GSS Gedächtnisprotokoll 24.07.2012

Teil 1: Lamersdorf

Aufgabe 1: Echtzeit-Scheduling [18 P.]

Auftrag	P_1	P_2	P_3	P_4
Periodendauer	4	6	12	8
Bedienzeitanforderung	1	2	3	1

a) [2 P.] Leiten Sie mathematisch her, ob es mit einem idealen Scheduler möglich ist, die Deadlines aller Aufträge einzuhalten.

b) [2 P.] Leiten Sie mathematisch her, ob es mit einem RMS Scheduler möglich ist, die Deadlines aller Aufträge einzuhalten.

c) [6 P.] Illustrieren Sie für das Intervall $t \in [0, 24]$ die Ausführungsreihenfolge mit RMS.

d) [6 P.] Illustrieren Sie für das Intervall $t \in [0, 24]$ die Ausführungsreihenfolge mit EDF.

Aufgabe 2: Prioritätsinversion [10 P.]

Auftrag	P_1	P_2	P_3
Periodendauer	25	20	100
Bedienzeitanforderung	5	10	20

Welche zwei Aufträge müssten sich mittels einer Semaphore eine Ressource teilen, damit es bei $t = 50$ zu einer Prioritätsinversion kommt? Illustrieren Sie die Ausführungsreihenfolge.

Aufgabe 3: Semaphoren [10 P.]

Gegeben sei folgende (unvollständige) Klasse:

```
public class Verwalter {

	private List<Ware> _waren;

	public Verwalter() {
		_waren = new ArrayList<Ware>();
	}

	public void preiseAnpassen() {
		for (Ware ware : _waren) {
			ware.justierePreis();
	}
}
```

Das Ziel ist es, jede Preisänderung von allen Waren atomar zu gestalten.

a) Sie finden heraus, dass es so etwas wie Semaphoren mit den Methoden `P()` und `V()` gibt. Mit welchem Wert müsste die Semaphore initialisiert werden?

b) Wie müsste der Quelltext geändert werden, wenn in der Klasse eine Semaphore `sem` zur Verfügung steht?

c) Das Programm stürzt direkt ab. Welchen Fehler wurde gemacht, der mit Monitoring nicht passiert wäre?

d) Sie finden das Konzept des Monitorings und passen Ihre Klasse Ware wie folgt an

```
public class Ware {

      ...

      public synchronized void justierePreis() {
            // Preis wird justiert
      }
}
```

Führt das zum gewünschten Ergebnis? Wenn nein, was könnte man besser machen?

Aufgabe 4: Paging [14 P.]

Spalte	P/A-Bit	Frame	$t_{geladen}$	$t_{zuletzt}$	Zugriffe	Referenziert	Modifiziert
13	0	0x6	?	?	?	0	1
14	1	0x8	?	?	?	1	1
15	0	0xA	?	?	?	0	0
16	1	0xC	?	?	?	0	0
17	1	0xE	?	?	?	0	0
18	1	0x4	?	?	?	0	0

Die virtuelle Adresse ist 16 Bit lang, die physikalische 12 Bit. Eine Seite ist 256 Byte groß.

a) [2 P.] Wie viele Einträge passen in die Tabelle?

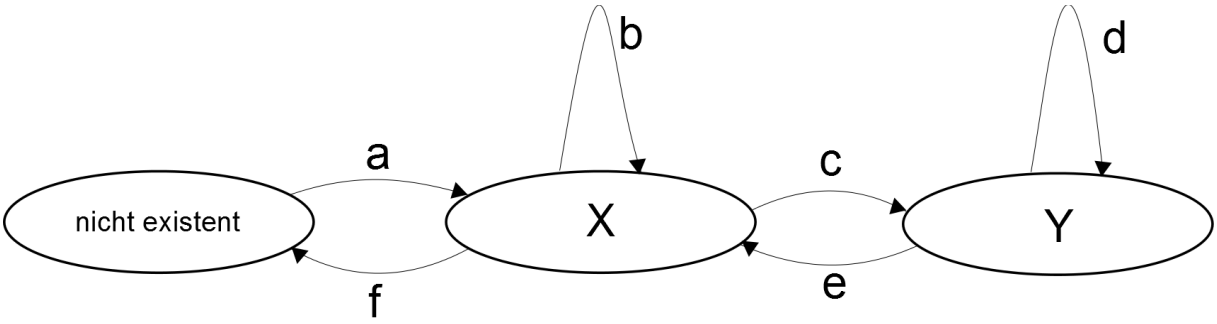
b) [4 P.] Wandeln Sie die folgenden virtuellen Adressen in physikalische Adressen um.

i) 0x0CEA
ii) 0x122C
iii) 0x10AB
iv) 0x0F99

c) [8 P.] Die Seite, die in Spalte 13 steht, soll geladen werden, allerdings gibt es keinen freien Pageframe. Welche Seite müsste ersetzt werden nach FIFO, LRU, NRU, LFU?

