Prüfungsprotokoll Theoretische Informatik

Fächerkombi: - Effiziente Algorithmen
- Algorithmische Kryptographie
- Compilerbau

Prüfung am 22.01.02 15 Uhr
Prüfungsdauer : 30 Min.
Note : 1.0

Prof. Hromkovic hatte vor der Prüfung einen Vortrag und kam erst so um 15:05 aus dem Seminarraum. Ich war zu dem Zeitpunkt schon ziemlich nervös, da ich schon um 14:00 Uhr auf die Hörn gelaufen bin.(Nicht zu empfehlen !) Dementsprechend war ich auch in der Prüfung sehr angespannt...
Aber Prof. Hromkovic und Walter machten einen sehr gelassenen Eindruck. Das lockerte während der Prüfung meine Nervosität. Nachdem Prof. Hromkovic nun da war rief er mich in sein Zimmer und es ging auch sofort los.

H: Womit wollen sie denn anfangen ?
M(Ich): Effiziente, Krypto und Compilerbau
H: Also gut dann legen wir mal los. Walter schrieb und er fragte... Erklären sie mal die Rekurrenzgleichungen ?
M: Aufgemalt und ineinander eingesetzt etc... Habe dann die Summenformel hingeschrieben das reichte
H: Was ist der Unterschied zw. Divide an Conquer und Dynamischer Programmierung.
M: Erklärt...und die Beispiele aufgezählt jeweils zu Dynamischer Prog. und D&C.
H: Kennen sie denn ein Bsp wo D&C ineffizient wird.
M: Habe Fibonacci gesagt und erklärt.
H: (Ging dann recht flott ins nächste Kapitel) Was ist denn NP vollständigkeit?
M: Eine Sprache L NP vollständig gdw....
H: OK. Welche Reduktionen kennen Sie ?
M: Alle die wir in der Vorlesung hatten.
H: Gut erklären Sie mir mal die Reduktion auf Hamilton Kreis.
M: Angefangen Konstruktion gemacht etc... Nach der Konstruktion erklärte ich den Rest mündlich. Er brach auch irgendwann ab und meinte ich denke sie können es (freu freu...)
H: Können Sie mir den sagen was ein PTAS ist ?
M: Ja kann ich. Also ein Algorithmus A für ein Optimierungsproblem U ist genau dann ein PTAS wenn ... die Bedingungen erklärt.
H: Kennen sie denn ein Beispiel
M : Ja den Greedy – Algorithmus für das einfache Rucksackproblem.
H: Können sie den Alg. auch erklären.
M: Ja kann ich. (habe alles erklären müssen. Incl. Laufzeitabschätzung und zeigen das der Relative Fehler höchstens ε ist.) Zwischendurch habe ich glaube noch erzählt was ein Relativer Fehler ist usw.
Das war es dann auch schon mit Effiziente... Walter fing an mich in Krypto zu fragen:
W: Sag mal welche Public Key Verfahren wir in der Vorlesung hatten
M : Habe alle aufgezählt. Aber den Williams verschwiegen den hatte ich nämlich nicht gelernt.
W: Da gab es noch einen der eine Weiterentwicklung von RSA ist.

