Schutz in verteilten Systemen durch Kryptologie – Ein Praktikum im Informatik-Hauptstudium

Andreas Ort[‡], Ralf Aßmann[*], Gerrit Bleumer[†], Manfred Böttger[*],
Dirk Fox[‡], Andreas Pfitzmann[†], Birgit Pfitzmann[†], Michael Waidner[‡]

Zusammenfassung

Trotz des zunehmenden Einsatzes von Informations- und Kommunikationstechnik sind Sicherheitsprobleme und Schutzmöglichkeiten immer noch nur wenigen bewußt. Das vorliegende, für die universitäre Lehre konzipierte Praktikum möchte mithelfen, dies zumindest bezüglich der Informatik Studierenden zu ändern. Hierzu behandelt es kritisch die in den immer mehr an Bedeutung gewinnenden verteilten Systemen wichtigen Eigenschaften „Vertraulichkeit, Authentizität und Anonymität", Verfahren zur Herstellung der gewünschten teilnehmerüberprüfbaren Sicherheit und ihren Einsatz. Das didaktische Konzept des Praktikums und der Einzelversuche wird näher erläutert, um Anregungen für ähnliche Projekte zu geben oder zu solchen zu ermutigen. Eine größere Zielgruppe wäre die Folge und somit ein verbreitertes Bewußtsein für Probleme und Lösungen.

Stichworte

Verteilte Systeme, Kryptologie, Kryptographie, Konzelation,
Authentikation, Unbeobachtbarkeit, Anonymität, Praktikum

1 Einleitung

An der Notwendigkeit von Datenschutz und Datensicherheit mag mittlerweile, zumindest in vernünftigen Fachkreisen, kaum noch gezweifelt werden. Dennoch ein leidvolles Thema in der Informatik, wurden die bedenkliche Sicherheit und die Risiken des zunehmenden Einsatzes von Informations- und Kommunikationstechnik doch allzu spät erkannt. Diese Lücken im nachhinein zu stopfen und gleichzeitig auf die bereits bestehenden Anforderungen Rücksicht zu nehmen, gleicht zwar einer Sysiphosarbeit, bleibt aber nichtsdestotrotz eine notwendige Aufgabe. Äußerst wichtig ist es darum, an die nachfolgenden Informatiker die Datenschutz- und Datensicherheitsproblematik als eine fachimmanente gleich in der Ausbildung heranzutragen. Dann besteht zumindest die Hoffnung, daß in weiteren Entwicklungen auf diesem Gebiet größere Versäumnisse vermieden werden.

Auch im engeren Bereich der Kommunikations- und Informationstechnik sind mögliche Ansatzpunkte für das Problem weit gestreut. Eine konzentriertere Auswahl ist nicht nur für die Wahrung des Rahmens dieses Artikels, sondern auch für die in der Ausbildung verwendeten Lehrformen notwendig. Die Wahl fiel auf den Themenbereich „Schutz in verteilten Systemen durch Kryptologie".

Verschiedene, sich unabhängig ändernde und nicht an einem Ort befindliche Wissenskontingente führen zu Kommunikation, die einen Abgleich der unterschiedlichen Wissensstände erlaubt. Angesichts der heute zu verarbeitenden Menge an Information (in Form von Daten) ist eine Verteilung notwendig und sinnvoll, z.B. wegen des verringerten Risikos des Totalverlustes. Verteilte Systeme

[*] Schneider & Koch & Co. Datensysteme GmbH, Daimlerstraße 15, W 7500 Karlsruhe 21

[†] Universität Hildesheim, Institut für Informatik, Samelsonplatz 1, W 3200 Hildesheim

[‡] Universität Karlsruhe, Institut für Rechnerentwurf und Fehlertoleranz, Postfach 6980, W 7500 Karlsruhe 1

sind demnach der Ausgangspunkt für weiteren Datenzuwachs und gleichzeitig die Ursache für weitere Kommunikation. Es besteht also eine prinzipielle Motivation, sich mit diesem Gebiet zu beschäftigen. Leider ist es einer Datenbank nicht möglich, den zugewiesenen Platz zwecks Konsistenzprüfung und -erhaltung zu verlassen; eine gegebenenfalls große geographische Weite überbrückende Kommunikation ist dann erforderlich. Dies liefert den zweiten Grund für die Themenauswahl, denn räumliche Distanz erzwingt heute in der Regel, sich einem Kommunikationsnetz und dessen Diensten anzuvertrauen. Das Persönliche der Kommunikation entfällt bzw. ist dem blinden Vertrauen oder dem wuchernden Mißtrauen gegenüber dem Diensterbringer gewichen. Diese Entwicklung bringt einen neuen Aspekt in die Kommunikation: die Anonymität. Sie kann sich gegenüber dem Diensterbringer, aber auch gegenüber dem Kommunikationspartner äußern. In beiden Fällen wird sie eine wichtige Rolle spielen.

Der verlorengegangenen Intimität von Kommunikation soll an dieser Stelle nicht nachgetrauert werden. Die Aufgabenstellung hier muß lauten, wie die wichtigen Bestandteile Vertraulichkeit und Authentizität der persönlichen Kommunikation gerettet werden können. Es gilt, den Widerspruch zwischen gewünschter vertraulicher und authentischer Kommunikation und der Notwendigkeit von „fremderbrachten“[1] Diensten aufzulösen. Überprüfung ist ein beliebtes Mittel, Mißtrauen abzubauen. Die Überprüfbarkeit der seitens der Kommunikationspartner zu verwendenden Dienste sollte hierbei allzeit möglich sein. Wenn sich ein Benutzer selbst von der Vertraulichkeit der verwendeten Dienste überzeugen kann, dann läßt sich zwischen den oben angesprochenen Extrema Vertrauen und Mißtrauen ein sachlicher, sich auf Geschäftsbasis bewegender Mittelweg finden (vgl. etwa mit dem Volkszählungsurteil [Bund_83] oder mit [Cha8_85]). Dieser Sachverhalt sei im folgenden mit dem in [Pfit_89] verwendeten Begriff des teilnehmerüberprüfbaren[2] (Daten-)Schutzes bezeichnet und bildet einen Schwerpunkt in dem gewählten Stoffgebiet. Zugleich ist der Wunsch, teilnehmerüberpüfbaren Schutz möglich zu machen und ihn einer breiten Öffentlichkeit darzustellen, der zentrale Grund für die Beschäftigung mit diesem Thema.

Um Mißverständnisse zu vermeiden, sei der ausgewählte Themenbereich nochmals kurz umrissen. Es dreht sich um die Sicherheit von Kommunikation in verteilten Systemen. Nur hier ist der Begriff des teilnehmerüberprüfbaren Schutzes sinnvoll anzuwenden, da in zentralisierten Systemen immer das Vertrauen in die (allmächtige) Zentrale gegeben sein muß. Mit Sicherheit ist nicht die technische Sicherheit (*safety*) oder die Fehlertoleranz des verwendeten Kommunikationsnetzes bei fehlerhaftem Verhalten gemeint, sondern die für einen Teilnehmer geforderte Sicherheit bezüglich Vertraulichkeit, Authentizität und auch Anonymität gegenüber dem fremden Diensterbringer oder den Kommunikationspartnern. Diese Sicherheit muß für den Teilnehmer überprüfbar sein, d.h. er muß sich versichern können, daß die vom Diensterbringer angebotenen, oben genannten Leistungskriterien auch wirklich erbracht wurden. Obwohl die Sicherheit von Applikationen (z.B. Datenbanken), denen ein verteiltes System zugrundeliegt, von weiteren spezifischen Kriterien (Stichworte: Paßwortkontrolle, vertrauenswürdiges Booten, Zugriffsrechte) abhängt, werden sie hier nicht weiter betrachtet.

