Aufgabensammlung zum Buch „Algorithmen und Datenstrukturen“ (Kapitel 9)

1 Aufgaben aus dem Buch

Zu folgenden Aufgaben, die direkt aus dem Buch entnommen sind, gibt es an der Universität Freiburg am Lehrstuhl Ottmann Musterlösungen. In der Version mit Lösungen sind diese angegeben. Hinter der fortlaufenden Aufgabennummer steht in Klammern die Nummer der Aufgabe im Buch.

Aufgabe 1 (Aufgabe 9.6):

Sowohl von Quicksort als auch von randomisiertem Quicksort wird ausgesagt, daß der Algorithmus im Mittel $O(n \log n)$ Schritte benötige. Beschreiben Sie den Unterschied der beiden Aussagen. Worüber wird hier jeweils der Durchschnittswert gebildet?

Aufgabe 2 (Aufgabe 9.7):

a) Benutzen Sie das logarithmische Exponentiationsverfahren, um nachzuweisen, daß die Identität

$$3^{700} \equiv 1 \pmod{701}$$

gilt.

b) Ist die Zahl 113 prim oder zusammengesetzt? Verwenden Sie das randomisierte Primzahltestverfahren. Die Wahrscheinlichkeit, daß Sie die korrekte Antwort geben, soll größer gleich 90% sein.

Aufgabe 3 (Aufgabe 9.8):

Ein *Zertifikat* bestätigt die Echtheit einen öffentlichen Schlüssel. Es enthält den Namen der ausgebenden Behörde, den Namen des Schlüsselinhabers und seinen öffentlichen Schlüssel. Es wird mit dem privaten Schlüssel der ausgebenden Behörde verschlüsselt oder signiert. Über den öffentlichen Schlüssel der Behörde kann es überprüft werden.

a) Geben Sie ein Beispiel für einen Mißbrauch an, der durch Zertifikate verhindert werden kann.

b) Alice möchte über das Internet mit ihrer Bank Kontakt aufnehmen. Sie kennt den öffentlichen Schlüssel der Bank noch nicht. Die Bank verfügt aber über ein Zertifikat einer Behörde, deren öffentlicher Schlüssel Alice bekannt ist. Geben Sie ein Protokoll an, mit dem die Bank Alice über eine Netzwerkverbindung ihre Identität beweisen kann. Versuchen Sie, möglichst viele Sicherheitsrisiken auszuschließen.

2 Ähnlich Aufgaben

Bei den folgenden Aufgaben handelt es sich um Aufgaben die an der ETH Zürich, am Institut für Theoretische Informatik und an der Universität Freiburg im Institut für Informatik in diversen Vorlesungen gestellt wurden. Inhaltlich sind diese Aufgaben mit dem behandelten Stoff im Buch verwandt. Zu allen Aufgaben gibt es Musterlösungen, die allerdings nur in der Version mit Lösungen enthalten sind.