

2. Probeklausur

in

Systeme II

Name :

Matrikelnummer :

Punkteverteilung (bitte freilassen!)

Aufgabe 1		von 8
Aufgabe 2		von 15
Aufgabe 3		von 7
Aufgabe 4		von 15
Summe		von 45

Die Klausur besteht aus 4 Aufgaben und 7 Seiten. Insgesamt können 45 Punkte erreicht werden. Bitte schreiben Sie auf jedes Blatt Ihre Matrikelnummer.

Bei Multiple-Choice-Aufgaben werden für jede falsch angekreuzte Antwort so viele Punkte abgezogen, wie es für eine richtige Antwort gibt. Einzelne Aufgaben werden mit mindestens 0 Punkten bewertet.

Zugelassene Hilfsmittel: Keine! Insbesondere keine schriftlichen Unterlagen oder elektronischen Geräte.

Schreiben Sie Ihre Lösung bitte in die vorgesehenen Platzhalter. Sollte der Platz nicht ausreichen, erhalten Sie auf Anfrage weiteres Papier.

Aufgabe 1

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

- Verbindungsorientierung
- Zuverlässigkeit
- Fairness
- Datenstrom / Pakete



Aufgabe 2

In einem Distance-Vector-Routing-Protokoll erhält Router B von den Nachbarn A und C die folgenden Tabellen T_A und T_C , 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		

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

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

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

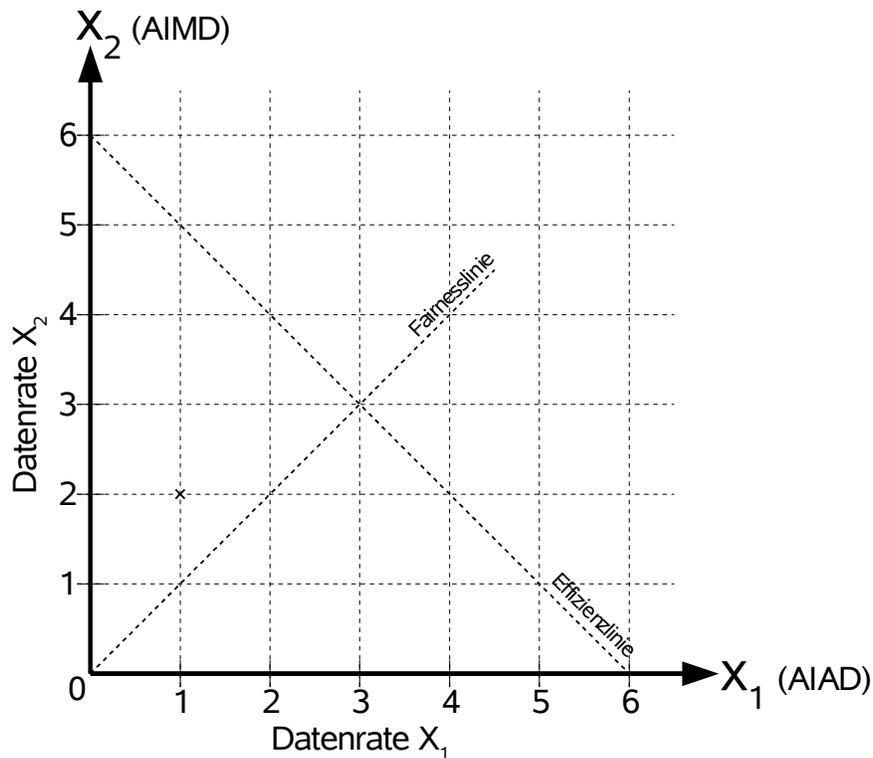
- ein asymmetrisches Verschlüsselungsverfahren

- eine kryptographische Hashfunktion

- ein Verfahren für digitale Unterschriften

Aufgabe 4

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 unteren Tabelle ebenfalls für die ersten 10 Runden die Werte (Punkte) der Datenraten von X_1 und X_2 ein.

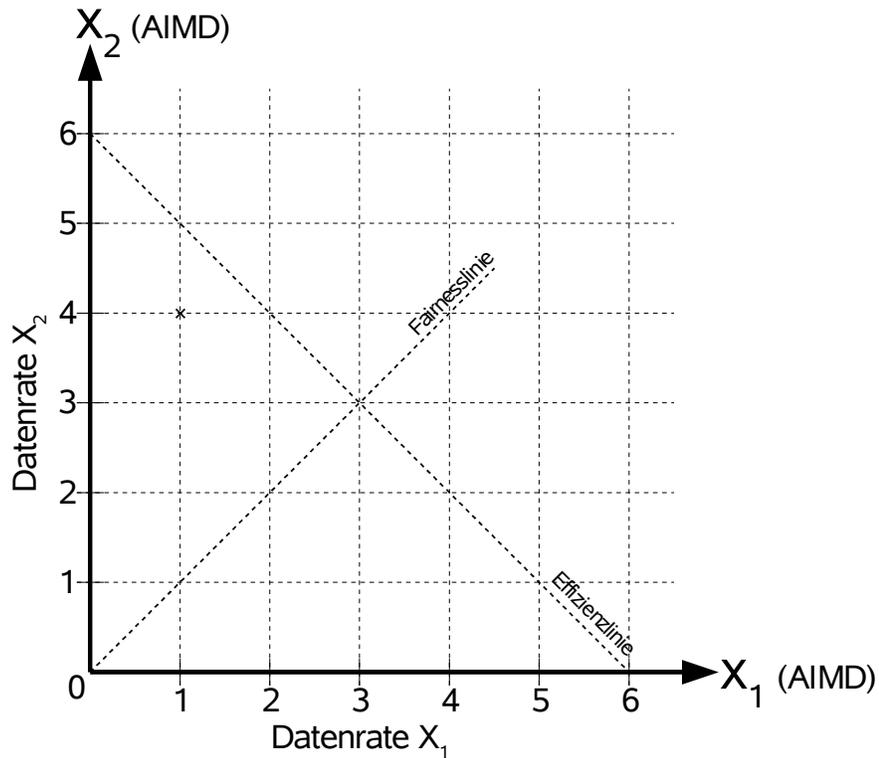


Runde	Punkt(X_1, X_2)	Runde	Punkt(X_1, X_2)
0	(1; 2)	6	
1		7	
2		8	
3		9	
4		10	
5	

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

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	