Bei der gegebenen Auswahl des Themenbereiches soll nun die geeignete Form der Vermittlung in der Lehre gefunden werden. Im universitären Bereich sind dies hauptsächlich Vorlesungen, Seminare

---

1 Um die Vielzahl von potentiellen Angreifern gegen die gewünschte Sicherheit (etwa Diensterbringer, Außenstehende, nicht an der Kommunikation beteiligte Netzteilnehmer) nicht immer vollständig spezifizieren zu müssen, werden diese im weiteren immer als „Fremde“ (im Gegensatz zu den beteiligten Kommunikationspartnern) bezeichnet.

2 „Teilnehmer“ deswegen, weil sich ein Benutzer eines Kommunikationsdienstes eines Kommunikationsnetzes bedient und damit ein Teilnehmer dieses Netzes ist.

und Praktika, im nachuniversitären Bereich dann „Workshops“, Tagungen, Schulungen etc. Aus der Notwendigkeit heraus, die beschriebene Problematik zur Vermeidung weiterer Fehler durch Unbesonnenheiten möglichst früh an die Menschen heranzutragen, gilt dem universitären Bereich das Hauptaugenmerk. Dem nachuniversitären Bereich bleibt die Schulung in der Sysiphosarbeit.

Bei der Vermittlung der Problematik in der Lehre ist zweierlei wichtig: Zum einen muß das Problem und dessen Folgen eindringlich geschildert werden, um die Notwendigkeit von Lösungen eingängig ableiten zu können. Eine Sensibilisierung anhand von Beispielen im alltäglichen Bereich ist dabei hilfreich, da sich die Materie dann nicht nur als reine Theorie darstellt. Zum anderen muß gezeigt werden, daß vernünftige (für die Volkswirtschaftswissenschaftler: wirtschaftliche; für die Mathematiker: beweisbar sichere; für die Informatiker: effiziente; für die Benutzer: handhabbare) Lösungen existieren und durchaus einsetzbar sind bzw. wären. Für Argumentationen eine wichtige Voraussetzung, um weitere Lücken im Bereich des Datenschutzes durch nicht zu haltende Ausflüchte zu verhindern.

Soll die pädagogisch sehr effektvolle Kombination von grundlegender Theorie und funktionierendem Verfahren ausgenutzt werden, dann scheidet die eher für einen inhaltlichen Überblick eines mittelgroßen bis großen Themenkomplexes geschaffene Form der Vorlesung aus. Spezielle Vorlesungen gehen zwar auf einen ausgesuchteren Themenkomplex ein, doch auch sie bleiben meist aus den verschiedensten Gründen ein Monolog, der wohl die Sensibilisierung ermöglicht, die Erfahrung der Machbarkeit des Ganzen aber in der Regel ausschließt.

Theorie umzusetzen bedeutet immer, sich für die vorgestellten Verfahren mögliche Einsatzgebiete zu suchen und sie dann entsprechend anzuwenden. Gleichzeitig findet automatisch eine Einengung auf Teilgebiete statt. Die dafür geschaffenen Lehrformen sind Seminare und Praktika. Bei ersteren beschränkt sich der Praxisbezug (wenn vorhanden) meistens nur auf verbale Erklärungen oder eine Demonstration. Für unser Anliegen stellt das Praktikum somit die geeignetste Form dar, weil es wegen der Erfahrbarkeit und intensiven Vorführbarkeit des Stoffes Vorteile bietet. Da ein hohes Problembewußtsein angestrebt wird, überwiegen diese die leider auch vorhandenen Nachteile: größerer Aufwand bei Erstellung, Durchführung und Teilnahme im Vergleich zu Vorlesungen und Seminaren.

2 Das Konzept

2.1 Aufbau und Gliederung

Die sich sowohl aus inhaltlichen Wünschen als auch aus praktischen Erwägungen ergebenden Voraussetzungen sollen jetzt genannt werden. Gleichzeitig wird daraus die im Bild 1 festgehaltene Gliederung des Praktikums entwickelt.

Aus den verschiedensten Gründen wurde eine vollständige Eigenständigkeit des Praktikums angestrebt. Es sollte, um jedem ohne einen über das Praktikum hinausgehenden Zeitaufwand den Einstieg in den Themenbereich des teilnehmerüberprüfbaren Datenschutzes zu ermöglichen, losgelöst von weiteren Lehrveranstaltungen sein. Diese Eigenständigkeit beschert dem Praktikum eine große Flexibilität und Einsatzweite und dem Themengebiet hoffentlich auch ein großes Publikum. Diese Konzeption erfordert, daß alle im Praktikum behandelten Bereiche *im Praktikum selbst* hinreichend erläutert werden. Es muß eine in sich abgeschlossene Einheit bilden, die auf keinerlei weitere Information aus anderen Quellen angewiesen ist. Dies zieht eine gewisse Stoffülle und einen erhöhten Zeitaufwand bei der Bearbeitung nach sich, verschärft also den bereits bestehenden Zeitnotstand. Andererseits war eine zu allgemeine Behandlung der ausgewählten Themen zu vermeiden, um Praktikumsteilnehmer

mit Vorkenntnissen nicht zu langweilen oder bei einer eventuell doch bestehenden Einführungsvorlesung trotzdem noch interessante Sachverhalte präsentieren zu können.

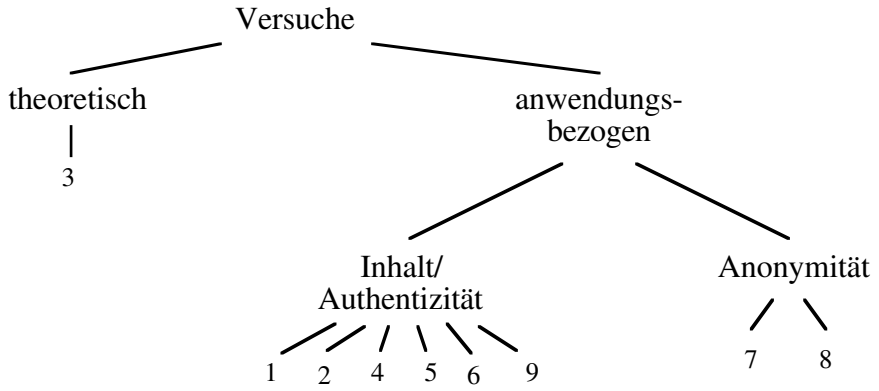

Bild 1: Inhaltliche Struktur des Praktikums

Diese Erwägungen resultierten in der im Bild 1 gezeigten Einteilung des Praktikums. Die drei ersten Versuche[3] machen die Praktikumsteilnehmer nicht nur mit der Thematik und den grundlegendsten Sachverhalten, sondern zugleich mit der Arbeitsumgebung (Rechner, System, Programmiersprache) vertraut. Dies geschieht einerseits durch die bewußt einfach gehaltenen Versuche 1 (Symmetrische Blockchiffren) und 2 (Betriebsarten von Blockchiffren), die direkt in die Kryptologie einführen. Ihr Ablauf entspricht den meisten folgenden Versuchen, so daß zu Beginn des Praktikums ein typischer Eindruck über das sich Anschließende hervorgerufen wird. Der Ablauf des sich anschließenden theoretischen Versuches 3 (Zahlentheoretische Algorithmen) ist untypisch, da hier besonders viel gelesen und fast nur mit Papier und Bleistift gearbeitet werden muß. Wegen der angestrebten Selbständigkeit des Praktikums und der für eine tiefere Behandlung von asymmetrischen kryptographischen Systemen (Versuche 4 und 5) häufig ungenügenden algebraischen, zahlentheoretischen und algorithmischen Kenntnisse ist solch ein Versuch nötig. Seine Durchführung erfolgt im Praktikum möglichst spät, um einerseits keine falschen ersten Eindrücke über die Ziele und die üblichen Abläufe der Versuche hervorzurufen und andererseits soviel Motivation bei der Durchführung der Versuche 1 und 2 anzusammeln, daß sie auch bei eher praktisch interessierten Teilnehmern für die zahlentheoretischen Algorithmen reicht. Die vorangestellte, gebündelte Behandlung immer wiederkehrender Sachverhalte, der Grundbausteine, erlaubt ein zügiges Formulieren der übrigen Versuche mit Minimierung der lästigen Redundanz und Konzentration auf Verfahren, die im Hinblick auf eine mögliche Anwendung vorgestellt werden. Darüberhinaus macht diese Einteilung das Praktikum auch didaktisch flexibel. Die bewußt einfacher gehaltenen ersten beiden Versuche und der von ihnen unabhängige dritte könnten – bei entsprechender Vorbildung – weniger intensiv behandelt oder ganz bzw. teilweise übersprungen werden, ohne gleich das gesamte Praktikum zum Zusammenbrechen zu bringen.

