

**Übung zur Vorlesung  
„Einsatz und Realisierung von Datenbanksystemen“  
im Sommersemester 2007**

Richard Kuntschke (richard.kuntschke@in.tum.de)

**Blatt 4**

**Aufgabe 1**

Betrachten Sie drei Subjekte (Benutzer)  $S_1$ ,  $S_2$  und  $S_3$ , wobei  $S_1$  ein Recht besitzt, das es weitergeben darf. Diskutieren Sie die folgenden beiden Autorisierungsabläufe:

- (a)
  - 1.  $S_2$  erhält das Recht von  $S_1$  und gibt es an  $S_3$  weiter.
  - 2.  $S_3$  erhält das Recht von  $S_1$ .
  - 3.  $S_2$  entzieht  $S_3$  das Recht.
  
- (b)
  - 1.  $S_1$  gibt sein Recht an  $S_2$  und  $S_3$  weiter.
  - 2.  $S_3$  erhält das Recht von  $S_2$ .
  - 3.  $S_2$  erhält das Recht von  $S_3$ .
  - 4.  $S_1$  entzieht  $S_2$  und  $S_3$  das Recht.

Geben Sie Algorithmen für die Rechtevergabe an, die die obigen Probleme berücksichtigen.  
Aufgabennummer im Buch: 12.1

**Aufgabe 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**, ...). Ein Beispiel wäre eine Volkszählungsdatenbank. Für diese Art von Systemen existiert das in der Einleitung erwähnte *Inferenzproblem*.

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.

Aufgabennummer im Buch: 12.3

**Aufgabe 3**

Implementieren Sie den RSA. Effiziente Algorithmen für die Teilprobleme finden Sie beispielsweise in [Rivest et al., 1978] und [Knuth, 1998].

Aufgabennummer im Buch: 12.6

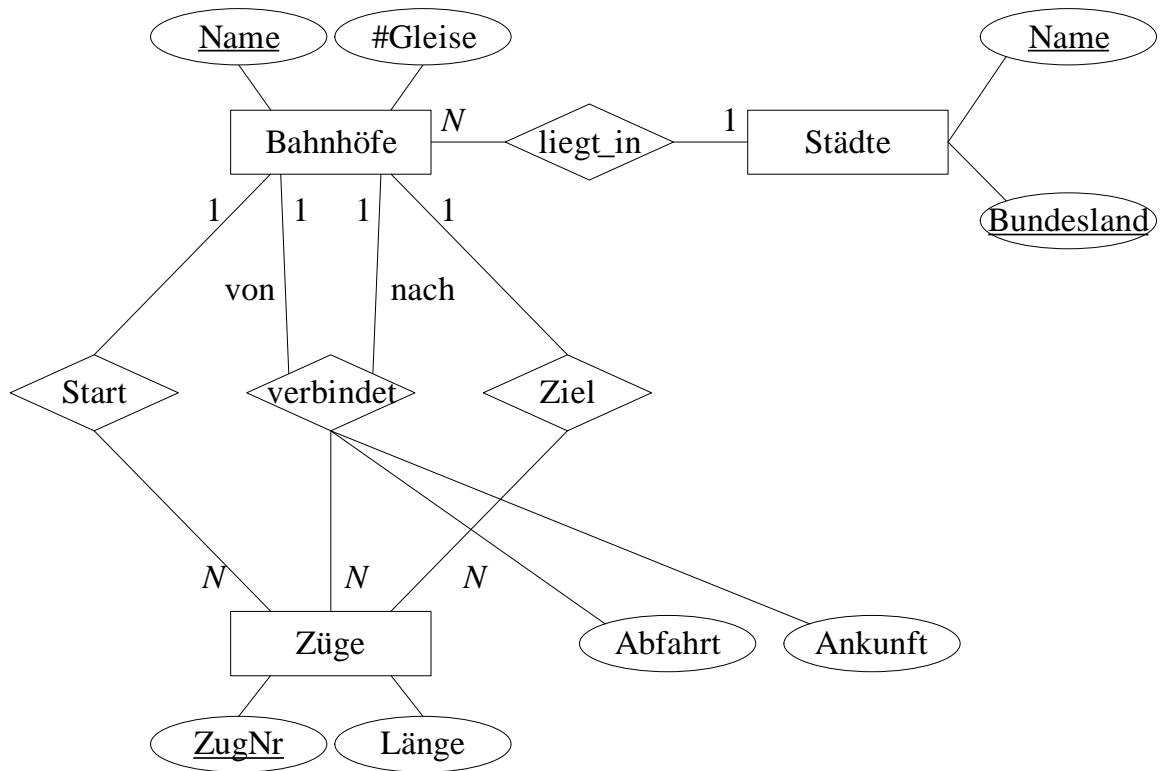


Abbildung 1: Modellierung eines Zugauskunftssystems

#### Aufgabe 4

Entwerfen Sie eine objektorientierte Datenbank für das in Aufgabe 2.6 des Übungsbuchs Datenbanksysteme konzeptuell entworfene Zugauskunftssystem. Sie sollten insbesondere Operationen zur Fahrplanermittlung integrieren. Führen Sie den objektorientierten Entwurf in UML-Notation aus. Verwenden Sie als Anhaltspunkt für die Modellierung das in Abbildung 1 gezeigte, entsprechende ER-Modell.

#### Literatur

[Knuth, 1998] Knuth, D. (1998). *The Art of Computer Programming/Seminumerical Algorithms*, volume 2. Addison-Wesley, Reading, MA, USA, third edition.

[Rivest et al., 1978] Rivest, R. L., Shamir, A., and Adleman, L. M. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126.