```
Prüfungsprotokoll Theoretische Informatik                         04.12.01

Hromkovic, Walter: EA, AK, CB

Effiziente Algorithmen:
H: Kennen Sie die Dynamische Programmierung?
S: Prinzip erläutert, sukzessives Zusammensetzen der Lösung
   aus Teilproblemen, jede Lösung wird nur einmal berechnet,
   Bottom-Up Strategie, Unterschiede zu DC klargemacht
H: Können Sie mal die Matrixmultiplikation erläutern?
S: Ausgehend für kleinste passende Matrixmultiplikationen werden
   sukzessive teiloptimale Lösungen berechnet, Definition der mij's
   hingeschrieben, bei der Formel hab ich mich leicht verhaspelt
H: Was kennen Sie denn für Reduktionen?
S: Sat auf 3Sat, Clique auf VC, Sat auf Färbbarkeit, VC auf Hamilton....
   (die billigste "Clique auf VC, ist mir natürlich nicht reingefallen)
H: Dann erklären Sie mal VC auf Hamilton!
S: Konstruktion des Graphen und Reduktion erläutert, Beweisideen erklärt,
   also eher unformal
H: Wie geht denn Simulated Annealing?
S: Physikalischen Hintergrund erklärt, Wahrscheinlichkeit für Verschlechterung a
uf-
   geschrieben und erläutert
H: Kennen Sie Christofides Algo?
S: Nein (der kam nicht vor in der Vorlesung) aber den 2Approximativen für das TS
P!
H: Dann erklären Sie den mal!
S: Algo erklärt, Tiefensuche auf MST, erklärt warum er 2approximativ ist
H: ja ok, geben wir nun weiter an Walter

Algorithmische Kryptographie:
W: Was ist denn der Hauptvorteil von Public Key
S: Das der Schlüssel von den Teilnehmern generiert wird...
   (Hier hätte man noch sagen sollen das One Way Fkt mit Trapdoor benutzt werden
W: Hmmmmhh....... erkläre mal den Aufbau von Public Key
S: Habe mal angefangen RSA zu erklären, Parameter, Verschlüsselung, Entschlüssel
ung...
   Soll ich die Eindeutigkeit noch zeigen? ....man muss da drei Fälle unterschei
den...
W: Glauben wir dir mal.... Was ist denn das leichte, was das schwere Problem?
S: (Achsooo war das!) Ja das schwere ist n zu faktorisieren und das leichte
   n mit p oder q zufaktorisieren.
W: Kennst du auch Knapsack?
S: Klar, Aufbau erläutert, stark steigender Vektor etc
W: Ist das den sicher?
S: Nein, Ansatz der Sägezahnkurven und der Wachstums/Schrumpffolgen erläutert,
   dort erhaltener stark steigender Vektor knackt KS System
W: Wie ist das denn mit Zero Knowledge?
S: Man versucht die Kenntnis eines Geheimnisses zu beweisen, ohne Information da
rüber
   preiszugeben
W: Kennen Sie das Geburtstagsprotokoll?
S: Dort versuchen 2 Teilnehmer zu bestimmen wer von ihnen der ältere ist, angefa
ngen das
   Protokoll ausführlich aufzuschreiben, ab der Hälfte nur noch mündlich in Stic
hworten
W: Wie geht das denn bei drei Teilnehmern?
S: da war ich überrrascht, auf die schnelle fiel mir garnix ein außer das das be
schriebene
   Protokoll auch auf drei mal auf drei Personen geht...war laut Walter in der Ü
bung aber
   daher wohl auch nicht so relevant.
W: Wie ist geht das denn mit monotoner Funktion?
S: Achso, ja dann ist es idealerweisee ein One Way Funktion die je das Alter der
```



```
 dreien
   als Eingabe bekommt
W: Warum kann denn bei Zero Knowledge allgemein keine Information bestimmt werde
n?
S: Weil der Verifier nur Informationen erhält die er auch durch Simulation eines
 Proovers
   erhalten würde
W: Wie ist denn da die Laufzeit?
S: wußte ich nicht so genau, lag dann auch ziemlich daneben
W: Doppelte Laufzeit....nagut, das wars mal zu AK

Compilerbau
H: Was hatten wir denn für Werkzeuge für die syntaktische Analyse?
S: LL(k) und LR(k), kontextfreie Grammatiken..
H: Nein eher Strategien!
S: Top-Down und Bottom up
H: Kennen Sie auch Normalenformen?
S: Ja, die Greibach Normalenform, EBNF ...aber die kann ich leider nicht definie
ren...
H: Ach ja das war ja Automatentheorie, nagut wie ist das denn mit LL(k)?
S: Habe das Diagramm hingezeichnet und erläutert, k lookahead steuert Regelwahl,
 Linksableitung
H: Wie funktionier die Semantische Analyse?
S: Die Syntaxbäume aus der syntaktischen Analyse werden attributiert, Top Down d
ie Inheriten Attribute,
   Bottom Up die synthetischen, Problem falls zirkuläre Abhängigkeiten, Beispiel
 Typberechnung
H: Kann wie funktiert das wenn es dort zu Fehlern kommt?
S: Ähhh.......zur allgemeinen Fehlererkennung könnte ich was sagen, die Beispiel
e aus der Vorlesung haben
   doch funktioniert oder?
H: Nagut, wie ist das im allgemeinen?
S: Eine Möglichkeit der Fehlererkennung besteht in der Betrachtung der FollowMen
gen, bis Wiederaufsatzpkt
   gefunden wird
H: Das ist reicht mal, warten Sie kurz draußen

Das wars für mich... hab ne 1.0 bekommen. Abschließend läßt sich noch sagen, es
war eine faire
Prüfung, die Atmosphäre war ok, man sollte wirklich alles können, da die Fragen
zum Teil schon
non-standard waren.
```