In dem anwendungsbezogenen Teil des Praktikums lassen sich weitere Einteilungen vornehmen. Betrachtet werden die bereits untersuchten Aspekte Vertraulichkeit, Authentizität und Anonymität. Jedem der folgenden Versuche läßt sich einer der Begriffe zuordnen.

Eine der Eingangsforderungen war, teilnehmerüberprüfbaren Schutz aufzuzeigen und entsprechende Verfahren vorzustellen. Diese Verfahren sollten dann in verteilten Systemen zur Anwendung kom-

---

3 Eine inhaltliche Kurzbeschreibung aller Versuche enthält Kapitel 3.

men. In der ersten Teilgruppe des anwendungsbezogenen Teiles des Praktikums („Inhalt/Authentizität“) werden die wichtigsten dieser Verfahren erläutert. Dabei ist zu beachten, daß sie durchaus noch nicht an verteilte Systeme gebunden sind; sie ließen sich auch in Einzelanwendungen oder bei persönlicher Kommunikation verwenden. Es ist aber wichtig festzuhalten, daß sie ebensogut in verteilte Systeme eingebettet werden können und dort erheblich zu der gewünschten Sicherheit beitragen. Unter diesem Gesichtspunkt werden sie, voneinander relativ unabhängig, der Reihe nach in einzelnen Versuchen vorgestellt. Aufeinander gebaut bilden sie so eine der tragenden Säulen des Praktikums.

Das große Themengebiet des Praktikums heißt verteilte Systeme. Sie setzen ein Kommunikationsnetz voraus, über welches auszutauschende Daten transferiert werden. Bislang wurde dieses Netz nie explizit erwähnt, da sich alle Verfahren um die Inhalte von Daten drehten. Diese können, wie in den vorangegangenen Versuchen gezeigt, ausreichend gesichert werden, auch wenn sie über ein von fremden Diensterbringern betriebenes Netz geschickt werden. Zwei Versuche beschäftigen sich mit dem Teilnehmer des Netzes und dessen Anonymität gegenüber „Fremden“. Im Gegensatz zu Vertraulichkeit und Authentizität geht es also bei der Anonymität nicht um die Inhalte von Daten, sondern, und dies rechtfertigt einen eigenen Teilbaum in der inhaltlichen Struktur, um die Kommunikationspartner.

Schließlich soll in diesem Praktikum die Machbarkeit von Verfahren dargestellt werden. Eine Beschränkung allein auf eine Einzelplatzanwendung oder eine kleine Praktikumsumgebung wirkt dabei wenig glaubhaft. Gezeigt werden muß, daß auch eine Einbettung in komplexere und realistische Sachverhalte durchaus denkbar und realisierbar ist. Aus diesem Grund ist ein Versuch, der zwischen den bislang behandelten Verfahren und alltäglichen Gegebenheiten Querbezüge herstellt, äußerst wichtig. Sinnvollerweise bildet er zugleich den Abschluß des Praktikums.

Inhaltlich gehört der Abschlußversuch mehr in die Gruppe „Inhalt/Authentizität“. Neben den oben genannten Gründen ist er auch didaktisch besonders wichtig, da hier Prinzipien nochmals aufgegriffen und miteinander kombiniert werden. Er kann als Zusammenfassung in Form eines Beispieles verstanden werden und überdacht so das gesamte Praktikum.

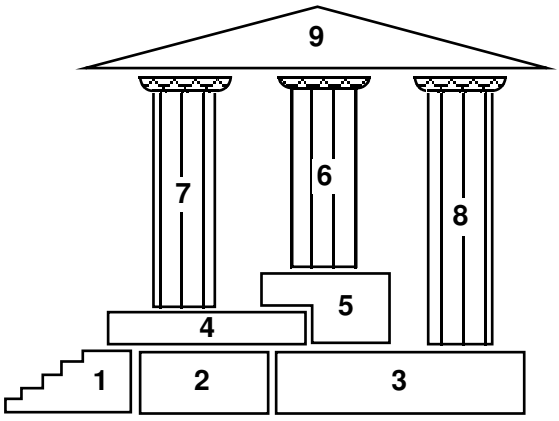

Bild 2: Der Tempel der Praktikums-Weisheit

2.2 Gestaltung

Die inhaltliche Struktur des Praktikums sagt noch nichts über die Gestaltung, geschweige denn über eine realistische Durchführung des Praktikums aus. Die inhaltliche Gestaltung richtet sich nach dem gegebenen Rahmen und orientiert sich an dem, was innerhalb der Lehrform *Praktikum* sinnvoll

vermittelt werden kann. Die Durchführbarkeit ist abhängig von den Gegebenheiten des Durchführungsortes, betrifft also mehr die organisatorischen Dinge. Beides soll in den nachfolgenden Abschnitten näher beschrieben werden. Es sei schon an dieser Stelle erwähnt, daß die Beschreibung der organisatorischen Sachverhalte nicht mehr als die Darlegung der ursprünglichen Gedanken hierüber sein kann, allenfalls noch eine Empfehlung für die Handhabung des Praktikums.

Die Intention eines Praktikums legt nahe, nicht benötigte Theorie außen vor zu lassen. Durch Versuch 3 können die theoretischen Sachverhalte dennoch ausführlich und in einer kompakten Form vermittelt werden. Dabei wurden allerdings nur die allernötigsten Beweise ausgeführt; als Konzession an Umfang und Zeit wurden die meisten durch die entsprechenden Literaturverweise ersetzt. Genauso verhielt es sich in allen anderen Versuchen. Beweise und ausführliche Argumentationen sind Vorlesungen oder Seminaren vorbehalten, im Praktikum muß mit einer knapperen Darstellung zugunsten anderer Schwerpunkte vorlieb genommen werden.

Einer dieser Schwerpunkte ist in diesem Praktikum die Darstellung von Schwächen und Mängeln der vorgestellten Verfahren. Es wurde gleichermaßen viel Wert darauf gelegt, die Verfahren klar und plausibel zu erklären und gleichzeitig *alle bekannten Schwachstellen offenzulegen*. Gerade das letzte Ansinnen wurde dann in die Aufgaben der einzelnen Versuche verlagert, um die Praktikumsteilnehmer nicht im Glauben eines Allheilmittels zu bestärken. Gezieltes Experimentieren oder Ausknobeln von Angriffsstrategien gegen ein Verfahren soll die jeweiligen Schwachpunkte aufdecken.

