Vorlesung Systemnahe Informatik
Sommersemester 2023

Prof. Dr. Peter Martini, Dr. Matthias Frank, Lennart Buhl M.Sc.

12. Übungszettel

Ausgabe:	Montag, 03. Juli 2023.
Abgabe:	Sonntag, 09. Juli 2023
Besprechung:	In den Übungen ab Montag, 10. Juli 2023.
Hinweis:	Abgabe erfolgt freiwillig per PDF über eCampus, siehe Hinweise in Aufgabe 1 auf dem 1. Übungszettel Sie können Kontakt zu Ihrer Tutor/in aufnehmen durch E-mail an cs4+ueb-si-XX@cs.uni-bonn.de mit XX als Gruppennummer.

Aufgabe 1: Hashing

Wie schon in der Vorlesung (Kapitel 4, Folie 25) erwähnt, ist Hashing unter anderem für den Bereich Sicherheit von großer Bedeutung. In dieser Aufgabe wird Einweg-Hashing/sicheres Hashing näher betrachtet, für das spezielle Anforderungen gelten.
Nehmen Sie an, Sie seien Sicherheitsberater für eine Bank. Die Firma Evil-Software möchte Ihrer Bank ein neues Produkt zur sicheren Dateiverifikation verkaufen. Das Produkt basiert auf einer XOR-Einweg-Hash-Funktion.
Ein Hash-Wert (Länge 1 Byte) wird bei der XOR-Einweg-Hash-Funktion dadurch gebildet, dass sämtliche Bytes der zu hashenden Datei mittels XOR verknüpft werden.

a) Verdeutlichen Sie die Vorgehensweise der XOR-Einweg-Hash-Funktion für die folgende Beispieldatei, die aus nur vier Bytes besteht:

   01011011

   10001010

   11010000

   11001000

b) Sehen Sie Probleme bei dem Einsatz der XOR-Einweg-Hash-Funktion zur Datei-Verifikation? Falls ja, erläutern Sie diese an dem Beispiel aus Teil a).

c) Gibt es andere, bessere Hashfunktionen? Legen Sie kurz den Unterschied dar.

Aufgabe 2: Segmentierung

Gegeben sei die folgende Segment-Tabelle 1:

Tabelle 1: Segment-Tabelle

Segment	Anfangsadresse	Limit
0	219	600
1	2300	14
2	90	100
3	1327	580
4	1952	96

a) Erstellen Sie eine Skizze des physikalischen Speichers (vgl. Kapitel 4, Folie 29).

b) Geben Sie die physikalischen Adressen zu den folgenden logischen Adressen an:

i. 0, 430

ii. 1, 10

iii. 2, 500

iv. 3, 400

v. 4, 112

Aufgabe 3: Demand-Paging

Beim Demand-Paging wird ggf. eine Seite verdrängt (Swap-Out) bevor die gewünschte Seite nachgeladen wird (Swap-In). Wir betrachten hier eine Fallunterscheidung beim Verdrängen: Wurde eine Seite im Speicher verändert bevor sie verdrängt wird (vgl. Modified/Dirty-Bit in der Seitentabelle)?

Im Folgenden gilt bei einem Seitenfehler:

- 8 Millisekunden werden benötigt, wenn ein freier Seitenrahmen verfügbar ist,
- 8 Millisekunden werden im Mittel benötigt, wenn eine auszulagernde Seite nicht verändert wurde,
- 20 Millisekunden werden benötigt, wenn eine auszulagernde Seite verändert wurde.

Des Weiteren nehmen wir an, dass 70% der zu ersetzenden Seiten modifiziert werden. Die Speicherzugriffszeit ist 100 Nanosekunden.

Bestimmen Sie die maximal akzeptierbare Seitenfehlerwahrscheinlichkeit, für eine mittlere effektive Zugriffszeit von nicht mehr als 1 Mikrosekunde.

Hinweis: Sie dürfen zur Lösung dieser Aufgabe einen Taschenrechner verwenden.