M: Ja das ist das Verfahren von Williams, da werden Zahlen der Form (a + b Wurzel c) benutzt. Den haben wir auch in der Vorlesung gemacht. (Mehr wollte er nicht wissen)
W: Gut erklär mal RSA
M. Aufbau erklärt.
W: Warum wird denn ggt(d, Phi(n)) ≡ 1 gesetzt.
M: Hmmm damit entschlüsselung eindeutig wird.
W: Ne. Denk mal an einen Schritt weiter
M: Achso, ja sonst gibt es kein e mit ed ≡ 1 (mod phi(n))
W: Was ist die Idee bei dem Eindeutigkeitsbeweis ?
M: Habe halt angefangen da w<n ist und ein j existiert so dass...
W: Danke das reicht. Und ist RSA sicher ??
M: (Kacke. Die Seiten im Skript hatte ich mir eigentlich gespart.) Na ja ist halt ne One Way Funktion Faktorisierung von n, die Rückrichtung zu berechnen ist ziemlich schwer. Wenn ich Phi oder d habe ist es genau so schwer wie n zu faktorisieren...
W: Gibt es so etwas wie Entschlüsselung von Teilinformationen ?
M: Ich glaube es gibt da so etwas wie Orakel die mir einer gewissen Wahrscheinlichkeit das letzte Bit verraten (Hatte ich von einem Kumpel, der die Prüfung eine Woche vor mir gemacht hatte gehört).
W: Was heißt das denn für Teilinformationen?
M: (Häh keinen blassen Schimmer) Ja das heißt das ich dann halt sukzessive immer das letzte Bit vom Orakel bekomme.
W: Mach mal ne Rückschluss, bzgl der Sicherheit von Teilinformationen !
M: Also da die Wahrscheinlichkeiten sehr gering sind. Ist RSA auch bzgl. Teilinformationen sicher.(Mehr geraten als gewusst!)
W: Ja richtig
M: (Das war knapp...)
W: Also gut. Welche Protokolle kennst du?
M: Alle aufgezählt. Die mir einfielen. Von Quittungen, Unterschriften, 0-1 Protokollen, ... bis k-Sharing, Blinde Signaturen, Verschlüsseln geheimer Nachrichten mit El Gamal. (Habe beim Aufzählen immer die Idee gesagt, zumindest bei denen es mir einfiel Bsp. Wir hatten 3 Varianten von 0-1 Protokollen erstens die einfache Variante, dann die mit den Quadratwurzeln und 3. die Variante wo A sich eine Zahl a aussucht mit Jacobi Symbol (a/n) gleich ist. Davon sind dann 50 % Quadratischer Rest und 50 % nicht usw....))
W: Kennst du das Geburtstag Protokoll ?
M: Ja. Angefangen zu malen. Als ich sagte das sich jetzt A Zahlen Z_u generiert und sich davor noch eine Primzahl mit den Eigenschaften... meinte er das reicht mir.
W: Gut. Sag mal was zu Oblivious Transfer (Hatte ich oben nur erwähnt)
M: Ja da gibt es 2 Varianten....Beide erklärt...
W: Kennst du ein Bsp für den 1.ten Fall(ist der einfachere Fall, kenn ich).
M: Ja das ist der Fall wo ich p,q,n generiere B sucht sich ein Zahl a aus schickt mir das Quadrat, ich berechne die Quadratwurzeln ... und und und
W: Sag mal was zu Zero Knowledge (Ab hier habe ich nichts mehr hingeschrieben)
M: Erklärt.
W: Sag mal was zur Sicherheit für P und V
M: Die Sicherheit für P ist... Für V ist ...
W: Wie viel Mehraufwand ist das denn für V sich diese Informationen zu beschaffen und zu verifzieren?

M: (Habe keine Ahnung, fange wieder an. Das gleiche zu erzählen wie oben das sich halt P problemlos drauf einlassen kann und die Sicherheit für V $1-1/n^k$ beträgt falls P doch schummeln sollte usw.)
W: H schaltet sich ein und sagt irgendwas.
M: Komme auf die Idee mit „Ja das ist dann 2k“ zu sagen und alle sind glücklich(Hatte das noch aus dem Skript in Erinnerung. weiß aber nicht warum das so ist. Wollte auch niemand von mir wissen)
H: (lächelt mich an) Manchmal versteht man halt die Frage nicht.
W: Gut. Dann sag mal was zu Quantum Computing
M: (Scheiße wo kommt das denn jetzt her. Habe das im Skript mal überflogen. Habe mir aber das was ich erzählte mehr oder weniger ausgedacht) Ja da geht es um Photonen die man ausrichten kann und mit der Ausrichtung dann die Bits kodieren kann. Wer dann das Gitter der Ausrichtungen kennt kann Entschlüsseln. Äääh mehr weiß ich nicht.
W: Gut wollte mal sehen ob du das kannst.(Grinst) Erklärt mir dann Quantum Computing (Tue so als ob ich zuhöre, sage ja)
W: OK ich bin fertig.
M: (endlich...)
H: OK Kommen wir zu Compilerbau. Erzählen sie mal etwas über die Phasen eines Compilers
M: Fange an mit allem loszulabern
H: Danke das reicht.
H: Was wissen Sie über die Lexikalische analyse
M: Habe angefangen bei den Lexemen, Symbol, Attribut, Endliche Automaten, Reguläre Ausdrücke Thompson Konstruktion NFAs DFAs...
H: Danke. Sagen sie etwas über die Syntaktische Analyse. Es gibt da 2 Techniken
M: Parser, Grammatiken(Habe mir den Stift in die Hand genommen und wollte LL(k), und LR(k) aufmalen)
H: Das sind ja jetzt spezielle Fälle. Was können sie mir über die Erkennung eines beliebigen w ε CFG sagen ?
M: Ja da kenn ich den CYK Algorithmus.
H: Können sie mir den erklären.
M: Sicher. Habe nur die Idee erläutert und die Laufzeit erklärt. Und das das ein Fall der dynamischen Programmierung ist.
H: Danke das reicht. Sagen sie noch etwas zur Semantischen Analyse
M: Benutze Attributgrammatiken (Habe dann noch ganz grob aufgemalt wie so ein Attributgleichungssystem aussehen könnte) Attributierung des Ableitungsbaumes. Inherite und Synthetische Attribute, je nach dem ob ich eine TD oder BU Attributierung mache...
H: Danke das reicht. Warten sie bitte draussen...

Abschliessend will ich noch sagen. Das mir bei der Vorbereitung auf die Prüfung die Protokolle sehr geholfen haben. Bei CB muss man wirklich nicht viel wissen. Also ich bin fertig dir viel Glück. Und Leute schreibt Gedächtnisprotokolle nach den Prüfungen.