Im Bereich des Informatikstudiums ist Praktikum nicht selten ein Synonym für Programmierarbeit – leider. Sicherlich ist es nicht leicht, eine andere *praktische* Tätigkeit als das Programmieren zu finden, doch ist immer auf eine ausgewogene Mischung zwischen zu vermittelnden Inhalten und dieser Tätigkeit zu achten. Schließlich soll möglichst effizient gelernt und nicht möglichst ausdauernd programmiert werden. Konzeptionell wurde das Programmieren auf das Auffüllen von Programmierrahmen beschränkt, um eine interessante und dennoch in begrenzter Zeit erfüllbare Aufgabenstellung zu gewährleisten. Doch auch hier war das Problem, was interessant, wichtig oder notwendig ist, nicht immer leicht entscheidbar. Die Gratwanderung ist schwierig. Eine einheitliche Form wurde für dieses Praktikum nicht gefunden, genausowenig übrigens, wie sich die Teilnehmer auf einen einheitlichen Wunsch hierfür einigen konnten. Doch davon später.

Für die Durchführung ist das Praktikum als eine vier Semesterwochenstunden umfassende Veranstaltung konzipiert. Nicht mitgerechnet sind dabei die zwei bis vier Stunden Vorbereitungszeit für jeden Versuch. (Da die Versuche in Umfang und Verhältnis Dokumentation zu Aufgaben schwanken, können hierzu keine spezielleren Angaben gemacht werden. Näheres findet sich bei der Beschreibung der einzelnen Versuche.) Die Versuche sollten in Zweier- oder Dreiergruppen bearbeitet werden. Das Praktikum kann dann für eine größere Anzahl von Teilnehmern angeboten werden. Die in der Gruppe stattfindenden Gespräche fördern zudem das Verständnis des Stoffes. Der Betreuungsaufwand liegt für fünf bis sieben Zweiergruppen bei zwei bis drei Tutoren. Zwecks leichter Nivellierung der möglicherweise unterschiedlichen Ausgangspositionen der einzelnen Gruppen sollten allgemeine Fragen vor der Durchführung des Versuches abgeklärt werden, ebenso ist eine abschließende Besprechung aller Praktikumsteilnehmer nach den einzelnen Versuchen einer Synchronisation dienlich. Hierfür stehen auch Musterlösungen zur Verfügung, die der Gesamtgruppe angepaßt eingesetzt werden sollten.

Aus organisatorischen und didaktischen Gründen wurde *eine* Programmiersprache für alle Versuche als verbindlich festgelegt. Sie mußte allen Anforderungen der einzelnen Versuche genügen und gleichzeitig hinlänglich bekannt sein, um zeitraubendes und von der Thematik ablenkendes Einarbeiten in diese Sprache zu vermeiden. Außerdem muß nicht nur ein Übersetzer, sondern auch eine kom-

fortable Programmierumgebung vorhanden sein. Da zu Beginn der Arbeiten weder für Ada noch für Modula eine komfortable Programmierumgebung zur Verfügung stand, fiel die Wahl auf THINK-Pascal, Version 3.0[4] [PASCAL_90], eine um das Modul-Konzept erweiterte Version von Standard-Pascal [JeWi_85] für den Apple Macintosh Rechner, System 6 [MacTI_87], für den die Praktikumssoftware geschrieben wurde. Diese Rechner standen zum Zeitpunkt der Entwicklung in ausreichender Menge an der Universität Karlsruhe, dem Geburtsort des Praktikums, zur Verfügung[5].

2.3 Formen

Das Praktikum setzt sich aus verschiedenen Einzelarbeiten zusammen, die ebenso verschieden ausgefallen sind. Dies macht sich besonders im Stil und Aufbau der Versuche bemerkbar, vor allen Dingen aber in der Form, wie die einzelnen Aufgaben in den Versuchen gestaltet sind. Vier Typen lassen sich aus dem Praktikum herausarbeiten, und jeder Typ hat für sich eine konzeptionelle wie auch historische Komponente.

Allen Versuchen ist jedoch gemeinsam, daß es nicht um die Kontrolle des durchgearbeiteten Stoffes geht. Es wird eine freiwillige und engagierte Mitarbeit der Praktikumsteilnehmer vorausgesetzt, die nur des eigenständigen Interesses am Verständnis des Stoffes wegen am Praktikum teilnehmen – so, wie es an der Universität eigentlich sein sollte. (Nur um ein allzu leichtes Trittbrettfahren zu vermeiden, wurde von dem ursprünglichen Gedanken, die Musterlösungen gleich mit auszugeben, abgesehen.)

Der Gesamtausführung nach orientiert sich das Praktikum am exemplarischen Prinzip [Gern_72]. Die Auswahl der einzelnen Themen der Versuche (dem Kampf gegen die Stoffülle gleich, siehe [Flit_55, Wage_58]) richtete sich nach thematischen Kriterien: Genau die Gebiete sollen behandelt werden, die als wesentlich und wichtig erachtet werden. Die Anordnung der Versuche selbst erfolgte dann wieder systematisch, gebunden an die Prämissen der Eigenständigkeit und den sich daraus ergebenden Konsequenzen für das Praktikum (vgl. hierzu auch [Derb_57]).

Der zweite Schritt des exemplarischen Prinzips, die Abstraktion, bleibt dem Praktikumsteilnehmer überlassen. Eingehende Metabehandlungen würden den Rahmen des Praktikums sprengen. Als hilfreich haben sich abschließende (Gesamt-)Gruppenbesprechungen nach jedem Versuch erwiesen.

Doch nun zu den vier Versuchstypen im Praktikum.

Der Allerweltsversuch: Experimentieren an einzelnen Rechnern
Unter diesen Typ fallen die meisten Versuche. Es sind die Nummern 1, 2, 4, 5, 7 und 9. Sie werden deswegen als „normale“ Versuche bezeichnet, weil sie das übliche Bearbeitungsschema unterstützen: Lesen und Verstehen, dann Austausch mit Anderen, dann Problem lösen und testen und schließlich Abschlußbesprechung. Nichtsdestotrotz sind viele Variationen innerhalb der Versuche möglich. Die gravierendsten Unterschiede ergeben sich bei der Art der Aufgabenstellung. Die Anordnung der Aufgaben, ob nun dem fließenden Text untergeschoben (Versuche 4, 7 und 9) oder am Ende der Unterlagen gestellt (Versuche 1, 2 und 5) sei dabei als nebensächlich angesehen. Wichtig bei diesem Punkt ist allein die Unabhängigkeit einer Aufgabe von der Lösung der vorhergehenden.

Der didaktische Hintergrund bei dieser Form von Versuchen ist das nochmalige, selbständige Aufarbeiten der in den Unterlagen gelieferten Informationen. Zwei verschiedene Intentionen kommen vor:

---

4 Inzwischen wurde auch erfolgreich auf THINK-Pascal Version 4.0 und auf Apple Macintosh System 7 umgestellt.

5 Die meisten der in den Versuchen auftauchenden Kryptoverfahren stehen auch für PCs (80x86) zur Verfügung. Langfristig ist es geplant, daß komplette Praktikum auch für PCs verfügbar zu machen.

Einmal sollen die wesentlichen Teile aus dem gegebenen Text extrahiert und zum Lösen der Aufgaben verwendet werden. Hier steht das Vertiefen des Stoffes im Vordergrund. Die andere Variation setzt den gegebenen Text als Basis für weitere, darüberhinausgehende Erkenntnisse. Diese Erkenntnisse sollten wesentliches zum Thema beitragen, etwa einen zentralen Satz oder eine wichtige Bedingung. Den Aufgaben kommt also die Rolle der Anleitung zur Neukombination der gegebenen Informationen zu. Beides entspricht der eingangs geschilderten Intention der Aufgaben.

