Diskrete Strukturen II

„Wahrscheinlichkeit und Statistik“

Vorlesung:

Mittwochs 9:15 - 10:00, Raum S1128

Freitags 8:30 - 10:00, Raum S1128

Zentralübung:

Dienstags 12:15 - 13:00, Raum 2750

Übungsleiter: Tom Friedetzky

email: friedetz@informatik.tu-muenchen.de

Skript: Ja! Erste Version voraussichtlich Anfang Juni.

Weitere Informationen:

`http://www14.informatik.tu-muenchen.de/lehre/1998SS/ds/`

Prof. Dr. Angelika Steger

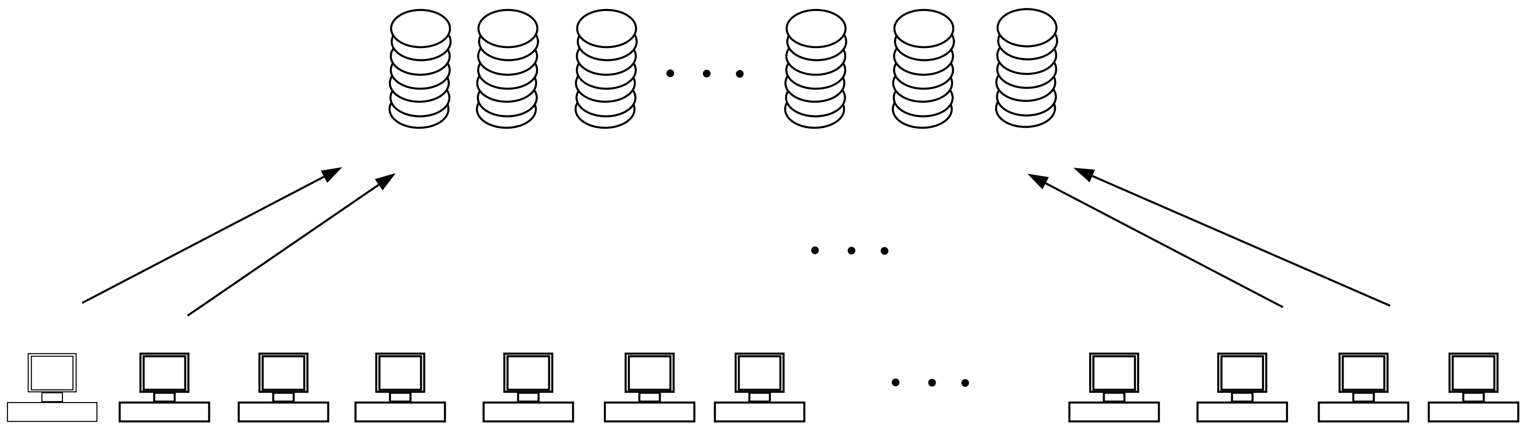
email: steger@informatik.tu-muenchen.de

Zimmer: S2217

Sprechstunde: Do 13-14 und nach Vereinbarung (email)

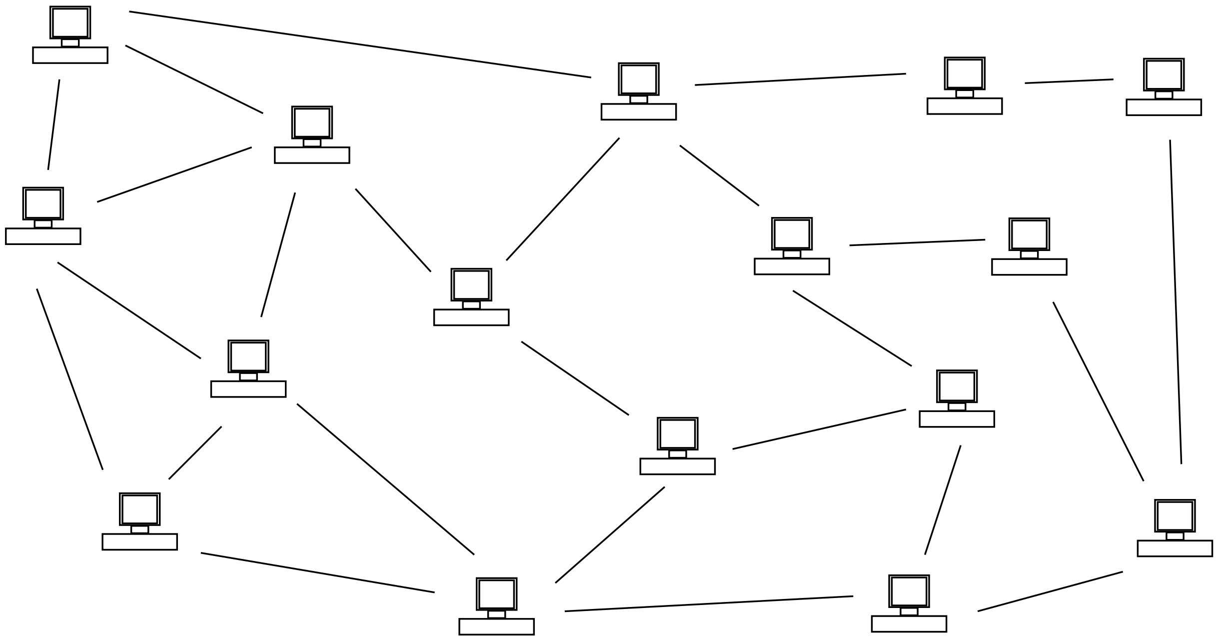
Fallbeispiel 1: Zuordnung von Datenbankanfragen

