Unverkäufliche Leseprobe

Albrecht Beutelspacher
Geheimsprachen
Geschichte und Techniken

128 Seiten, Paperback
ISBN: 978-3-406-49046-0

I. Kryptographie: Geheimwissenschaft oder Wissenschaft von Geheimnissen?

Schon als kleines Kind machte ich erste Erfahrungen mit einer Geheimsprache. Wenn meine Eltern sich am Tisch über Dinge unterhielten, die uns Kinder „nichts angingen“, so taten sie das auf Französisch. Wir rätselten und stellten phantastische Vermutungen an – die aber meiner Erinnerung nach nie der Wahrheit entsprachen.

Später entwickelten wir Kinder dann eigene Geheimsprachen und versuchten damit, unsere Kommunikation vor den Eltern zu schützen – vermutlich mit wenig Erfolg.

In der Tat assoziiert man zu den Begriffen „Kryptographie“ oder „Verschlüsselung“ Geheimschriften, Geheimsprachen, Geheimcodes, Geheimtinte – Dinge, die gemeinhin nur für Heranwachsende in einer bestimmten Entwicklungsphase interessant und wichtig sind.

Das Gegenteil ist richtig: Wir sind im täglichen Leben umgeben von kryptographischen Diensten und Mechanismen: Telefonkarten, Geldautomaten, Handys, e-commerce, die Wegfahrsperre am Auto – ohne Kryptographie würde das alles nicht funktionieren! Die Kryptographie, eine beeindruckende Erfolgsstory.

Dabei war die Kryptographie jahrhundertelang, ja jahrtausendelang eine Wissenschaft, die sich ruhig entwickelte. Man wußte, was man zu tun hatte. Es gab klare Vorgaben, nämlich die diplomatischen und militärischen Nachrichten des eigenen Landes zu verschlüsseln und die entsprechenden Nachrichten der anderen zu „knacken“. Natürlich ereignete sich dabei auch Aufregendes; dies hing aber in der Regel mit den politischen oder militärischen Ereignissen zusammen, die die Kryptologen durch ihre Arbeit beeinflußt haben. Es waren aber immer die gleichen Aufgaben, und die tägliche Arbeit bestand aus der typischen Mischung aus Streß und Langeweile – eine Arbeit für geduldige Tüftler, eine Arbeit, die unter Ausschluß der Öffentlichkeit vollzogen wurde.

Das hat sich grundlegend geändert. Die Kryptographie hat in den letzten Jahrzehnten sowohl praktisch als auch theoretisch eine enorme Bedeutung erlangt, sie ist eine öffentliche Wissenschaft mit unglaublicher Dynamik – und politischen Konsequenzen geworden. Es gibt inzwischen so viele Tagungen über Kryptographie, daß kein einzelner Mensch sie mehr alle besuchen kann, es gibt viele Bücher (gute und schlechte), es gibt jede Menge wissenschaftliche Veröffentlichungen, ja es gibt Zeitschriften, die sich nur mit Kryptographie befassen. Dies hat mindestens die drei folgenden Gründe:

Die Rolle des Computers und des Internets. Dadurch, daß Nachrichten, also Texte, Daten, Bilder usw., elektronisch erzeugt, gespeichert, übermittelt, bearbeitet und verwaltet werden können, haben wir nicht nur unglaubliche Vorteile erzielt, sondern uns auch erhebliche Nachteile eingehandelt – jedenfalls, wenn keine geeigneten Maßnahmen ergriffen werden. Einige Beispiele machen dies klar: Daten können kopiert, verändert, gelöscht werden, ohne daß dies Spuren hinterläßt. Daraus ergeben sich unüberschaubare wirtschaftliche Folgen (zum Beispiel unberechtigtes Kopieren von geheimen Unterlagen oder gar von elektronischem Geld), Beeinträchtigungen und Bedrohungen für die Gesellschaft (beispielsweise die Manipulation der Steuerungssoftware in Kernkraftwerken und Flughäfen) sowie Auswirkungen auf das Individuum („gläserner Mensch"). Die Kryptographie stellt Mittel bereit, um diesen Gefahren zu begegnen. Wenn Kryptographie von vornherein und richtig eingesetzt wird, dann muß man anschließend keine aufwendige Technologiefolgenabschätzung veranstalten; denn es treten in gewissem Sinne keine schädlichen Nebenwirkungen auf.

