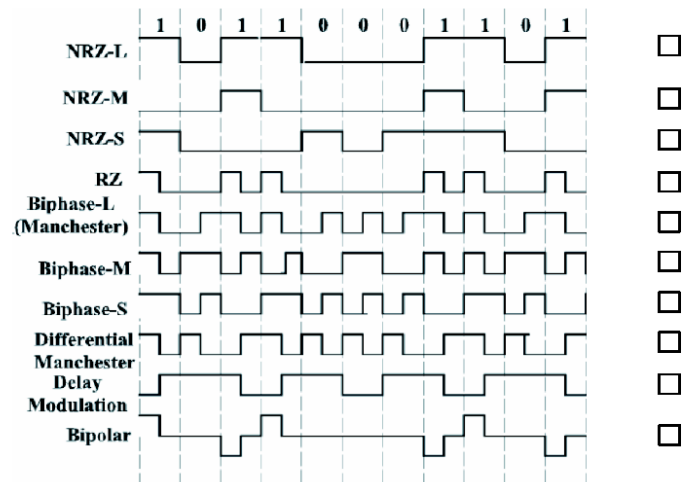
- **Bei Selbsttaktung beinhaltet das Übertragungssignal (implizit) die notwendigen Informationen zur Synchronisation.**
 - Jedes Symbol $\{0,1\}$ wird stets durch eine Signaländerung codiert.
 - Ausnahme Delay Modulation: mindestens jedes zweite Symbol
 - Signaländerung dient gleichzeitig zur Synchronisation.
- **Für die Dauer eines Taktes wird auf die Synchronität der Uhren von Sender und Empfänger vertraut**

Aufgabe 2

Wie funktioniert Selbsttaktung?



Kreuzen Sie alle selbsttaktende Protokolle an!



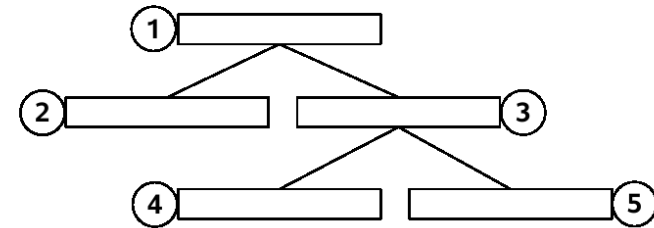


Aufgabe 3

➤ vgl. 7. Vorlesung, Folie 7

Aufgabe 3

Tragen Sie die verschiedenen Ansätze zur Fehlerkontrolle in passender Zuordnung in das Diagramm ein. Erläutern Sie kurz (max. ein Satz) die einzelnen Begriffe!




1:

2:

3:

4:

5:



Fehlerkontrolle

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelbauer

- **Zumeist gefordert von der Vermittlungsschicht**
 - Mit Hilfe der Frames
- **Fehlererkennung**
 - Gibt es fehlerhaft übertragene Bits
- **Fehlerkorrektur**
 - Behebung von Bitfehlern
 - Vorwärtsfehlerkorrektur (Forward Error Correction)
 - Verwendung von redundanter Kodierung, die es ermöglicht Fehler ohne zusätzliche Übertragungen zu beheben
 - Rückwärtsfehlerkorrektur (Backward Error Correction)
 - Nach Erkennen eines Fehlers, wird durch weitere Kommunikation der Fehler behoben

Fehlerkontrolle

Fehlererkennung Fehlerkorrektur

 Vorwärtsfehlerkorrektur Rückwärtsfehlerkorrektur

Systeme-II 7. Vorlesung - 7



Aufgabe 4

➤ es gilt:

$$\sin(a+b) = \sin(a) * \cos(b) + \cos(a) * \sin(b)$$

Matrikelnummer: _____

20.07.2006

Aufgabe 4

Stellen Sie die Funktion $s(t) = A \sin(2\pi ft + \phi)$ als

$$s(t) = a_1 \sin(b_1 t) + a_2 \cos(b_2 t)$$

dar, indem Sie die Koeffizienten von a_1, a_2, b_1, b_2 in Abhängigkeit von A, f und ϕ bestimmen.



Aufgabe 5

➤ CRC berechnen:

- Eingabe um [Grad des Generator-Polynoms] Stellen mit 0 ergänzen.
- Ergänzte Eingabe durch das Generator-Polynom dividieren.
- Rest = Kontrollsumme

Systeme II SS 2006

I. Probeklausur

Aufgabe 5

Berechnen Sie mittels CRC eine 4-Bit-Kontrollsumme der Eingabe

0101.1011.1101.0010

Das Generatorpolynom sei $x^5 + x^4 + x^2 + 1$.

Bestimmen Sie nun eine weitere Eingabe, die mit 1 beginnt und gleiche Länge hat, mit der gleichen Kontrollsumme.