Nach der thematischen Bewertung, was wichtig ist und was gezeigt werden soll, bleibt die systematische Aufbereitung des ausgewählten Stoffes mit dem Versuch, eine argumentativ lückenlose Gestaltung zu finden. Aus didaktischen Erwägungen dürfen innerhalb des Versuches keine Argumente fehlen; Lücken sind als „weiterführende“ Gebiete zu tarnen und entsprechend mit Literaturhinweisen auszustatten. Unterstützend wirken immer anschauliche Graphiken (siehe z.B. Bild 2: Der Tempel der Praktikums-Weisheit). Kernpunkte sind natürlich die Aufgaben innerhalb eines Versuches; ihnen ist besondere Aufmerksamkeit zu widmen. Neben den organisatorischen Gesichtspunkten, wie etwa zu erwartender Bearbeitungsaufwand, ist besonders der Grad der Schwierigkeit zu beachten und dessen Angemessenheit im Verhältnis zu Kontext und Mächtigkeit der Aufgabe zu bewerten. Gerade bei Programmieraufgaben ist diese Abschätzung kritisch, da hier die Relation zwischen dem eigentlichen Knackpunkt und dem Arbeitsaufwand eher ungünstig ausfällt.

Die Demonstration

Werden für eine geeignete Programmierumgebung oder für das zu Zeigende mehr als ein Rechner benötigt, dann ist Experimentieren als Lernform ungeschickt. Das Problem entsteht bei Fehlern, die sich auf alle beteiligten Rechner auswirken. Dadurch entsteht ein enormer organisatorischer Überhang, etwa das lästige Zurücksetzen (z.B. Neustart) aller Rechner auf einen Ausgangszustand bei Fehlern. Hierfür ist nicht die Unfähigkeit der Versuchsgestalter bei der Absicherung einer Versuchsumgebung verantwortlich, sondern der Gegensatz zwischen einer notwendigerweise restriktiven Absicherung gegen alle möglichen Fehler und der gewünschten Offenheit des Experimentierfeldes. Ein zufriedenstellender Mittelweg kann nicht gefunden werden.

Eine Lösung des Problems besteht in der Erstellung einer Simulation der gewünschten Umgebung, die aber auf *einem* Rechner läuft, somit den möglichen Fehlerraum lokal hält. Diese Möglichkeit wurde etwa in Versuch 7 gewählt. Versuch 8 geht den anderen Weg. Alle Aufgaben sind allein mit Papier und Bleistift zu lösen, eine Programmieraufgabe wird bewußt ausgeschlossen.

Um dennoch die Machbarkeit der vorgestellten Verfahren zu beweisen und die Sachverhalte nochmals praktisch zu verdeutlichen, schließt sich den zugegebenermaßen theoretischen Aufgaben eine Demonstration an, die – da von den kundigen Tutoren geleitet – relativ kontrolliert und fehlerfrei abgewickelt werden kann. Der Didaktik wird diese Versuchsform dann und nur dann gerecht, wenn die Demonstration ausführlich kommentiert und erläutert wird. Eine funktionierende Umgebung, die ein Experimentieren mit den in dem Versuch gewonnenen Erkenntnissen erlaubt, will und kann sie nicht sein, da eine solche Umgebung gegen die möglichen Fehler genauso gesichert sein müßte, wie ein Programmierrahmen auch. Dies wurde aber aus den oben genannten Gründen gerade verworfen.

Das Tutorium

Sicherlich eine ungewöhnliche Form für ein Praktikum. Für den Versuch 3, der sich der algebraischen Fundamente annimmt, aus folgenden Gründen aber verständlich und akzeptabel. Abweichend von der grundsätzlichen Einstellung, die Praktikumsteilnehmer seien willens, sich durch jede Materie zu quälen, wird bei den äußerst wichtigen mathematischen Grundlagen besonderer Wert auf sorgfältiges Durcharbeiten gelegt. Wenn eine Vorbereitung des Versuches zu Hause gefordert wurde,

dann läßt sich die Erfüllung dieser Forderung leicht durch eine Besprechung einzelner Fragen in der Gruppe klären. Den Tutoren kommt dann die Rolle der Beantworter von Fragen und der Diskussionsleitung zu. Andererseits ist die Durchführung des Versuches auch gleich in der Gruppe denkbar, eben einem Tutorium (an der Universität) gleich. Hier leisten die Tutoren Hilfestellungen und kontrollieren die Lösungen von Aufgaben, gleichzeitig also die Durcharbeitung des Stoffes.

Die Aufgaben und Beispiele folgen, wie im klassischen Mathematikunterricht üblich, dem bereits erwähnten exemplarischen Prinzip.

Diese Form ist nicht ganz ungefährlich, weil sie leicht in einen Vortrag des Tutors abzurutschen droht. Dann wird nur zu leicht die so schändliche Konsumhaltung eingenommen, ohne daß wirklich etwas verstanden worden wäre.

Das Lernsystem
Ein besonderer Versuch wird der Versuch 6 sein. Hier sollen die Methoden des rechnergestützten Lernens („Lernsysteme“) eingesetzt werden. Daraus ergibt sich, nach dem bisherigen Entwurf, eine sich aufbauende und entwickelnde Darstellung des Stoffes. Rekapitulierende Fragen, auf Fragebögen zusammengestellt und den Versuchsunterlagen beigefügt, wiederholen das auf dem Bildschirm Durchgeblätterte.

Da dieser Versuch noch nicht fertiggestellt ist, kann weiteres nur spekulativ geäußert werden. Darum sei an dieser Stelle zunächst einmal auf die entsprechende Literatur über Lernsysteme verwiesen, etwa [EJLS_87, SeLi_89].

3 Die Versuche

In diesem Kapitel werden die im Praktikum enthaltenen Versuche beschrieben. Die Beschreibung erfolgt chronologisch, so wie die Versuche bearbeitet werden. Nur die Inhalte werden kurz beleuchtet, für detailliertere, didaktische Hintergründe und Erfahrungen ist an dieser Stelle kein Platz. Die Angabe der Literatur für einen Versuch erfolgt äußerst spezifisch. Bei Recherchen ist gegebenenfalls die in den zuvor beschriebenen Versuchen erwähnte Literatur hinzuzuziehen.

Versuch 1: Symmetrische Blockchiffren
Der erste Versuch befaßt sich, in Anlehnung an die historische Entwicklung, mit symmetrischen Blockchiffren. Es wird das Prinzip der Feistel-Chiffre (nach H. Feistel) (Stichworte: Iterationsrunde, Vertauschung von Halbblöcken) und ein bedeutender Vertreter dieser Chiffre erklärt: DES (Stichworte: Permutationen, S-Boxen, Teilschlüssel). Kritik an DES und diesbezüglich weiterführende Literatur schließen den Versuch ab.
Literatur: [Aßma_88, DDFG_84, DES_77, PfAß1_90]

Versuch 2: Betriebsarten von Blockchiffren
Nach einer zwischen Block- und Stromchiffren differenzierenden Einleitung werden die wichtigen Betriebsarten von Blockchiffren und deren Zusammenhänge erklärt. Ihre Verwendung und ihre Schwächen bei Konzelation und Authentikation werden beschrieben, wobei bzgl. letzterem eine Einschränkung auf symmetrische Verfahren gemacht wird. Die behandelten Betriebsarten sind im einzelnen: Electronic Codebook Mode (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB) und Plain Cipher Block Chaining (PCBC).
Literatur: [DaPa_83, DaPr_89, MeMa_82, Pfit_89]

