Kryptografie für Dummies

Symmetrische und asymmetrische Verschlüsselung verstehen

» Hier geht's direkt zum Buch

DAS VORWORT

Einleitung

Über dieses Buch

Kryptografie ist die Lehre vom Verschlüsseln geheimer Botschaften – ursprünglich. Allein das ist hochspannend, aber heute ist Kryptografie weiter gefasst: In Zeiten von Internet und mobiler Kommunikation werden kryptografische Verfahren benutzt, um die gesamte Kommunikation sicher zu machen – sicher gegen Abhören, gegen Verfälschen, gegen Täuschen.

Dieses Buch bietet Ihnen eine Auswahl an grundlegenden Ideen und Verfahren der Kryptografie, verbunden mit dem mathematischen Hintergrund. Keine Angst – die benötigte Mathematik ist einfacher als gedacht. Und es ist allemal besser, wenn Sie selbst ein Gefühl für die Sicherheit der Verfahren erlangen, als sich auf Hörensagen zu verlassen.

Und vielleicht wollen Sie auch einige der verwendeten Algorithmen probehalber einmal in der Programmiersprache Python programmieren? Python ist eine einfach zu verstehende Programmiersprache, und sie ermöglicht das Rechnen mit sehr großen Zahlen, wie sie in der Kryptografie verwendet werden.

Was Sie in diesem Buch nicht finden werden, ist Anekdotisches aus dem Reich der Geheimsprachen. Auch keine Geschichten über das Knacken von Codes, über die Machenschaften von Spionen oder über die Angriffe von Hackern. Leider! Aber darüber gibt es spannende andere Bücher.

»Wie verschlüssele ich meine E-Mails?« Dieses Buch enthält keine Anleitung darüber, wie Sie für Ihr E-Mail-Programm die entsprechende Verschlüsselungssoftware installieren. Aber es liefert Ihnen das Hintergrundwissen – warum Sie einen öffentlichen und einen privaten Schlüssel brauchen, was Signieren bedeutet und wie es funktioniert.

Im Internet finden Sie sehr gut geschriebene Anleitungen für die E-Mail-Verschlüsselung – zugeschnitten auf Ihr E-Mail-Programm, stets in der aktuellen Version, mit Abbildungen der erscheinenden Bildschirmformulare, mit Tipps, was Sie anklicken müssen.

Sie werden in diesem Buch auch keine detaillierte Implementierung von Sicherheitsstandards finden, wie etwa TLS oder WPA-2. Dies wäre zu technisch – wenn Sie sich aber damit beschäftigen, werden Sie dort die grundlegenden Verfahren wiederfinden, die Sie in diesem Buch kennengelernt haben.

Darauf soll es Ihnen ankommen – sich für die Ideen der modernen Kryptografie zu begeistern, die zuweilen erscheinen wie schwarze Magie:

- ✔ mit einem *öffentlich zugänglichen* Schlüssel einen Text verschlüsseln, aber keiner kann den Text wieder entschlüsseln, nur der berechtigte Empfänger,

- ✔ einen geheimen Schlüssel über eine *öffentliche Leitung* vereinbaren,
- ✔ jemanden davon überzeugen, ein Geheimnis zu kennen, *ohne das Geheimnis preiszugeben.*

Konventionen in diesem Buch

Sie werden in diesem Buch viele neue Begriffe lernen, die wissenschaftlich genau definiert sind. Aber zu jeder neuen Definition finden Sie entsprechende Beispiele, sodass es Ihnen leichtfällt, die neuen Begriffe zu »verinnerlichen«.

Und so manche Berechnung verstehen Sie um vieles leichter, wenn Sie einmal selbst mit einem Zahlenbeispiel nachrechnen. Hierbei helfen Ihnen die an vielen Stellen zu findenden »Beispiele mit kleinen Zahlen«.

Kryptografie ist international – alle Normen und Spezifikationen sind in englischer Sprache abgefasst. Daher finden Sie zu den verwendeten deutschen Begriffen auch immer die entsprechende englische Bezeichnung.

Jedes Kapitel schließt mit einem kleinen Abschnitt »zum Üben« ab. Machen Sie davon Gebrauch! Mit ein bisschen Übung gelingt alles viel besser. Und Sie können überprüfen, ob Sie alles verstanden haben, und dann guten Gewissens zum nächsten Kapitel übergehen.

