Kryptographie

Skript zur Vorlesung im SS 94

Birgit Pfitzmann

Universität Hildesheim
Institut für Informatik
Version 9.4.1995

Gliederung

Vorwort

Dieses Skript ist, wie man leicht sieht, aus Folien hervorgegangen. Die Folien waren aber von vornherein auch für diesen Zweck entworfen, da es kein zu dieser Vorlesung ähnliches Buch gibt und die parallele Erstellung eines ausformulierten Skripts beim ersten Mal kaum möglich ist. Die vorliegende Version ist korrigiert, enthält aber keinen neuen Stoff im Vergleich zu den Originalfolien. Allerdings wurden einige Erklärungen verbessert und ganz wenige Begriffe und die Kapitelnumerierung geändert. (Falls es jemals in einer Prüfung zu Verwirrung kommt, sollte die Version der Studierenden gelten.) Die Vorlesung war 2-stündig mit 1-stündigen Übungen.

Die starke Betonung allgemeiner Sicherheitsbegriffen und Spezifikationstechniken am Anfang ist für eine Kryptographievorlesung zweifellos ungewöhnlich. Einerseits glaube ich wirklich, daß solche Dinge für die meisten, die beruflich mit Sicherheit zu tun haben, wichtiger sind als viele Einzelheiten kryptographischer Algorithmen. Andererseits leugne ich nicht, daß manche wichtigen kryptographischen Themen in dieser Vorlesung fehlen und ich am Schluß gern ein paar Vorlesungswochen mehr gehabt hätte. Im Hildesheimer Studienplan gehört diese Vorlesung aber zum Vertiefungsfach „Sicherheit“ und wird meist mit der Vorlesung „Sicherheit in Rechnernetzen“ von Andreas Pfitzmann kombiniert, die zu einem großen Teil Kryptographie in etwas klassischerer Gestalt behandelt. Die fehlenden Teile können also in jenem Skript oder den im folgenden angegebenen Büchern nachgelesen werden.

Dank

Vieles an meiner eigenen Sicht von Kryptographie, gerade im formalen Bereich, habe ich zusammen mit *Michael Waidner* erarbeitet. Folglich sind sicher viele Ideen von ihm in diesem Text verstreut. Zum Teil gilt dies auch für *Andreas Pfitzmann* und *Matthias Schunter*. Der Teil über Wissenslogik ging aus einem gemeinsamen Seminar mit *Michaela Huhn*, *Joachim Biskup*, und *Ulla Goltz* hervor. Dank sei auch *Gerrit Bleumer* für die Vertretung beim Secret Sharing und Kommentaren dazu und den HörerInnen der Vorlesung für ihre Fragen und Kommentare. Insbesondere hat *Henrik Hüne* einen Teil der Musterlösungen erarbeitet, die ich hier allerdings nicht mit abdrucke, und *Stefan Wagenführ* eine ganze Liste von Fehlern aufgespürt.