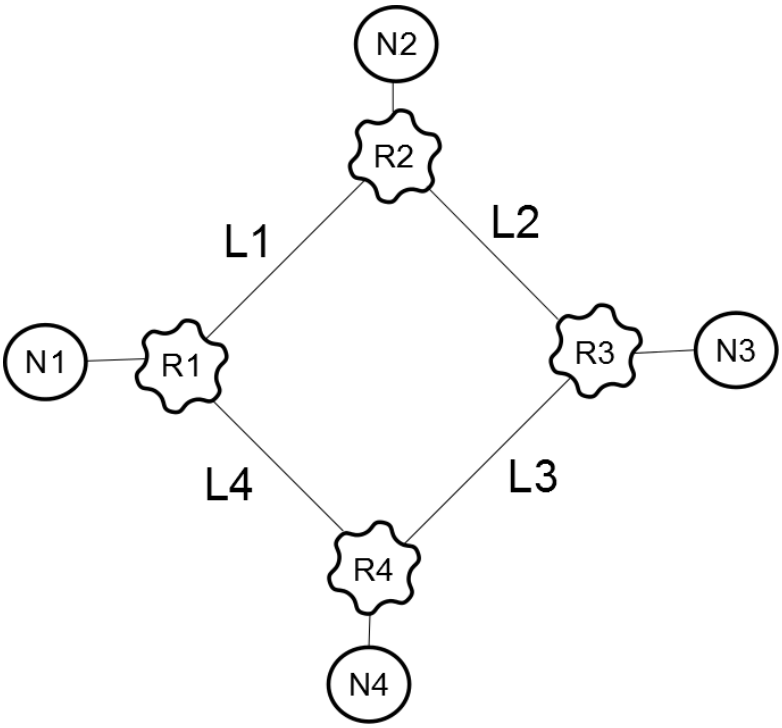
Aufgabe 5: Dateisysteme [10 P.]

a) [4 P.] Beschriften Sie im Bild die Zustände X und Y und die Zustandsübergänge a bis f.



b) [6 P.] Beschreiben Sie die drei Schichten des Dateiverwaltungssystems (oder so ähnlich).

Aufgabe 6: Routing [10 P.]



a) [4 P.] Geben Sie die stabilen Tabellen an. Folgendes ist vorgegeben:

Für R1			Für R2			Für R3			Für R4		
Z	L	K	Z	L	K	Z	L	K	Z	L	K
N_1			N_1			N_1	L_3		N_1		
N_2			N_2			N_2			N_2	L_4	
N_3	L_1		N_3			N_3			N_3		
N_4			N_4	L_2		N_4			N_4		

b) Leitung 4 fällt aus. Geben Sie die Tabellen nach der ersten Phase an, also wenn sich nichts mehr ändert.

c) In a) war von jedem Knoten aus jeder andere Knoten erreichbar. Ist dies nach b) der Fall? Wenn nein, was müsste noch getan werden?

Aufgabe 7: Agenten [8 P.]

a) [4 P.] Nennen Sie vier Eigenschaften von Software Agenten (außer autonom).

b) [4 P.] Was bedeutet autonom im Kontext von Software Agenten?

Teil 2: Federrath

Aufgabe 1: Angreifermodell [4 P.]

a) [2 P.] Was ist der Sinn des Angreifermodells?

b) [2 P.] Welche Aspekte beschreibt es?

Aufgabe 2: Passwörter [4 P.]

In Ihrem System bestehen Passwörter aus fünf Zeichen, wobei ein Zeichen ein Großbuchstabe, Kleinbuchstabe oder eine Ziffer sein kann.

a) [2 P.] Wie viele verschiedene Passwörter gibt es?

b) [2 P.] Zusätzlich soll mindestens eins der Zeichen ein Sonderzeichen sein, es gibt dabei zehn Sonderzeichen zur Auswahl. Wie viele verschiedene Passwörter gibt es?

Aufgabe 3: Kryptographie [4 P.]

a) [2 P.] Was ist der Hauptunterschied zwischen symmetrischen und asymmetrischen Verfahren?

b) [2 P.] Nennen Sie Vor- und Nachteile der symmetrischen gegenüber der asymmetrischen Verfahren.

Aufgabe 4: Rainbow Tables [4 P.]

a) [2 P.] Was ist der Zweck einer Rainbow Table?

b) [2 P.] Worin liegt der Vorteil der Rainbow Tables gegenüber einem Brute-Force-Angriff?

Aufgabe 5: iTAN [12 P.]

a) [2 P.] Wie bezeichnet man allgemein solche Authentisierungsprotokolle wie iTAN?

b) [10 P.] Skizzieren Sie einen Man-in-the-middle-Angriff bei einem iTAN-Verfahren zwischen Kunde und Bank.

Aufgabe 6: RSA [8 P.]

Alice und Bob senden sich verschlüsselt Würfelergebnisse zu.
Für Alice gibt es folgende Werte: $e_A = 3, p_A = 5, q_A = 11, d_A = 27$.
Für Bob gibt es folgende Werte: $e_B = 3, p_B = 17, q_B = 5, d_B = 43$.

Bob sendet Alice sein Würfelergebnis $c_B = 9$

Zeigen Sie, dass es Eve möglich ist mit einem Chosen-Plaintext-Angriff und nur mit dem Wissen von c_B und den öffentlichen Schlüsseln von beiden das Ergebnis zu entschlüsseln.