Szenario:



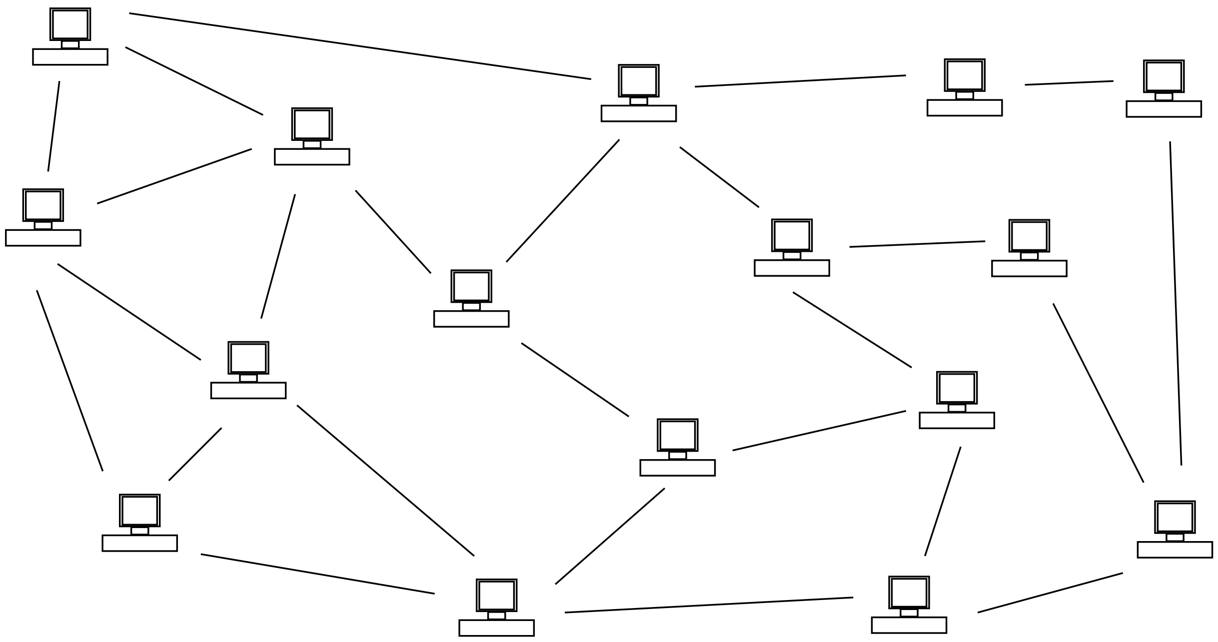
Aufgabe: Entwerfe ein möglichst einfaches Verfahren, das jede Anfrage genau einem Server zuordnet — und zwar so, daß alle Server möglichst gleich viel Arbeit erhalten.

Fallbeispiel 2: Verteilung von Information in (großen) Netzwerken



Aufgabe: Entwerfe ein möglichst einfaches Verfahren (das lokal in jedem Prozessor läuft) mit dem Informationen möglichst schnell allen Prozessoren des Netzwerkes bekannt gemacht werden können.

Fallbeispiel 3: Sicherheit in (großen) Netzwerken

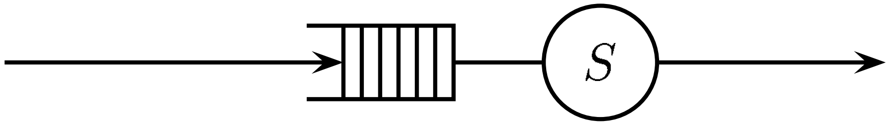


Annahme: Verbindungen zwischen zwei Rechnern brechen mit einer gewissen Wahrscheilichkeit zusammen.

Frage: Mit welcher Wahrscheilichkeit besteht dennoch immer zumindest eine Verbindung zwischen je zwei Rechnern?

Fallbeispiel 4: Warteschlagen

Szenario:



Annahme: Jobs kommen mit einer gewissen Verteilung an;
Ausführungszeit ist ebenfalls zufällig verteilt;

Fragen: Was ist die (durchschnittliche) Wartezeit in der Queue?
Wie sollten Jobs abgearbeitet werden?
(„first come first serve“ oder „round robin“ oder ...)

Fallbeispiel 5: Kryptographie

Ziel: Verschlüsseln (oder auch Authentisieren) von Information.

Näheres in der Vorlesung:

$\longrightarrow$Kryptographie

oder z.B. auch unter

http://www.rsa.com

Verschlüsselungsverfahren RSA:

Wähle zwei (etwa 384 stellige) Primzahlen p, q;

......

Frage: Wie macht man das ???

1. Mögl.: Durchprobieren aller möglichen Teiler ...

Dauer: etwa 10^{41} Jahre

2. Mögl.: Verwende besten bekannten Algorithmus ...

Dauer: etwa 2 Jahre

3. Mögl.: Verwende ein probabilistisches Verfahren ...

Dauer: ein paar Sekunden