FernUniversität
Gesamthochschule in Hagen

Fachbereich Informatik

Lehrgebiet Praktische Informatik VI
Prof. Dr. Jörg M. Haake

FernUniversität - Gesamthochschule D-58084 Hagen

Informatikzentrum
Universitätsstr. 1
D-58084 Hagen

Vorname Name _____

Straße Hausnr. _____

PLZ Ort _____

Klausur zum Kurs

Verteilte Systeme (1678)

am 5. März 2005

Klausurort:	
Vorname Name:	
Matrikelnummer:	

Aufgabe	1	2	3	4	5	6	7	8	Summe
Punkte	10	15	16	13	12	12	10	12	100
bearbeitet									
erreichte Punkte									

Hinweise zur Bearbeitung der Klausur zum Kurs Verteilte Systeme 1678

Wir begrüßen Sie zur Klausur *Verteilte Systeme* und bitten Sie, diese Hinweise vollständig und aufmerksam durchzulesen, bevor Sie mit der Bearbeitung der Aufgaben beginnen.

1. Prüfen Sie bitte die Vollständigkeit dieser Unterlagen:
   - Deckblatt
   - diese Hinweise und 8 Aufgaben auf den Seiten 1 bis 9
   - eine Teilnahmebestätigung zur Vorlage beim Finanzamt
2. Bevor Sie mit der Bearbeitung der Aufgaben beginnen, tragen Sie bitte auf dem Deckblatt Name, Anschrift und Matrikelnummer ein.
3. Falls Sie eine Teilnahmebestätigung wünschen, füllen Sie diese bitte aus.
4. Schreiben Sie Ihre Lösungen bitte auf die Aufgabenblätter bzw. die dafür vorgesehenen Leerseiten (benutzen Sie auch die Rückseiten, wenn der Platz nicht reicht).
5. Auf jedes Blatt, auf dem sich Teile Ihrer Lösung befinden, schreiben Sie bitte oben Ihren Namen und Ihre Matrikelnummer.
6. Wenn Sie eine Prozedur oder ein Programm schreiben sollen, achten Sie auf eine klare Gliederung und eine *ausführliche* Kommentierung.
7. Wenn Sie Zahlenwerte ausrechnen sollen, skizzieren Sie auch den Rechenweg.
8. Es sind keine Hilfsmittel zugelassen.
9. Zum Bestehen der Klausur reichen 50 von 100 Punkten auf jeden Fall aus.

Wir wünschen Ihnen bei der Bearbeitung der Klausur viel Erfolg!

Aufgabe 1: **Kommunikation** **10 Punkte**

Sie erhalten den Auftrag, einen Internet-Radiosender zu realisieren. Welches Transportprotokoll würden Sie wählen? Begründen Sie Ihre Entscheidung und nennen Sie die Nachteile der von ihnen nicht gewählten Transportprotokolle.

Aufgabe 2: **Zeit** **15 Punkte**

Es seien 4 Prozesse mit den Prozessnummern 0, 1, 2, 3 gegeben. Die Prozesse laufen auf verschiedenen Rechnern, die jeweils über eine Uhr verfügen. Die Uhren laufen mit unterschiedlichen aber konstanten Raten, die in Abbildung 1 angegeben sind. Die Prozesse tauschen miteinander Nachrichten aus.

1. Tragen Sie die Werte der Uhren mit Korrektur durch den Algorithmus von Lamport ein.
2. Sind folgende Ereignisse nebenläufig? Wenn nicht, wie stehen sie bezüglich der Relation $\longrightarrow$ zueinander?
   - b und d
   - b und c
   - b und e

   Nehmen Sie dabei an, dass die Zeitpunkte noch nicht um eine Prozessnummer erweitert sind.
3. Die Zeitpunkte sind jetzt durch eine Prozessnummer erweitert. Ordnen Sie die Ereignisse a, b, c, d und e in der richtigen Reihenfolge ein.

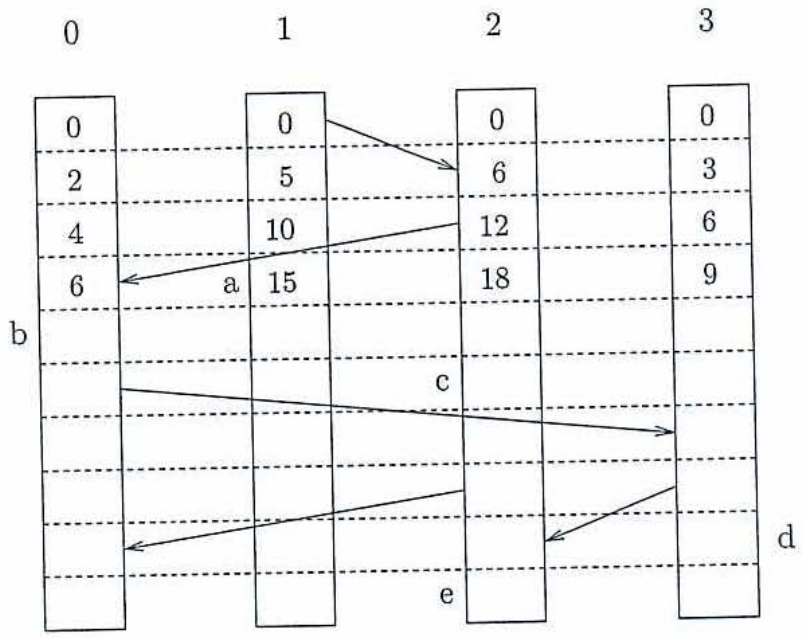

Abbildung 1: Nachrichtenaustausch zwischen den Prozessen 0, 1, 2, 3.

