Prüfungsprotokoll:

Prüfer: Prof. Hromkovic
Beisitzer: Dr. Unger

Fächer: Effiziente Algorithmen (Hromkovic)
Algorithmische Kryptographie (Unger)
Semantik und Verifikation verteilter Systeme (Noll)

1. Effiziente Algorithmen:

- Lokale Suche
  - Was ist das? Prinzip? Lokales vs. globales Optimum
  - Beispiel?
  - Pathologischer Fall beim TSP!!! (wichtig für 1.0!!! sonst nicht schlimm)

- pseudo-polynomiale Algorithmen
  - Was ist das? Definition?
  - Beispiel? (DPKP - Erklärung und Komplexität)

- Divide & Conquer
  - Prinzip?
  - Beispiel?
  - Mergesort? Funktionsweise ? Komplexität? Rekurrenzgleichung?
  -> Master Theorem? Beweis! (bis zur Summenformel hat gerreicht, Fallunterscheidung nicht notwendig)

- Approximative Algorithmen
  - Prinzip? Güte?
  - Beispiel: Vertex Cover (bei Beweis unterbrochen - "Seh' ich, können Sie..." [;-)]
- "Kennen sie Delta-TSP?" - "Ja, und zwar..." - "Danke! Nächstes Thema!"

2. Semantik und Verifikation verteilter Systeme

- Was sind parallele Prozesse?

- Möglichkeiten der Kommunikation? (Voll nicht in der Vorlesung gewesen...)

- Wie gehen Sie vor, wenn Sie einen Prozeß/ein System modellieren wollen?

3. Algorithmische Kryptographie
- DES
  - Funktionsweise (sehr grob!)
  - Warum schwer zu knacken?
  - Vorteile? ("Ist ziemlich schnell! Hab' ich was vergessen?" - "Nö!")
  - Hinweis auf mutmaßliche Hintertür...

- RSA
  - Prinzip? Warum teilerfremde d und phi(n), bzw. e und phi(n)?
  - Was ist phi(n)? Wie berechnet?

- Warum eindeutig?
- Vorteile? (u.a. Protokolle)

- Protokolle
  - Welche? Was macht man damit? Welche noch? (Wollte auf Altersvergleich hinaus - kannte ich zwar, wußte aber nicht wie' s geht- Mist!)
  - Oblivious Transfer: Protokolle?
    - zuerst a) Übertragung nur zu 50% erfolgreich
    - b) nicht mehr gefragt
  - Zero-Knowledge: k-Färbbarkeit? Warum ist k-Färbbarkeit-Protokoll Zero-Knowledge?
  - Bei Simulation von Zero-Knowledge: Welcher Aufwand für Wiederholung eines fehlgeschlagenen Protokolls? ("??Ehrm??" - "Wie groß ist der Aufwand, wenn wiederholt werden muß?" - "Ehrm, doppelt so hoch (kann er doch nicht meinen..)?" - "Ja, danke, fertig!")