Was Sie nicht lesen müssen

Im Teil II erhalten Sie einen Crash-Kurs in Mathematik – soweit diese für das Verstehen der kryptografischen Verfahren erforderlich ist. Wenn Sie Mathematik studiert haben, lassen Sie diesen Teil getrost aus oder überfliegen ihn nur kurz. Aber vielleicht wollen Sie ja auch Ihre mathematischen Kenntnisse noch einmal kurz auffrischen …

Manchmal ist spezielle Mathematik, etwa über elliptische Kurven, auch direkt in dem Kapitel angegeben, wo sie gebraucht wird.

In Teil IV finden Sie kleine Programmstücke in der Programmiersprache Python, in denen die (relativ wenigen) grundlegenden Algorithmen der Kryptografie programmiert sind, wie zum Beispiel der Primzahltest. Die Darstellung dieser Algorithmen als Programm erleichtert Ihnen das genaue Nachvollziehen und ermöglicht Ihnen sogar das Ausprobieren. Python ist eine sehr leicht zu verstehende Programmiersprache – aber wenn Sie mit Programmieren gar nichts am Hut haben, dann lassen Sie diesen Teil weg.

Törichte Annahmen über den Leser

Sie wollen die Ideen der modernen Kryptografie verstehen. Aber Sie sind kein Mathe-Genie – dennoch aber sind Sie offen dafür, hinzuzulernen, wenn man es Ihnen vernünftig

erklärt. Sie haben keine grundsätzliche Abneigung gegen Zahlen. Und auch die eine oder andere Formel sind Sie bereit zu schlucken, denn Sie lesen ein Fachbuch.

Vielleicht haben Sie auch schon ein wenig Programmiererfahrung, dann sind die kleinen Programmstücke für Sie keine schwere Kost. Wenn Sie aber noch nie programmiert haben, dann sind es vielleicht Appetithäppchen, um damit anzufangen.

Auf jeden Fall erhalten Sie einen ersten Einblick in die Probleme und Lösungen der Kryptografie, wenn Sie

- ✔ im Studium an Lehrveranstaltungen aus diesem Bereich teilnehmen,
- ✔ im Beruf mit IT-Sicherheit zu tun haben
- ✔ oder sich ansonsten mit Hintergrundwissen versorgen möchten.

Wie dieses Buch aufgebaut ist

Wie jedes »…für Dummies«-Buch ist auch dieses in mehrere Teile aufgeteilt. Bei diesem Buch sind es sogar derer neun.

Teil I: Verschlüsseln

Am Anfang staunen Sie darüber, dass nahezu das geballte Wissen dieses ganzen Buches dahintersteckt, wenn Sie im Internet eine gesicherte Webseite aufrufen, etwa um eine Banküberweisung zu machen. Es wird sichergestellt, dass Sie die echte Bank-Webseite aufrufen und dass Dritte die übermittelten Daten nicht einsehen und nicht unbemerkt verändern können. Dazu werden die Daten verschlüsselt.

Zur Einstimmung geht es dann zunächst um die klassische Verschlüsselung: Die Buchstaben eines Textes werden in bestimmter Weise durch andere Buchstaben ersetzt – aus HALLO wird XPBGQ. Nebenbei erlernen Sie dabei die Modulo-Rechnung (die Sie eigentlich schon können, aber sich vielleicht nicht darüber bewusst sind).

Anschließend lernen Sie ein zentrales Konzept der modernen Kryptografie kennen: die Public-Key-Verschlüsselung, also das Verschlüsseln mit einem Schlüssel, der veröffentlicht ist. Wie kann das gehen? Mit mathematischen Verfahren, die sehr einfach sind, aber wirksam, weil sie mit sehr großen Zahlen arbeiten.

Teil II: Kryptische Mathematik

Hier wundern Sie sich vielleicht darüber, dass die Mathematik der Kryptografie gar nicht so schwer ist. Überfliegen Sie diesen Teil und vergewissern Sie sich, dass Sie Modulo-Rechnung und ein wenig Gruppentheorie beherrschen. Und wenn nicht, dann lesen Sie diesen Teil ein bisschen eingehender.

Teil III: Kryptografische Verfahren

In diesem Teil lernen Sie die wichtigsten kryptografischen Verfahren kennen. Sie vereinbaren mit einem Kommunikationspartner einen geheimen Schlüssel über eine öffentliche Leitung. Dies ist mit ein wenig Mathematik, die Sie dann schon kennen, möglich! Darauf aufbauend erhalten Sie mit zwei weiteren kleinen Berechnungen ein Public-Key-Verschlüsselungsverfahren.

Im Anschluss machen Sie das Gleiche noch einmal, und zwar auf Basis elliptischer Kurven (klingt kompliziert, ist aber einfacher als gedacht). Was Sie an zugehöriger Mathematik benötigen, bekommen Sie mitgeliefert.