Aufgabe 3: **Client-Server/Threads** **16 Punkte**

Wir betrachten einen Web-Server. Es kommen Anfragen für Seiten hinein und die angeforderten Seiten werden an die Clients zurückgesendet.
Auf einige Seiten wird viel häufiger zugegriffen als auf andere Seiten. Web-Server nutzen diese Tatsache aus, um die Performance dadurch zu verbessern, dass sie eine Sammlung von stark frequentierten Seiten im Hauptspeicher bereithalten (Cache), damit diese Seiten nicht von der Festplatte geholt werden müssen.

1. Wenn eine Anfrage zu einer Seite ankommt, überprüft der Web-Server-Prozess zuerst, ob sie zulässig ist. Danach prüft er den Cache, um zu sehen, ob die benötigte Datei dort schon vorhanden ist. Wenn ja, dann wird die Seite direkt vom Cache geholt und sofort zurückgegeben, sagen wir, das ganze dauert insgesamt 500 μs. Wenn die angeforderte Seite nicht im Cache ist, dann ist ein Zugriff auf die Festplatte notwendig, was in der Hälfte der Fälle vorkommen soll, dafür werden zusätzliche 9 ms = 9000 μs benötigt. In dieser Zeit ist der Prozess blockiert.

   Wie viele Anfragen kann der Server durchschnittlich pro Sekunde bearbeiten?

2. Eine alternative Möglichkeit ist, einen Multithreaded-Webserver zu verwenden. Ein Thread bekommt eine Anfrage und überprüft, ob es möglich ist, sie aus dem Cache zu beantworten, auf den alle Threads Zugriff haben. Falls nicht, holt er die Seite von der Platte und blockiert so lange, bis die Übertragung fertig ist. Sobald der Thread blockiert, wird ein anderer Thread zur Ausführung der nächsten Anfrage ausgewählt. Wir nehmen an, dass es genügend Festplatten gibt.

   Wie viele Threads sollte der Multithreaded-Webserver haben, damit die CPU die ganze Zeit beschäftigt ist?

Aufgabe 4: **Sicherheit** **13 Punkte**

Das Übertragen von unverschlüsselten Kennwörtern über nicht abhörsichere Verbindungen stellt ein Sicherheitsrisiko dar. Entwerfen Sie ein Autorisierungsprotokoll, mit dem sich ein Benutzer A beim Host B als autorisiert ausweisen kann, ohne dass sensitive Daten wie Kennwörter oder private Schlüssel übertragen werden müssen. Dieses Protokoll soll das wechselseitige Misstrauen beider Parteien berücksichtigen: Host B will ausschließen, dass sich jemand anderes als Benutzer A ausgibt, und Benutzer A will sicher sein, dass er wirklich mit Host B kommuniziert. Beschreiben Sie die einzelnen Schritte des Protokolls und die notwendigen Voraussetzungen.

Hinweis: Bauen Sie ihr Protokoll auf einem Verfahren mit öffentlichem Schlüssel auf.

Aufgabe 5: **Kryptographie** **12 Punkte**

Sie erhalten die Geheimbotschaft `iiwqysloqdyxxv` und sollen diese entschlüsseln. Sie wissen, dass die Vigenèrechiffre mit dem Schlüssel `def` zur Verschlüsselung verwendet wurde, P und C sind jeweils $\mathbb{Z}_{26}$. Für die Buchstaben wird die Kodierung $(a \to 0, b \to 1, \ldots, z \to 25)$ verwendet.
Wie lautet der Klartext?

Aufgabe 6: **Versionenverwaltung** **12 Punkte**

Erklären Sie die Bedeutung der folgenden CVS-Kommandos jeweils mit ein bis zwei Sätzen.

- `cvs checkout project`
- `cvs add file`
- `cvs commit file`
- `cvs status file`
- `cvs update file`
- `cvs log file`

Aufgabe 7: **Verteilte Dateisysteme** **10 Punkte**

Welche Eigenschaften verschaffen AFS (Andrew File System) eine bessere Skalierbarkeit als NFS (Network File System)? Wo sehen Sie die Grenzen der Skalierbarkeit von AFS?

Aufgabe 8: **CSCW** **12 Punkte**

Wir betrachten das BSCW-System. Welche der folgenden Anforderungen an ein System für vernetzte, kooperative Gruppenarbeit werden von BSCW unterstützt? Wenn ja, wie? Ein bis zwei Sätze sollten jeweils als Antwort ausreichen.

- Bildung einer Gruppe, Einrichtung eines Arbeitsbereichs für die Gruppe, exklusiver Zugriff nur für Gruppenmitglieder
- Ablage von und Zugriff auf Dateien im Arbeitsbereich
- Reservierter, exklusiver Zugriff auf eine bestimmte Datei für ein Gruppenmitglied für eine bestimmte Zeit
- Automatische Benachrichtigungen über Änderungen an den gemeinsamen Dateien
- Rückgriff auf ältere Versionen einer Datei
- Anzeige der Unterschiede von verschiedenen Versionen einer Datei