Versuch 3: Zahlentheoretische Algorithmen
Aufbauend auf den Grundlagen der Komplexitätstheorie und einer modularen Arithmetik werden elementare Algorithmen aus dem Bereich der Zahlentheorie und der Algebra beschrieben. Dies sind unter anderen der „Square and Multiply"-Algorithmus, der Euklidsche Algorithmus und der Chinesische Restealgorithmus. Im Hinblick auf die kommenden Versuche werden außerdem quadratische Reste (Stichworte: Legendre- und Jacobi-Symbol), Primalitätstests (Stichwort: Rabin-Miller-Test) und Blum-Zahlen eingeführt.
Literatur: [Bleu_91, Bund_88, Horn_76, Lips_81, Ries_87]

Versuch 4: Asymmetrische Konzelationssysteme
Einer formalen Einführung von asymmetrischen Konzelationssystemen (mit Abgrenzung von den bereits eingeführten symmetrischen) folgen die Begriffserläuterungen der charakteristischen Stichworte „öffentliche und geheime Schlüssel" und „Einbahnfunktion mit Geheimnis" (trapdoor one-way function). Um anschließend die Schwächen der vorgestellten Verfahren präziser beschreiben zu können, erfolgt ein Blick auf passive und aktive Angriffe und Angreifermodelle. Als ein wichtiger Vertreter von asymmetrischen Konzelationsverfahren wird RSA vorgestellt; im sich anschließenden Versuch wird am durchaus realistischen Szenario eines Euroscheckformulars demonstriert, daß der Einsatz von RSA als deterministisches Konzelationssystem nicht unbedingt Vertraulichkeit garantiert. Als Alternative werden dann noch probabilistische Verschlüsselungen (Stichworte: Blum-Goldwasser-System, kryptographisch starke Pseudozufallsgeneratoren) eingeführt.
Literatur: [BlBS_86, Bleu_91, BlGo_85, Denn_84, DiHe_76, RSA_78]

Versuch 5: Digitale Signatursysteme
Lehnt sich Versuch 4 hauptsächlich an den Begriff der kryptographisch sicheren Konzelation an, so steht in diesem Versuch der Begriff der Authentikation im Mittelpunkt. Dem geht eine formale Einführung des Begriffes „digitales Signatursystem" voraus. Das in Versuch 4 vorgestellte asymmetrische Kryptoverfahren RSA wird hier nocheinmal aufgegriffen und auf Tauglichkeit für Authentikation geprüft (Aufgabe als Angriff auf RSA gestaltet). Als Verbesserungen werden Hashfunktionen angeführt, und schließlich mündet alles in das digitale Signatursystem GMR. Es ist hervorzuheben, daß dieser Versuch extrem auf die in Versuch 3 behandelten Themen zurückgreift.
Literatur: [DaPr_89, FoPf_91, Fox3_91, GoMR_88]

Versuch 6: Schlüsselaustausch und Ende-zu-Ende-Verschlüsselung
Dieser Versuch behandelt sichere und authentische Schlüsselverteilalgorithmen in verteilten Systemen. Unterschieden werden symmetrischer und asymmetrischer Schlüsselaustausch mit anschließender Untersuchung der Erweiterungsmöglichkeiten zu hybriden Protokollen. Die Sicherheit der Protokolle wird mit simulierten Angriffen getestet.
Literatur: [DaPr_89, Hamm_92, NeSc_78, NeSc_87, OtRe_87]

Versuch 7: Das MIX-Netz
In diesem und dem folgenden Versuch wird die Anonymität eines Netzteilnehmers ins Rampenlicht gezerrt, also eine vollkommen andere Zielrichtung eingeschlagen. Die Idee des zur Erreichung der Anonymität eingesetzten Verfahrens (Stichwort: MIX) wird ausführlich dargelegt und die Funktionsweise anhand eines einfachen Schemas (Stichwort: Senderanonymität) erklärt. Vor allzu sorglosem Einsatz von RSA wird auch hier mit einem Angriff, als Aufgabe gestaltet, gewarnt. Als Abschluß wird auf mögliche Erweiterungen und Verbesserungen hingewiesen (Stichworte: Empfängeranonymität, Kanäle).
Literatur: [Chau_81, Ort_91, Pfit_89]

Versuch 8: Das DC-Netz
Mit der gleichen Grundthematik wie Versuch 7 beschäftigt, stellt dieser Versuch ein anderes Konzept zur Wahrung der Anonymität vor: Das DC-Netz. Im Gegensatz zu dem MIX-Netz ist es sogar informationstheoretisch sicher (das MIX-Netz nur komplexitätstheoretisch), leider aber wesentlich ineffizienter. Neben der prinzipiellen Funktionsweise enthält dieser Versuch auch den zugehörigen Sicherheitsbeweis. Ein weiteres Problem, nämlich das der Kollisionen von Nachrichten, und dessen Lösungsmöglichkeiten werden in dem zweiten Teil des Versuches behandelt.
Literatur: [Bött_90, Chau_88, Pfit_89]

Versuch 9: Wertetransfersysteme
Der abschließende Versuch greift vieles der vorausgegangenen nochmals auf und stellt es in den Kontext von Wertetransfersystemen. Es werden die Sicherheit und die Unbeobachtbarkeit von Zahlungssystemen untersucht (Stichworte: Blind geleistete Signaturen, Pseudonyme). Abschließend wird auf die Problematik beim Werteaustausch (Stichwort: Unteilbarkeit) eingegangen.
Literatur: [BüPf_90, Chau_89, PWP_90, Schm_91]

4 Schluß

4.1 Erfahrungsbericht

Ein erster inoffizieller Probedurchlauf mit Teilen des beschriebenen Praktikums erfolgte als Blockveranstaltung im Juli 1990 am Institut für Rechnerentwurf und Fehlertoleranz der Universität Karlsruhe. Dieser Probedurchlauf bestätigte die Richtigkeit der Konzeption und Dimensionierung des Praktikums.

Das vollständige Praktikum wurde als Blockveranstaltung im Wintersemester 1991/92 an der Universität Hildesheim durchgeführt. Es nahmen fünf Gruppen zu je zwei Teilnehmern teil. An dieser Stelle sollen die wichtigsten Erfahrungen dieses Durchlaufes kurz genannt werden. Dabei sind die bisher erwähnten Prämissen und Ziele im Auge zu behalten.

Begleitende Vorlesung: Von der Eigenständigkeit des Praktikums unberührt, gab es in Hildesheim im vorangegangenen Sommersemester 1991 eine zu dem Praktikum passende Einführungsvorlesung mit Übungen. Diese Vorlesung war von drei Fünftel der Praktikumsteilnehmer besucht worden, die darüberhinaus im Wintersemester 1991/92 begleitend an einem Seminar über Theorie und Einsatz digitaler Signatursysteme teilnahmen. Die restlichen zwei Fünftel absolvierten das Praktikum ohne einschlägige Vorbildung, wobei die Hälfte von ihnen auch noch nicht sehr versiert im Programmieren war. Um so erstaunlicher und befriedigender ist es demnach, daß beide Gruppen, also die mit und die ohne Vorkenntnisse, mit dem Praktikum zufrieden waren und sich in der Bearbeitungszeit pro Versuch um nur ca. eineinhalb Stunden unterschieden.

Betreuungsaufwand: Die Anzahl der betreuenden Tutoren unterlag kurzfristigen Schwankungen, doch kann „zwei“ als Mittelwert genannt werden. Von einer Überforderung der Tutoren kann nicht gesprochen werden, so daß auch wegen der zu erwartenden Perfektionierung der Versuchsunterlagen die Anzahl der Gruppen bei gleichbleibender Betreuung etwa auf sieben gesteigert werden könnte.