Bedeutung der Authentifikation (Nachweis der Echtheit). Die klassische Kryptographie beschäftigte sich ausschließlich mit Verschlüsselung, also der Verheimlichung von Nachrichten. Die moderne Kryptographie hat ein ganz neues Themenfeld erobert, die Authentifikation. Dabei geht es nicht um Ver-

heimlichung einer Nachricht, sondern darum, die Unversehrtheit, die Echtheit einer Nachricht zu garantieren. Dies spielt überall dort die entscheidende Rolle, wo Werte transferiert werden: Wenn man an einer Tankstelle oder in einem Geschäft mit „ec-Karte und Geheimzahl" bezahlt, muß man sicher sein, daß der bestätigte Betrag nicht durch Manipulationen am Terminal oder im Netz verändert werden kann. Ein wesentlicher Teil der Entwicklungen der modernen Kryptographie zielt auf Authentifikation, insbesondere auf „digitale Signaturen".

Die Rolle der Mathematik. Die Entwicklung der modernen Kryptographie war nur möglich, weil sich die Kryptographie von einer „Kunst" zu einer Wissenschaft, genauer gesagt: zu einer mathematischen Wissenschaft gemausert hat. Durch den Rückgriff auf mathematische Methoden und Strukturen haben kryptographische Systeme einen viel höheren Grad an Vertrauenswürdigkeit erlangt. Das liegt auch an dem speziellen Charakter mathematischer Aussagen. Die Mathematik unterscheidet sich – in mehr oder weniger starkem Grad – von anderen Wissenschaften dadurch, daß in ihr eine Aussage nicht deshalb akzeptiert wird, weil sie empirisch verifiziert wurde, oder weil die Experten diese für wahr halten, oder weil nichts gegen sie spricht, oder ... Nein, die Mathematik hat einen rigorosen Wahrheitsbegriff: In ihr wird eine Aussage nur dann akzeptiert, wenn sie mit den strengen Regeln der Logik bewiesen wurde.

Das klingt zunächst abstrakt. Was das jedoch für die Kryptographie bedeutet und welche weitreichenden Folgen dies hat, wird klar, wenn wir Beispiele betrachten. Wenn ein Staat für den diplomatischen Verkehr ein Verschlüsselungssystem einsetzt, dessen Sicherheit mathematisch beweisbar ist, dann muß er sich nicht den Kopf darüber zerbrechen, was wäre, wenn dieses System doch geknackt würde. Umgekehrt, wenn „der Gegner" weiß, daß man ein solches System einsetzt, dann weiß er auch, daß mit kryptologischen Methoden hier nichts auszurichten ist. Wir werden später sehen, daß es sol-

che Systeme gibt – und warum sie, trotz ihrer anscheinend überwältigenden Vorteile, so wenig eingesetzt werden.

Ein anderes Beispiel ist vielleicht noch deutlicher. Seit Jahrhunderten gibt es einen ständigen Kampf zwischen den Notenbanken, die „fälschungssichere" Geldscheine und Münzen herstellen und denjenigen, die trotz der angeblichen Fälschungssicherheit Geldscheine nachmachen und fälschen. *Wenn* es Geld gäbe, dessen Sicherheit auf kryptographischen Mechanismen beruht, und zwar auf solchen, deren Sicherheit mathematisch beweisbar ist, *dann* bestünde keine Gefahr der Geldfälschung mehr. Im vorletzten Kapitel werden wir ausführlich die Möglichkeit von elektronischem Geld diskutieren, dessen Sicherheit kryptologisch gewährleistet werden kann.

