

- b) Läßt sich das Nebenläufigkeitsverhalten noch verbessern, wenn man zusätzlich den Vorzustand des Empfängers untersuchen kann (Begründung)?

Aufgabe 5

PVM (8 + 12 Punkte)

Betrachten Sie folgendes Programm zur Multiplikation von zwei Matrizen.

```
static void matrix(int *A, int *B, int *C, int n, int m) {
// multipliziert Zwei Matrizen A und B, mit n Zeilen, m Spalten
// C enthaelt am Ende das Matrizenprodukt

int i,j,k;    // Zaehler int sum;    // Zwischensumme

    for (i = 0; i < n; i++)        // ueber alle Zeilen der Zielmatrix iterieren
    {
        for (j = 0; j < m; j++)    // ueber alle Spalten der Zielmatrix iterieren
        {
            sum = 0;                // Zwischensumme zuruecksetzen
            for (k = 0; k < n; k++)
            {
                // Das Skalarprodukt bilden - dabei ist
                // A[i*n+k] k-tes Element des i-ten
                // Zeilenvektors
                // B[j+k*m] k-tes Element des j-ten
                // Spaltenvektors
                sum = sum + (A[i*n+k] * B[j+k*m]);
            }
            C[i * n + j] = sum;
        }
    }
}
```

- a) Wie kann dieses Programm parallelisiert werden? Geben Sie zwei Parallelisierungsalternativen an.
- b) Beschreiben Sie die Schritte, die bei der parallelisierten Version ausgeführt werden müssen, um die parallelen Prozesse zu koordinieren und die Berechnungsdaten zu verwalten.

Aufgabe 6

Zweiwegevergleich (8 + 4 Punkte)

Von einer gemeinsam benutzten Datei sind durch parallele Änderungen zwei Versionen entstanden.

- Version A

Die Tragödie ist Nachahmung einer guten
und in sich geschlossenen Handlung
wobei diese formenden Mittel
in den einzelnen Abschnitten
je verschieden angewandt werden,
die Jammer und Schaudern hervorruft
und hierdurch eine Reinigung von derartigen Erregungszuständen bewirkt.

- **Version B**

Die Tragödie ist Nachahmung einer guten
und in sich geschlossenen Handlung
von bestimmter Größe,
in anziehend geformter Sprache,
die Jammer und Schaudern hervorruft

- a) Beschreiben Sie die nötigen Schritte, die zum Erstellen einer kombinierten Version unter Verwendung des Zweiwegevergleichs nötig sind.
- b) Wie lautet die kombinierte Version?

Aufgabe 7:

Verschiebechiffre (14 Punkte)

Sie erhalten den Text ‚axnmxblmxbgxi knxyngz‘ mit dem Hinweis, daß er aus den Buchstaben ‚a‘ bis ‚z‘ mit einer Verschiebechiffre erzeugt wurde. Wie lautet der Klartext? Wie lautet der Schlüssel?

Aufgabe 8

Public-KeyKryptographie (10 Punkte)

Erläutern Sie am Beispiel von RSA, wie ein Public Key Kryptosystem in ein Public-KeySignaturschema umgewandelt werden kann.