Bearbeitungsaufwand: Das Praktikum wurde als Blockveranstaltung in acht vollen Tagen durchgeführt. Die Tage begannen um neun Uhr morgens und endeten (für die Praktikumsteilnehmer) zwischen sechs und neun Uhr abends, wobei eine eineinhalbstündige Mittagspause eingelegt wurde. Ein kürzerer Zeitraum dürfte der Erfahrung nach kritisch werden, da Versuch 6 zukünftig etwas mehr

Zeit beanspruchen wird. Die Durchführungsform der Blockveranstaltung hat sich bewährt, doch dürfte auch einer wöchentlichen Abarbeitung der Versuche verteilt über das Semester nichts im Wege stehen.

Programmiersprache: Obwohl in Hildesheim im Grundstudium die Programmiersprache Modula 2 [Wirt_83] im Vordergrund steht, gab es nur geringfügige, bei einer Einarbeitung in eine andere Sprache nur allzu natürliche Probleme.

Programmierrahmen: Ein strittiges Thema, nicht nur unter den Erstellern des Praktikums, sondern auch bei den Rezipienten. Den einen war es zu wenig Programmiererei, den anderen zu viel; die einen wollten die große Freiheit und dementsprechend wenig Vorgaben, den anderen waren die Anleitungen gerade recht und wieder andere stöhnten angesichts einer zu großen Komplexität der Strukturen. Angesichts dieser Erfahrung dürfte die Palette der Angebote in diesem Praktikum zufriedenstellend sein: Für jeden ist etwas dabei. Dementsprechend wurde an den einzelnen Versuchen nicht viel geändert; nur schwere, detaillierte Kritik an didaktisch ungünstigen Darstellungen wurde aufgenommen und verarbeitet.

4.2 Ausblick

Im Sommersemester 92 findet an der Universität Hildesheim semesterbegleitend ein Praktikum „Schutz in verteilten Systemen durch Kryptologie für Fortgeschrittene" (Praktikum 2) statt, in dem gemeinsam Aufgaben definiert, aufgeteilt und gelöst werden sollen. Hier gibt es natürlich keine vorbereiteten Versuchsunterlagen und insbesondere keine Musterlösungen. Die Stoffülle für den einzelnen Teilnehmer wird zwangsläufig kleiner, das Programmieren anstrengender – dafür die Eigenverantwortlichkeit und Gestaltungsfreiheit größer. Das Praktikum 2 verfolgt also andere Ziele als das in diesem Papier beschriebene Praktikum 1. Wir sind gespannt, wie die Teilnehmer zurechtkommen und wie sehr sich die Teilnahme an Vorlesung, Seminar und Praktikum 1 für den Arbeitsfortschritt bei Praktikum 2 auszahlt.

Bild 3 faßt zusammen, wie die Ausbildung im Bereich „Schutz in verteilten Systemen durch Kryptologie" in den nächsten Jahren an der Universität Hildesheim geplant ist.

Gerne geben wir unsere Erfahrungen mit den erwähnten Lehrveranstaltungen an Interessenten weiter, insbesondere auch die erwähnten ausführlichen Versuchsunterlagen inkl. Programme und Anleitungen für die Tutoren zur Versuchsdurchführung für Praktikum 1. Sind vernetzte Apple Macintoshs mit mindestens 4 MByte Arbeitsspeicher und Festplatte sowie THINK-Pascal vorhanden, so kann das Praktikum mit nach unserer Schätzung etwa 2 Personenmonaten Vorbereitungsaufwand zur Erarbeitung des Tutorenwissens durchgeführt werden. Über Rückmeldungen und Kritik würden wir uns freuen.

Eine offene Frage ist für uns, ob die Versuchsunterlagen, Programme und Anleitungen zur Versuchsdurchführung soweit vervollkommnet werden können, daß das Praktikum 1 ohne Hilfe (insbesondere also ohne Tutoren) auch im außeruniversitären Bereich durchgeführt werden kann. Gelänge das, so würde die zu Beginn des Papieres angesprochene Verbreitung eines Bewußtseins für Sicherheitsprobleme und Schutzmöglichkeiten sehr erleichtert.

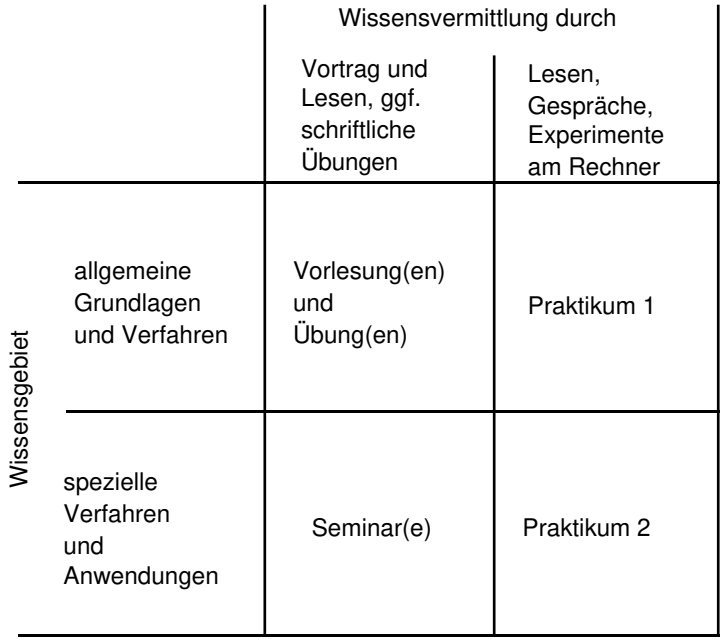

Bild 3: Ausbildung im Bereich „Schutz in verteilten Systemen durch Kryptologie“

5 Ein herzliches Dankeschön

an *Karlheinz Hammerer* für seine Implementierungsarbeiten im Bereich Schlüsselaustausch (Versuch 6), *Johannes Krohn* für manchen Tip zum Mac, *Jörg Lukat* für Hilfe beim Einarbeiten in AppleTalk, *Andreas Schmidt* für die Realisierung von Versuch 9 sowie einen Teil der Implementierung von Versuch 2 und *Jan-Peter Wilhelms* für das Installieren und Testen der Software an der Universität Hildesheim sowie an die 14 *Teilnehmer* der beiden Praktikumsdurchläufe für ihre Mitarbeit und Kritik.

6 Literatur

Aßma_88 Ralf Aßmann: Effiziente Software-Implementierung von verallgemeinertem DES; Diplomarbeit am Institut für Rechnerentwurf und Fehlertoleranz der Universität Karlsruhe, Februar 1989.

BlBS_86 L. Blum, M. Blum, M. Shub: A Simple Unpredictable Pseudo-Random Number Generator; SIAM J. Comput. 15/2 (1986) 364-383.

Bleu_91 Gerrit Bleumer: Eine Praktikumsumgebung für Kryptoprotokolle sowie Erstellung der Versuche „Zahlentheoretische Algorithmen“ und „Asymmetrische Konzelationssysteme“; Diplomarbeit am Institut für Rechnerentwurf und Fehlertoleranz der Universität Karlsruhe 1991.

BlGo_85 Manuel Blum, Shafi Goldwasser: An Efficient Probabilistic Public-Key Encryption Scheme Which Hides All Partial Information; Crypto '84, LNCS 196, Springer-Verlag, Berlin 1985, 289-299.

Bött_90 Manfred Böttger: Realisierung des DC-Netz-Versuchs und einer einheitlichen Praktikums-Netzschnittstelle; Diplomarbeit am Institut für Rechnerentwurf und Fehlertoleranz der Universität Karlsruhe, Juli 1990.

Bund_83 Bundesverfassungsgericht: Das Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983 - 1 BvR 209/83 u. a.; Datenschutz und Datensicherung DuD /4 (1983) 258-281.

Bund_88 Peter Bundschuh: Einführung in die Zahlentheorie; Hochschultext, Springer-Verlag, Heidelberg 1988.

