

**Aufgabe 1:****Client-Server/Threads****7 + 8 Punkte**

Wir betrachten einen Web-Server. Es kommen Anfragen für Seiten hincin 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  $500 \mu\text{s}$ . 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~~  $9 \text{ ms} = 9000 \mu\text{s}$  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~~ **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~~ **genügend Festplatten** gibt.

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

**Aufgabe 2:**

**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 3:**

**Zeit**

**5 + 5 + 5 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  $\rightarrow$  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.

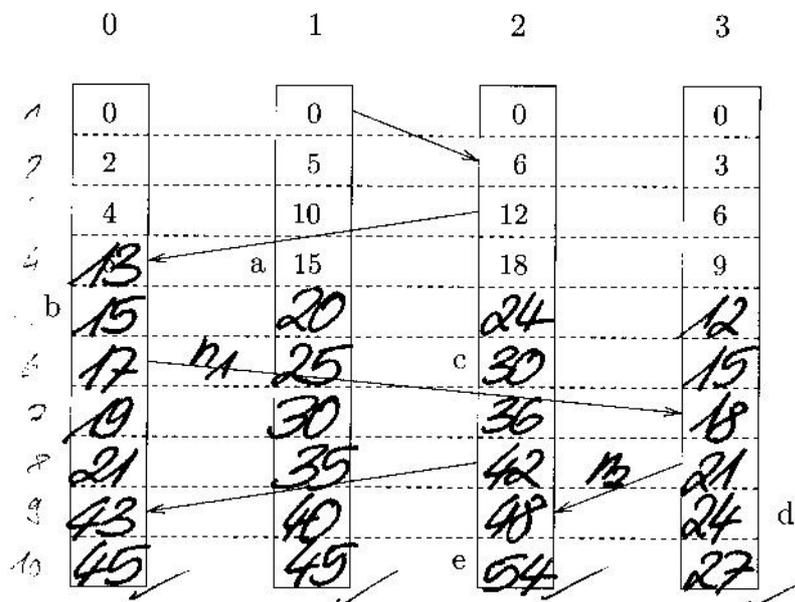


Abbildung 1: Nachrichtenaustausch zwischen den Prozessen 0, 1, 2, 3.

**Aufgabe 4:****Kryptographie****12 Punkte**

Sie erhalten die Geheimbotschaft  $\text{huygkpkqkqvxdp}$  und sollen diese entschlüsseln. Sie wissen, dass die Vigenèrechiffre mit dem Schlüssel  $cde$  zur Verschlüsselung verwendet wurde,  $P$  und  $C$  sind jeweils  $\mathbb{Z}_{26}$ . Für die Buchstaben wird die Kodierung  $a \rightarrow 0, b \rightarrow 1, \dots, z \rightarrow 25$  verwendet.

Wie lautet der Klartext?

**Aufgabe 5:****Sicherheit****12 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 6:**

**Versionsverwaltung**

**12 Punkte**

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

- `cv`s checkout project
- `cv`s add file
- `cv`s commit file
- `cv`s status file
- `cv`s update file
- `cv`s log file

**Aufgabe 7:**

**Verteilte Dateisysteme**

**7 + 5 Punkte**

1. • Beschreiben Sie den **automount**-Mechanismus von NFS. Wie funktioniert er und was sind die Vorteile?
2. • Bei vielen **automount**-Implementierungen werden die importierten Verzeichnisse nicht direkt an der gewünschten Stelle installiert (gemountet), sondern in einem speziellen Verzeichnis, in das dann ein symbolischer Link verweist, warum?

**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.

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