Prof: Prof. Juraj Hromkovic
Themen: Cryptographie nach Delfs, Effiziente Algorithmen nach Buch 2-te Auflage (er hat mir voher die Kapitel angegeben die ich lernen muss), Automatheorie (also eigentlich Applied Automatatheory) nach Skript von Prof. Thomas von vor ein paar Jahren (die 80 seiten version).
Datum: 2.4.04
Note: 1.0
Dauer: 30 min

Reihenfolge: Crypto, Effi, Automaten

H: Welche public key Cryptosysteme kennen Sie?
O: RSA, Rabin, El Gamal

H: Erklären Sie mal Rabin.
O: Funktion aufgeschrieben, n=p*q. man quadriert, ist einfach. Wurzelziehen ist schwer wenn man die Faktoren p und q von n nicht kennt.

H:Erklären Sie RSA
O: n=p*q. man hat e zum Encrypten und d zum Decrypten. e ist das inverse von d modulo phi(n). zum encrypten nimmt man die message hoch e, zum decrypten nimmt man das Cryptogram hoch d.

H: Wie findet man e und d?
O: Man wählt eins zufällig aus und findet das andere mittels des erweiterten euklidischen Algo.

H:Woher weiss man dass das eine ein Inverses hat?
O: *einfache Frage, aber ich war irgendwie verwirrt* Er hat dann ein Beispiel gemacht, dann kam ich drauf: das muss prim zu n sein.

H: Können Sie die Eindeutigkeit zu RSA beweisen?
O: Ja

H: Machen Sie mal.
O: hab angefangen, es gibt 3 Fälle. Erstmal p und q teilen w nicht, gezeigt. Dann p teilt w, q nicht, dann hat er abgebrochen, ist gut.

H:Sagen Sie was zu digitalen Signaturen
O: man benutzt da den secret key um eine message zu signieren, bla...

H:Wo ist das Problem dabei? (er hat die frage schon was genauer gestellt, aber ich kann mich nicht mehr errinern)
O: hab dann was gesagt von wegen, wenn der eine dem anderen messages zum signieren gibt, dann kann er da ein Cryptogram drin verstecken usw. aber das wollte er nicht hören.

H: es geht eher um zu wissen ob der andere der ist, von dem man annimmt dass er es ist (oder so...). geht richtung Identification Schemes....

O:ja, der eine hat ein secret, will dem anderen zeigen, dass er es kennt, aber ohne es preiszugeben.

H:Was kennen Sie da?
O:z.B. Fiat – Schamir. Hab dann das vereinfachte Fiat-Shamir erklärt.

H: Gehen wir zu Effi...
O: Yehaaaa ☺ (kleiner scherz, so locker war ich noch lange nicht)

H: Teile und Herrsche, was ist das?
O: man teilt Problem auf in kleinere Unterprobleme. Löst diese und fügt die Lösungen der Teilprobleme zu Lösung des Gesamtproblems zusammen.

H: Können Sie ein Beispiel nennen?
O: Multiplizieren von Zahlen. Hab dann angefangen mit der schlechten Methode, hab dann gesagt dass man die einen 2 Multiplikationen durch eine einzige ersetzen kann, hab die Formel aufgeschrieben. Zur Komplexität wollte er nichts wissen.

H: Parametrisierte Komplexität. Was ist das?
O: man versucht die Komplexität eines Problems anhand eines parameters festzulegen. Hab dann das mit unendlich viele Parameter , unendlich viel bla gesagt. Dann hat er noch mal nachgehackt und hab dann erklärt was ein par-param. Pol time Algo ist, also dass es polynom. In der Größe der Eingabe ist, aber nicht was den Paramter angeht.

H: Beispiel?
O: VC, es gibt 2 Beispiele

H: Erklären Sie mal beide.
O: hab mit dem ersten angefangen, mit den beiden Hilfssätzen. Den ersten musste ich erklären, also warum alle Knoten mit Grad größer k im VC von Größe k sein müssen.
Dann den Algo erklärt, Komplexität wollte er nicht wissen.
Dann den zweiten Algo erklärt, auch keine Komplexität.

H:Was sind Diamanten?
O: Erklärt. auch was sie bringen.

H:Wo benutzt man die?
O: HC<=RHC, pathologisches TSP

H:Erklären Sie HC<=RHC
O: Konstruktion aufgemalt, wie die Kanten der Diamonds verbunden werden etc.

H:Gehen wir zu automatentheorie. Erklären Sie diese Kongruenz auf Sprachen.
O: ~L Def. Aufgeschrieben.

H:Wie funktioniert die Minimierung?
O: Trennbarkeit und dann Algortithmus erklärt.

H:Was ist mit der Minimierung von NFAs?
O: Hm, das ist sehr schwer

H:Ja, das ist schwer. Wie schwer ist das?
O: Np-vollständig? Ich hatte keine Ahnung, stand nicht im Skript.

H: Ne, ach, Sie haben nach dem alten Skript gelernt oder?
O: Ja, das von vor 2 Jahren oder so.

H: Ja dann, was sind Baumautomaten?
O: Automaten auf Bäume laufen und Baumsprachen erkennen

H: Was gibt's da für welche?
O: Top down, buttom up.

H: Wie funktionieren die?
O: Hab dann so angefangen, die haben Zustände, eine Transitionsfunktion bzw. Relation, Endzustände...

H:Wann akzeptiert ein Baumautomat einen Baum?
O:Bei DTA gibts die Evaluationsfunktion, delta*(Baum) muss ein Endzustand sein. Bei NTA ist der Lauf des Automaten auf einen Baum selber ein Baum aus Zuständen und an der Wurzel muss ein Endzustand sein, dann ist das ein akzeptierender Run.

H:Ok, gehen Sie mal kurz raus.

Fazit: Sehr netter Prof., der Assistent auch sehr nett, der hat nämlich nix gefragt ☺