BüPf_90 Holger Bürk, Andreas Pfitzmann: Value Exchange Systems Enabling Security and Unobservability; Computers & Security 9/8 (1990) 715-721.

Chau_81 David Chaum: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms; Communications of the ACM 24/2 (1981) 84-88.

Cha8_85 David Chaum: Security without Identification: Transaction Systems to make Big Brother Obsolete; Communications of the ACM 28/10 (1985) 1030-1044.

Chau_88 David Chaum: The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability; Journal of Cryptology 1/1 (1988) 65-75.

Chau_89 David Chaum: Privacy Protected Payments - Unconditional Payer and/or Payee Untraceability; SMART CARD 2000: The Future of IC Cards, Proceedings of the IFIP WG 11.6 International Conference; Laxenburg (Austria), 19.-20.10.1987, North-Holland, Amsterdam 1989, 69-93.

DaPa_83 D. W. Davies, G. I. P. Parkin: The Average Cycle Size of the Key Stream in Output Feedback Encipherment; Cryptography; Proceedings, Burg Feuerstein 1982, Edited by Thomas Beth; LNCS 149, Springer-Verlag, Heidelberg 1983, 263-279.

DaPr_89 D. W. Davies, W. L. Price: Security for Computer Networks, An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer; (2nd. ed) John Wiley & Sons, New York 1989.

DDFG_84 Marc Davio, Yvo Desmedt, Marc Fosséprez, René Govaerts, Jan Hulsbosch, Patrick Neutjens, Philippe Piret, Jean-Jacques Quisquater, Joos Vandewalle, Pascal Wouters: Analytical characteristics of the DES; Crypto '83, David Chaum (ed.) Plenum Press, New York 1984, 171-202.

Denn_84 Dorothy E. Denning: Digital Signatures with RSA and Other Public-Key Cryptosystems; Communications of the ACM 27/4 (1984) 388-392.

DES_77 Specification for the Data Encryption Standard; Federal Information Processing Standards Publication 46 (FIPS PUB 46), January 15, 1977.

Derb_57 Joseph Derbolav: Das „Exemplarische“ im Bildungsraum des Gymnasiums. Versuch einer Ortbestimmung des exemplarischen Lernens, 1957; aus [Gern_72].

DiHe_76 Whitfield Diffie, Martin E. Hellman: New Directions in Cryptography; IEEE Transactions on Information Theory 22/6 (1976) 644-654.

EJLS_87 Dieter Euler, Ralf Jankowski, Andreas Lemz, Paul Schmitz, Martin Twardy: Computerunterstützter Unterricht: Möglichkeiten und Grenzen; Vieweg, Braunschweig 1987.

Flit_55 Wilhelm Flitner: Der Kampf gegen die Stoffülle: Exemplarisches Lernen, Verdichtung, Auswahl, 1955; aus [Gern_72].

FoPf_91 Dirk Fox, Birgit Pfitzmann: Effiziente Software-Implementierung des GMR-Signatursystems; Proc. Verläßliche Informationssysteme (VIS'91), März 1991, Darmstadt, Informatik-Fachberichte 271, Springer-Verlag, Heidelberg 1991, 329-345.

Fox3_91 Dirk Fox: Unterlagen zu Versuch 5 „Digitale Signatursysteme“.

Gern_72 Berthold Gerner: Das exemplarische Prinzip – Beiträge zur Didaktik der Gegenwart; (5. ed.) Wege der Forschung Band XXX, Wissenschaftliche Buchgesellschaft, Darmstadt 1972.

GoMR_88 Shafi Goldwasser, Silvio Micali, Ronald R. Rivest: A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks; SIAM J. Comput. 17/2 (1988) 281-308.

Hamm_92 Karl-Heinz Hammerer: Softwareimplementierung eines rechnergestützten Einführungskurses über Schlüsselaustausch und Ende-zu-Ende-Verschlüsselung in einer Versuchsumgebung; Diplomarbeit am Institut für Rechnerentwurf und Fehlertoleranz der Universität Karlsruhe, in Vorbereitung.

Horn_76 Bernhard Hornfeck: Algebra; 3. Auflage, de-Gruyter-Lehrbuch; Walter de Gruyter & Co, 1976.

JeWi_85 Kathleen Jensen, Niklaus Wirth: User Manual and Report, (3. ed.), ISO Pascal Standard; Revised by A. B. Mickel, J. F. Miner, Springer-Verlag, Heidelberg 1985.

Lips_81 John D. Lipson: Elements of algebra and algebraic computing; Addison-Wesley Publishing Company, Advanced Book Program; Reading, Mass. 1981.

MacTI_87 Macintosh: Technical Introduction to the Macintosh Family; Addison Wesley Publishing Co., Inc., Reading, 1987.

MeMa_82 Carl H. Meyer, Stephen M. Matyas: Cryptography - A New Dimension in Computer Data Security; (3rd printing) John Wiley & Sons, 1982.

NeSc_78 Roger M. Needham, Michael D. Schroeder: Using Encryption for Authentication in Large Networks of Computers; Communications of the ACM 21/12 (1978) 993-999.

NeSc_87 R. M. Needham, M. D. Schroeder: Authentication Revisited; Operating Systems Review 21/1 (1987) 7.

Ort_91 Andreas Ort: Implementierung eines MIX-Netzes sowie Konzeption und Realisierung des MIX-Netz-Versuches; Diplomarbeit am Institut für Rechnerentwurf und Fehlertoleranz der Universität Karlsruhe, Frühjahr 1991.

OtRe_87 Dave Otway, Owen Rees: Efficient and Timely Mutual Authentication; Operating Systems Review 21/1 (1987) 8-10.

PASCAL_90 Symantec Corporation: THINK Pascal, The Fastest Way to Finished Software; User Manual, Symantec Corporation, 1990.

PfAß1_90 Andreas Pfitzmann, Ralf Aßmann: More Efficient Software Implementations of (Generalized) DES; Interner Bericht 18/90, Fakultät für Informatik, Universität Karlsruhe 1990.

Pfit_89 Andreas Pfitzmann: Diensteintegrierende Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz; Universität Karlsruhe, Fakultät für Informatik, Dissertation, Feb. 1989, IFB 234, Springer-Verlag, Heidelberg 1990.

PWP_90 Birgit Pfitzmann, Michael Waidner, Andreas Pfitzmann: Rechtssicherheit trotz Anonymität in offenen digitalen Systemen; Datenschutz und Datensicherung DuD 14/5-6 (1990) 243-253, 305-315.

Ries_87 Hans Riesel: Prime Numbers and Computer Methods for Factorization; Progress im Mathematics, Birkhäuser Boston, Basel, Stuttgart 1985, 2nd revised and corrected printing 1987.

RSA_78 R. L. Rivest, A. Shamir, L. Adleman: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems; Communications of the ACM 21/2 (1978) 120-126.

Schm_91 Andreas Schmidt: Softwareimplementierung unbeobachtbarer und sicherer Zahlungssysteme in einer Versuchsumgebung; Diplomarbeit am Institut für Rechnerentwurf und Fehlertoleranz der Universität Karlsruhe September 1991.

SeLi_89 Christoph Seidel, Antonius Lipsmeier: Computerunterstütztes Lernen: Entwicklungen – Möglichkeiten – Perspektiven; Verlag für Angewandte Psychologie, Stuttgart 1989.

Wage_58 Martin Wagenschein: Das exemplarische Lehren als ein Weg zur Erneuerung der höheren Schule, 1958; aus [Gern_72].

Wirt_83 N. Wirth: Programming in MODULA-2 (2nd. ed.); Springer-Verlag, Berlin 1983.