

**Blatt 7**

Kai Großjohann

Abgabe bis 4. Dezember 2002

**Aufgabe 1: Deadlock-Vermeidung mit Zeitstempeln**

Beweise, dass bei der Zeitstempelmethode keine Deadlocks auftreten können.  
Hinweis: Argumentiere mit Hilfe des Wartegraphen.

3 Punkte

**Aufgabe 2: Überlisten von Zugriffsrechten**

Eine statistische Datenbank ist eine Datenbank, die sensitive Einträge enthält, die deswegen nicht einzeln betrachtet werden dürfen, sondern nur über statistische Operationen. Beispielsweise sind die Operationen Summe von Spalten, Durchschnitt von Spalten, und Zählen der Tupel im Ergebnis erlaubt. Man könnte dies für Umfrageergebnisse verwenden.

In diesem Fall existiert das *Inferenzproblem*.

Nimm an, du hast die Erlaubnis, im `select`-Teil einer Anfrage ausschließlich die Operationen `sum` und `count` zu verwenden. Ferner werden Anfragen vom System abgewiesen, die nur ein Tupel der Relation betreffen.

Du möchtest nun das Gehalt eines bestimmten Professors herausfinden, von dem du weißt, dass er ein C4-Prof ist und dass er von allen C4-Profis am meisten verdient. Beschreibe, wie du das System überlistest.

3 Punkte

**Aufgabe 3: Mandatory Access Control**

Im Buch wurde gesagt, dass Leute mit unterschiedlicher Sicherheitsstufe nur schlecht zusammen arbeiten können. Woran liegt das?

Was muss passieren, damit die Zusammenarbeit trotzdem möglich ist? (Das, was hier passiert, ist aufwendig.)

Wie könnte man diesen Aufwand umgehen? Welche Probleme handelt man sich mit dieser Umgehungsmethode ein?

2 Punkte

**Aufgabe 4: Kryptografie**

Es gibt zwei Gruppen von Verschlüsselungsmethoden: die symmetrischen Verschlüsselungsverfahren (zu denen DES gehört), und die asymmetrischen Verfahren (zu denen RSA gehört). Bei den symmetrischen Verfahren werden zur Verschlüsselung und zur Entschlüsselung der gleiche Schlüssel verwendet, bei den asymmetrischen Verfahren gibt es einen Schlüssel zum Verschlüsseln und einen anderen zum Entschlüsseln.

Stelle die Vor- und Nachteile dieser beiden Verfahren gegenüber.

Bei den symmetrischen Verfahren muss ja geheime Information sicher (außerhalb des Verfahrens) übertragen werden, nämlich der Schlüssel. Das ist bei den asymmetrischen Verfahren nicht nötig. Trotzdem gibt es ein Problem bei der Übertragung der Schlüssel. Welches?

2 Punkte