2. Probeklausur

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelbauer

2. Probeklausur

Systeme II

vom

27.07.2006



Aufgabe 1

➤ TCP ist verbindungsorientiert

- Bevor es zum Datenaustausch kommt verständigen sich Sender und Empfänger darüber.

➤ TCP ist zuverlässig

- Pakete werden garantiert und in ursprünglicher Reihenfolge beim Empfänger an die Applikation geliefert.

➤ TCP ist fair

- Ein Algorithmus zur Bandweitenallokation (AIMD) ermöglicht eine (annähernd) gleiche Verteilung der Bandbreite auf aller Nutzer.

➤ TCP ist Paketorientiert

- Daten werden in Pakete unterteilt und verschickt. Vgl. auch Zuverlässigkeit.

Aufgabe 1

Charakterisieren und erläutern Sie die Unterschiede von TCP und UDP anhand der folgenden Begriffe:

- Verbindungsorientierung
- Zuverlässigkeit
- Fairness
- Datenstrom / Pakete

➤ UDP hingegen arbeitet

- verbindungslos,
- unzuverlässig,
- ohne Rücksicht auf die Bandbreite,
- mit Datenströmen statt Paketen, also insb. ohne Acknowledgements.



Aufgabe 2

Aufgabe 2

In einem Distance-Vector-Routing-Protokoll erhält Router B von den Nachbarn A und C die folgenden Tabellen T_A und T_B , wobei $T_x(y, z) = w(x, y) + \delta(y, z)$ den kürzesten Weg von x nach z über y beschreibt.

T_A von A	über B	über F
nach B	1	4
nach C	2	5
nach D	8	6
nach E	6	5
nach F	5	3

T_C von C	über B	über D
nach A	2	8
nach B	1	9
nach D	8	2
nach E	6	4
nach F	5	5

Bestimmen Sie aus diesen Tabellen die Distance-Vector-Tabelle von B .

T_B von B	über	über
nach		
nach		
nach		
nach		
nach		

Diese Distance-Vector-Tabellen werden sich in Zukunft ändern. Woraus kann man dies schlussfolgern? Begründen Sie!



Aufgabe 2

Nennen Sie ein Protokoll, bei dem das Count-to-Infinity Problem auftreten kann.

Erläutern Sie das Count-to-Infinity Problem! Zeigen Sie auch ein Beispiel mit mindestens drei Knoten.



Aufgabe 3

➤ Kryptographische Hashfunktionen

- Erzeugen zu beliebiger Eingabe einen Code (Hashwert), sodass kein anderer Text gefunden werden kann, der den selben Code hat.
- Mittels des Hashcodes kann geprüft werden, ob ein vorliegender Text dem Originaltext entspricht.

➤ Beispiele für Kryptographie

- vgl. 21. Vorlesung, Folie 2

**Verschlüsselungs-
methoden**

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Symmetrische Verschlüsselungsverfahren**
 - z.B. Cäsars Code
 - Enigma
 - DES (Digital Encryption Standard)
 - AES (Advanced Encryption Standard)
- **Kryptografische Hash-Funktion**
 - SHA-1, SHA-2, MD5
- **Asymmetrische Verschlüsselungsverfahren**
 - RSA (Rivest, Shamir, Adleman)
 - Diffie-Helman
- **Digitale Unterschriften (Elektronische Signature)**
 - PGP (Phil Zimmermann), RSA

Systeme-II 21. Vorlesung - 2

Aufgabe 3

Kreuzen Sie für die Bedrohungen *Verleugnung der Kommunikation* und *Fälschen von Information* alle betroffenen Sicherheitsziele an!

Sicherheitsziele	Bedrohungen						
	Maskierung	Abhören	Zugriffsverletzung	Verlust oder Veränderung (übertragener) information	Verleugnung der Kommunikation	Fälschen von Information	Sabotage (z.B. Überlast)
Vertraulichkeit	X	X	X				
Datenintegrität	X		X	X			
Verantwortlichkeit	X		X				
Verfügbarkeit	X		X	X			X
Zugriffskontrolle	X		X				

Welche Aufgabe haben kryptographische Hash-Funktionen?

Nennen Sie jeweils ein Beispiel für:

- ein symmetrisches Verschlüsselungsverfahren

- ein asymmetrisches Verschlüsselungsverfahren

- eine kryptographische Hashfunktion

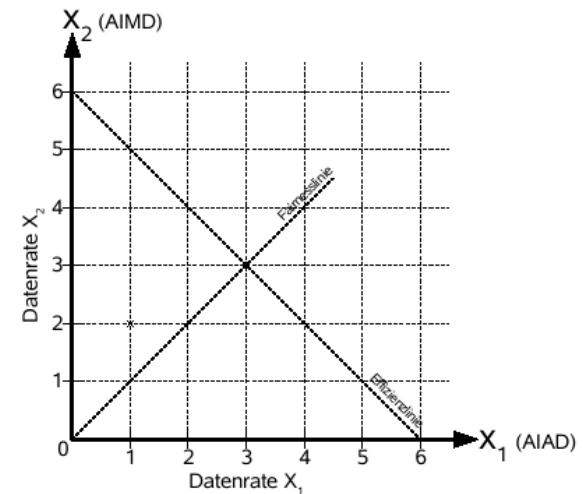
- ein Verfahren für digitale Unterschriften