Die moderne Kryptographie ist keine Geheimwissenschaft, nichts, was nur im verborgenen blüht, kein Tabu, das seine Kraft verliert, wenn es dem Licht der Öffentlichkeit ausgesetzt wird. Nein, die moderne Kryptographie ist eine Wissenschaft, die ihre Ergebnisse austauscht und öffentlich diskutiert.

Wenn wir das Wesen dieser Wissenschaft genauer bestimmen wollen, stoßen wir fast zwangsläufig auf den Begriff „Vertrauen". Nicht in dem Sinne einer Forderung, daß man zu dieser Wissenschaft oder zu ihren Ergebnissen Vertrauen haben müsse, sondern dergestalt, daß „Vertrauen" das Thema der Kryptographie ist. Wir beschreiben das nur scheinbar anders, wenn wir sagen: Kryptographie ist die Wissenschaft von den Geheimnissen.

Was soll das heißen? Stellen wir uns zwei Personen vor, die ein gemeinsames Geheimnis haben. Das kann ein gemeinsames Erlebnis, eine Erinnerung oder auch nur ein Wort sein. Die Tatsache des Geheimnisses impliziert, daß keiner der beiden dies an einen Dritten weitergibt. Dies wäre ein Vertrauensbruch. Die beiden Menschen vertrauen sich. Kurz: Ein gemeinsames Geheimnis setzt gegenseitiges Vertrauen voraus.

In der Kryptographie setzen wir den Akzent nur ein klein wenig anders: Gemeinsames Vertrauen wird durch ein gemeinsames Geheimnis repräsentiert. Kryptographie ist eine

Wissenschaft, in der Vertrauen geschaffen und übertragen wird.

Die moderne Kryptographie lebt von der Entdeckung und der Diskussion scheinbar paradoxer Fragen.

Was kann man aus einem gemeinsamen Geheimnis machen? Angenommen, zwei Personen haben bereits ein gemeinsames Geheimnis, vielleicht ein geheimes Wort oder eine geheime Zahl, können sie daraus ein größeres Geheimnis machen („aus wenig mach viel“)? Oder gilt ein „Erhaltungssatz für Geheimnisse“?

Wie können sich zwei Personen ein gemeinsames Geheimnis verschaffen? Sie können das, wenn sie eine vertrauliche Umgebung haben: Wenn sie alleine sind, können sie sich das Geheimnis zuflüstern, wenn sie dem Briefgeheimnis vertrauen, kann der eine dem anderen ein von ihm gewähltes Geheimnis zuschicken. Aber in diesen Fällen wird bereits ein Mechanismus zur Geheimhaltung vorausgesetzt. Wir fragen daher radikaler: Können sich zwei Personen auch ohne vertrauliche Umgebung ein gemeinsames Geheimnis verschaffen? Genauer gefragt: Können zwei Personen, die bislang noch nie einen Kontakt hatten, durch eine öffentliche Unterhaltung ein gemeinsames Geheimnis erhalten, ohne daß die mithörende Umgebung eine Chance hat, auf dieses Geheimnis zu kommen („aus nichts mach etwas“)? Im Kapitel über Public-Key-Kryptographie werden wir diese Frage beantworten – positiv!

Kann man Vertrauen auch ohne gemeinsames Geheimnis übertragen? Nicht ohne Geheimnis, aber ohne *gemeinsames* Geheimnis?

Ein besonders wichtiger Aspekt ist der Nachweis der Identität einer Person. Ich beweise meine Identität dadurch, daß ich nachweise, ein bestimmtes Geheimnis zu haben. Es gibt einfache Methoden für einen solchen Nachweis: Ich kann zum Beispiel mein Geheimnis einfach übertragen – aber eine solche Methode hat viele Nachteile. Auch hier fragen wir radikal: Kann ich jemanden überzeugen, ein bestimmtes Geheimnis zu kennen, ohne ihm das Geringste zu verraten? Im Kapitel über

Zero-Knowledge-Verfahren werden wir das Geheimnis lüften und auch diese Frage positiv beantworten!

