TU München, Fakultät für Informatik
Lehrstuhl III: Datenbanksysteme
Prof. Dr. Thomas Neumann

Übung zur Vorlesung
Einsatz und Realisierung von Datenbanksystemen im SoSe15

Moritz Kaufmann (moritz.kaufmann@tum.de)
http://db.in.tum.de/teaching/ss15/impldb/

Blatt Nr. 3

Hausaufgabe 1 Beim strikten 2PL commit werden die folgende Schritte in angegebener Reihenfolge ausgeführt:

1. Eintragen des commit in den Logbuffer
2. Persistieren des Logbuffer
3. Freigabe aller Sperren
4. Rückmeldung an den Benutzer

Manche Datenbanksysteme führen Schritt 3 als ersten Schritt aus. Was kann dies für Vorteile bringen? Sind trotzdem noch alle Garantien vom strikten 2PL gewährleistet, wenn ja unter welchen Bedingungen?

Hausaufgabe 2 Eine statistische Datenbank ist eine Datenbank, die sensitive Einträge enthält, die aber nicht einzeln betrachtet werden dürfen, sondern nur über statistische Operationen. Legale Operationen sind beispielsweise Summe, Durchschnitt von Spalten und Anzahl der Tupel in einem Ergebnis (**count**, **sum**, **avg**, ...).

Nehmen wir an, Sie haben die Erlaubnis, im **select**-Teil einer Anfrage ausschließlich die Operationen **sum** und **count** zu verwenden. Weiterhin werden alle Anfragen, die nur ein Tupel oder alle Tupel einer Relation betreffen, abgewiesen. Sie möchten nun das Gehalt eines bestimmten Professors herausfinden, von dem Sie wissen, dass sein Rang „C4“ ist und er den höchsten Verdienst aller C4-Professoren hat. Beschreiben Sie Ihre Vorgehensweise.

Hausaufgabe 3 Skizzieren Sie die Funktionsweise von SSL. Erläutern Sie hierzu, wie der einfache TLS Handshake funktioniert. Eine Lösungsmöglichkeit wäre das Zeichnen eines passenden Message Sequence Charts.

Hausaufgabe 4 Sie haben die Users-Tabelle eines Pizzalieferanten ausgelesen, jedoch scheint sein Passwort uncharakteristisch kompliziert zu sein. Das von Ihnen erhaltene Resultat ist das Folgende:

```
id          name        password
----------  ----------  --------------------------------
1           wolfgang    4d75e8db6a4b6205d0a95854d634c27a
```

- Was könnte der Grund für dieses hexadezimale, 32 Stellen lange Passwort sein?
- Können Sie trotzdem den Klartext finden?
- Wie können Sie das Passwort sicherer Speichern?
- Wie können Sie für diese Art von Passwortspeicherung Bruteforce-Attacken erschweren?

Hausaufgabe 5 Implementieren Sie den RSA - beispielsweise in Python. Verdeutlichen Sie sich die Funktionsweise des RSA an einem geeigneten Beispiel, d.h. verschlüsseln Sie eine kleine Nachricht mit einem (nicht zu großen) Schlüssel und bringen Sie das Beispiel inklusive Verschlüsselung und Entschlüsselung mit in die Übung.

Würde bei RSA eine abgefangene verschlüsselte Nachricht mit bekanntem Inhalt die Suche nach dem Private Key erheblich vereinfachen? Begründen Sie kurz.

Hausaufgabe 6 Bob hat ein Vorlesungsverzeichnis für die Universität programmiert und unter `http://db.in.tum.de/~kaufmann/sql_verzeichnis.html` online gestellt.

Um die Suche zu erleichtern, kann die Anzahl der SWS durch ein Parameter eingeschränkt werden. Finden sie eines speziell präparierte Parameterm, bei dessen Eingabe statt der Vorlesungen die Liste der Studenten ausgegeben wird. Die Datenbank folgt dem bekannten Universitätsschema.

Bob erfährt von der Sicherheitslücke und schlägt vor die bekannten Tabellen einmalig mit zufälligen Namen umzubenennen, so seien sie nicht zu finden. Würde diese *Sicherheitsmaßname* helfen?