Aufgabe 4

Aufgabe 4

Zeichnen Sie in das folgende Diagramm den Verlauf einer Datenratenanpassung, wenn Teilnehmer X_1 AIAD (additively increase / additively decrease) und Teilnehmer X_2 AIMD (additively increase / multiplicative decrease) benutzt. Beginnen Sie dabei im Punkt (1; 2) und gehen Sie davon aus, dass die Teilnehmer synchron agieren und dass die additive Datenratenänderung immer in Einerschritten erfolgt, während bei der multiplikativen Änderung die Datenrate halbiert wird. Tragen Sie in der untenen Tabelle ebenfalls für die ersten 10 Runden die Werte (Punkte) der Datenraten von X_1 und X_2 ein.



Runde	Punkt(X_1, X_2)	Runde	Punkt(X_1, X_2)
0	(1; 2)	6	
1		7	
2		8	
3		9	
4		10	
5	

Schon nach Runden (Erhöhung *oder* Verringerung) ist der optimale Punkt (3; 3) erreicht.

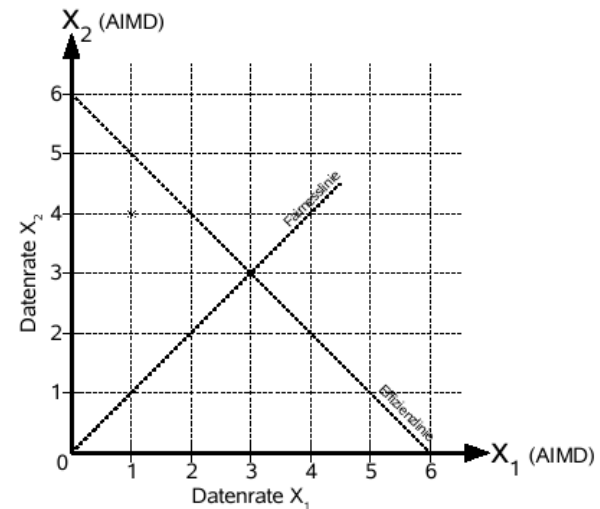


Aufgabe 4

- Ist einmal ein Punkt der Fairnesslinie erreicht, müssen beide Teilnehmer in jeder Runde stets das gleiche machen. Andernfalls würde die Fairnesslinie wieder verlassen werden.

Warum kann bei einer Kombination unterschiedlicher Verfahren bei den Teilnehmern keine faire Datenratenverteilung aufrecht erhalten werden?

Zeichnen Sie nun den Datenratenverlauf, wenn beide Teilnehmer AIMD benutzen, ausgehend vom Punkt (1; 4). Tragen Sie in der unteren Tabelle ebenfalls für die ersten 10 Runden die Werte (Punkte) der Datenraten von X_1 und X_2 ein.



Runde	Punkt(X_1, X_2)	Runde	Punkt(X_1, X_2)
0	(1; 4)	6	
1		7	
2		8	
3		9	
4		10	
5	



“Implizite” Aufgaben

➤ werden nach folgendem Verfahren in die Gesamtpunktzahl eingerechnet

➤ Fall A:

- richtige Antwort: $n = 1$ Punkt
- falsche Antwort: $n = 0$ Punkte
- Alle insgesamt erreichten Punkte werden mit n multipliziert.

➤ Fall B:

- richtige Antwort: $m_i = 1$ Punkt
- falsche Antwort: $m_i = 0$ Punkte
- Alle auf dem zugehörigen Zettel erreichten Punkte A_i werden mit m_i multipliziert.

➤ Gesamtpunktzahl $G = n \cdot \sum_i A_i \cdot m_i$

Prof. Dr. Christian Schindelhauer

Freiburg i. Br., den 20.07.2006

1. Probeklausur

in

Systeme II

A

Name :

Matrikelnummer :

Punkteverteilung (bitte freilassen!)

Aufgabe 1		von 5
Aufgabe 2		von 10
Aufgabe 3		von 5

B

Matrikelnummer: _____ 20.07.2006

Aufgabe 2



➤ Rückgabe der Probeklausuren

- jetzt gleich im Anschluss
- getrennt für 1. und 2. Probeklausur
- wegen akuten Namenmangels auf den Klausuren
 - nennt jeder seine Klausurnummer
 - hat dafür genau einen Versuch (pro Klausur)!

➤ Abschlussveranstaltung

- wann: jetzt
- wo: draußen
- Kulinarisches:
 - Getränke nach Bestellung
 - Speisen durch Selbstversorgung



Ende!



Albert-Ludwigs-Universität Freiburg
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

Systeme II
Arne Vater