Eine Bemerkung zur Terminologie: Wir verwenden in diesem Buch die Begriffe „Kryptographie“ und „Kryptologie“ synonym. Manche Autoren machen zwischen diesen Begriffen feine Unterschiede; die Unterschiede sind aber keinesfalls so groß wie zwischen Geographie und Geologie, Philosophie und Philologie oder gar Astronomie und Astrologie. Mißverständnisse sind ausgeschlossen.

In den beiden folgenden Kapiteln behandeln wir die klassische Kryptographie. Wir beginnen mit wirklichen Geheimschriften und historisch wichtigen Geheimcodes, wie etwa dem Cäsar-Code. Anschließend werden wir diskutieren, ob diese Codes sicher sind. Dazu müssen wir klären, was Sicherheit überhaupt bedeutet.

Im dritten Kapitel stellen wir die Frage, wie gut Geheimcodes sein können. Zunächst geht es ziemlich grundsätzlich um „unknackbare Codes“. Dann werden wir praktisch eingesetzte Verfahren erörtern, insbesondere den DES-Algorithmus und das PIN-Verfahren, das vom Geldausgabeautomaten und vom elektronischen Einkaufen bekannt ist.

Das vierte Kapitel konzentriert sich auf die Public-Key-Kryptographie, die 1976 erfunden wurde. Mit Hilfe der dort entwickelten Verfahren gelingt es, vertraulich zu kommunizieren, ohne vorher ein Geheimnis ausgetauscht zu haben. Diese „erste“ Revolution der Kryptographie hat eine Bedeutung, die weit über die engere Wissenschaft hinausgeht.

Daran anschließend werden die Mitte der 80er Jahre entdeckten „Zero-Knowledge-Algorithmen“ dargestellt. Diese zeigen, wie jemand eine andere Person davon überzeugen kann, ein bestimmtes Geheimnis zu kennen, ohne ihm dabei das Geringste zu verraten.

Die Möglichkeit von elektronischem Geld war in den letzten Jahren sowohl für Wissenschaftler als auch für Praktiker eine Herausforderung, da e-commerce im eigentlichen Sinne nur auf Basis elektronischer Zahlungssysteme möglich ist. Im

vorletzten Kapitel zeigen wir, daß solches Geld möglich ist, man zur Realisierung aber viele komplexe kryptographische Mechanismen der höchsten Qualität einsetzen muß.

Im letzten Kapitel stellen wir uns schließlich kritischen Fragen, die in Gesellschaft und Politik kontrovers diskutiert werden: Darf Kryptographie unbeschränkt eingesetzt werden, oder muß ihr Gebrauch kontrolliert werden? Kriminelle und Terroristen können durch Kryptographie ihre Machenschaften erfolgreich vor dem Auge des Gesetzes verbergen. Soll man das dulden oder verbieten? Kann ein Verbot durchgesetzt werden? Kann man den Mißbrauch von Kryptographie verhindern?

Noch ein Wort zu Inhalt und Stil. Moderne Kryptographie ist eng mit der Mathematik verbunden. Insbesondere beruhen die meisten modernen Algorithmen auf mathematischen Strukturen. Dies ist unvermeidlich. Daher ist auch in diesem Buch Mathematik unvermeidlich.

Ich werde aber immer, wenn es schwierig zu werden droht, zwei Dinge machen. Zum einen werde ich alle auf Mathematik beruhenden Verfahren zunächst mit Szenen aus dem täglichen Leben so erklären, daß zum Verständnis keinerlei Mathematik notwendig ist. Zum anderen werde ich alle benötigten mathematischen Tatsachen an den entsprechenden Stellen darstellen; dies sind die Abschnitte „Natürliche Zahlen zum ersten, zum zweiten, zum dritten".

Sie können also das Buch auf drei Ebenen lesen: zum einen auf einer vollkommen unmathematischen Ebene (diese Teile machen den mit Abstand größten Teil des Buches aus), zum zweiten stelle ich Ihnen detailliertere Beschreibungen mit mathematischen Begriffen vor. Schließlich haben Sie auch die Möglichkeit, die mathematischen Hintergründe zu verstehen.