

Kryptographie

Skript zur Vorlesung im SS 94

Birgit Pfitzmann

**Universität Hildesheim
Institut für Informatik
Version 9.4.1995**

Gliederung

Vorwort.....	vi
Dank.....	vi
0 Vorbemerkungen.....	1
0.1 Verwaltung.....	1
0.2 Literaturempfehlungen.....	3
1 Einleitung.....	7
1.1 Was ist Kryptologie?.....	7
1.2 Einige Beispiele.....	8
1.3 Tätigkeiten in Kryptologie.....	14
2 Entwurfszyklus für.....	16
2.1 Vor Spezifikation.....	16
2.2 Spezifikation.....	20
2.2.1 Einzelziele \leftrightarrow Gesamtspezifikation.....	20
2.2.2 Dienst- und Geheimhaltungsziele.....	22
2.3 Vertrauensmodell.....	27
2.4 Komponentenzerlegung und -spezifikation.....	32
2.5 Implementierung der Komponenten.....	35
3 Wichtigste allgemeine Begriffe.....	37
3.1 Wissen und Geheimhalten.....	37
3.1.1 „Wissen“ wie in der Wissenslogik.....	39
3.1.2 Geheimhaltung mit Wahrscheinlichkeiten.....	49
3.1.3 Ergänzungen.....	64
3.2 Verteilte Systeme und ihre Spezifikation.....	70
3.2.1 Einführung.....	71
3.2.2 Was ist „Verhalten an Schnittstellen“?.....	76
3.2.3 „Normale“ Dienstspezifikationen.....	90
3.2.4 Konkrete Beispiele für Spezifikations Sprachen.....	97
3.2.5 Zusammenschalten interaktiver Komponenten.....	106
3.3 Einbau von Vertrauensmodell und Benutzern.....	109
3.3.1 Vertrauensmodell.....	109
3.3.2 Benutzer und Sicherheitsgrade.....	111

4	Informationstheoretisch sichere Systeme.....	120
4.1	Zum Rechnen in Restklassenringen \mathbb{Z}_n	121
4.1.1	Allgemeines	121
4.1.2	Multiplikative Gruppe \mathbb{Z}_n^*	124
4.1.3	Körper \mathbb{Z}_p für p prim	127
4.2	Authentifikationssysteme.....	128
4.2.1	Grobe Spezifikation, noch unerfüllbar.....	128
4.2.2	Initialisierung	129
4.2.3	Spezifikation mit mehr Einzelheiten.....	133
4.2.4	Einfache Standardkomponenten	138
4.2.5	Sicherheitsgrad	143
4.2.6	Definition spezialisiert auf einfache Einmalauthentikation.....	144
4.2.7	Spielzeugsystem: $M = \{0, 1\}$, $\sigma = 1$	149
4.2.8	Konkrete große Systeme	150
4.2.9	Padding.....	161
4.2.10	Mehrere Nachrichten.....	162
4.2.11	Varianten mit anderen Zielen.....	164
4.3	Informationstheoretisch sichere Konzelation.....	166
4.3.1	Komponenten bei „nicht-interaktiven“ Systemen für 1 Nachricht.....	166
4.3.2	One-Time-Pad für eine Nachricht fester Länge	167
4.3.3	Varianten	169
4.3.4	Ergänzung für mehrere Nachrichten	170
4.3.5	Optimal?	170
4.4	Vollständiges Secret-Sharing	172
4.4.1	Grundschema von Shamir.....	172
4.4.2	Beweis der Geheimhaltung.....	179
4.4.3	Erweiterungen	181
5	Komplexitätstheoretische Sicherheit.....	185
5.1	Komplexitätstheoretische Beschränkung genauer	186
5.2	Kryptographische Annahmen und ihre Verwendung	191
5.2.1	Wozu Annahmen?.....	191
5.2.2	Verwendung von Annahmen.....	192
5.2.3	Faktorisierungsannahme(n).....	194
5.2.4	Diskreter-Logarithmus-Annahmen.....	207
5.2.5	RSA-Annahme(n) u.ä.....	221
6	Systeme unter zahlentheoretischen Annahmen.....	226
6.1	„Beweisbar sichere“ Commitments	226
6.1.1	Spezifikation	226
6.1.2	System.....	227
6.1.3	Sicherheit.....	233
6.1.4	Erweiterungen	237
6.2	Münzwurf	239

6.3	Signaturen.....	242
6.3.1	Grundidee.....	243
6.3.2	ElGamal-System.....	245
6.3.3	Definitionen allgemeiner.....	248
6.3.4	Zur Sicherheit des ElGamal-Systems.....	251
6.3.5	Ad-hoc-Gegenmaßnahme.....	253
6.3.6	Varianten.....	262
6.3.7	Praxis der Schlüsselverwaltung.....	263
6.3.8	Ausblick: Fail-stop-Signaturen.....	266
6.4	Asymmetrische Konzelation und Schlüsselaustausch.....	272
6.4.1	Konstruktionsidee.....	273
6.4.2	Diffie-Hellman-Schlüsselaustausch.....	274
6.4.3	ElGamal-Konzelation.....	277
6.4.4	Allgemeines zu asymmetrischer Konzelation.....	285
7	Ausblick: Nicht (oder kaum) behandelte Systemklassen.....	288
7.1	Primitive.....	288
7.1.1	Einwegfunktionen.....	288
7.1.2	Trap-door-Einwegpermutationen.....	290
7.1.3	Hashfunktionen.....	291
7.1.4	Pseudozufallszahlengeneratoren.....	291
7.1.5	Blockchiffren und Pseudozufallsfunktionen.....	294
7.2	Mehr Authentikation und Konzelation.....	298
7.3	Höhere Protokolle.....	300
	Anhang: Seminarprogramm „Höhere Protokolle“.....	301
	Aufgaben.....	307
	Literatur.....	315

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.