Und Sie lernen ein modernes symmetrisches Verschlüsselungsverfahren kennen, das AES-Verfahren, auch wieder mit der hier benötigten Mathematik.

Teil IV: Berechnungsverfahren

Im vierten Teil geht es um die drei wichtigsten Berechnungen in kryptografischen Verfahren: die schnelle modulare Exponentiation, den Primzahltest und den erweiterten euklidischen Algorithmus. Wenn Sie dann auf den Geschmack gekommen sind, nehmen Sie sich noch den Chinesischen-Restsatz-Algorithmus vor.

Sie programmieren diese Algorithmen in Form von kleinen Programmstücken in der Programmiersprache Python. Aber auch wenn Sie nicht programmieren mögen, lernen Sie die entsprechenden Algorithmen hier kennen.

Teil V: Authentifizieren

Nun kommen Sie zu einem früher häufig vernachlässigten Thema: der sicheren Authentifikation. Wie können Sie sicher sein, dass ein Kommunikationspartner wirklich derjenige ist, für den er sich ausgibt?

Auch Sie selbst müssen sich oft durch Eingabe eines geheim gehaltenen Passwortes gegenüber Computern, Webportalen oder Geldautomaten authentifizieren. Aber Sie müssen Ihr Geheimnis jedes Mal preisgeben, wenn Sie das Passwort eingeben. Erstaunlich, dass es Authentifizierungsverfahren gibt, bei denen Sie beweisen, ein Geheimnis zu kennen, ohne es zu verraten!

Teil VI: Sicherheit

Jetzt geht es zur Sache: Sie greifen das RSA-Verschlüsselungsverfahren an! Dabei entwickeln Sie ein grundsätzliches Gefühl dafür, wie schwer oder leicht es ist, einen Code zu knacken. Wichtig ist auch zu wissen, dass ein Verfahren möglicherweise zwar im Prinzip sicher ist, aber im Einzelfall auch unsicher, wenn ungünstige Parameter gewählt werden.

Teil VII: Zufall

Der siebte Teil beschäftigt sich mit dem Zufall und der Notwendigkeit, ihn in der Kryptografie richtig zu nutzen. Viele Verfahren nutzen Zufallsbits, um nicht vorhersehbar und nicht nachvollziehbar zu sein. Aber hierfür ist es wichtig, dass auch die erzeugten Zufallsbits ebenfalls wirklich nicht vorhersehbar und nicht nachvollziehbar sind.

Teil VIII: Anwendungen

Hier gibt es ein freudiges Wiedererkennen der kryptografischen Verfahren, wenn Sie die Sicherheits-Protokolle des Internet untersuchen. Erfahren Sie, wie https funktioniert und was ein Zertifikat ist.

Teil IX: Top-Ten-Teil

Im letzten Teil erfahren Sie endlich, welche von allen den Dingen, die Sie gelernt haben, die wichtigsten sind.

Anhänge

Hier finden Sie die Lösungen zu den kleinen Übungsaufgaben, sodass Sie nachschauen können, ob Sie das Gleiche herausbekommen haben. Und Sie finden ein paar Buchvorschläge zum Weiterlesen, wenn Sie für die Kryptografie Feuer gefangen haben …

Symbole, die in diesem Buch verwendet werden

Neben diesem Symbol finden Sie eine wichtige **Tatsache**, wie etwa eine Definition oder einen Lehrsatz.

So wichtig eine genaue Definition auch ist – verstehen lässt sie sich viel leichter anhand eines **Beispiels**.

Vorsicht: Bevor Sie in eine Falle tappen, lesen Sie lieber diesen kleinen Abschnitt.

Solange Sie selber noch keine umfassenden Erfahrungen haben, empfinden Sie den einen oder anderen **Tipp** bestimmt als hilfreich.

Neben diesem Symbol finden Sie in Kästen interessante Zusatzinformationen und Beispiele, die nicht zwingend notwendig sind, um dem Text zu folgen.

Hier finden Sie Übungsaufgaben, die Ihnen helfen, Ihr Wissen zu testen und zu festigen. Die Lösungen zu den Aufgaben finden Sie im Anhang B.

Wie es weitergeht

Lesen Sie einfach los! Aber lesen Sie nicht mehr weiter, wenn Sie merken, dass Sie nicht mehr folgen können (falls dies mal vorkommt). Dann gehen Sie noch einmal ein Stück zurück.

Es lohnt sich auf jeden Fall, die eingestreuten Aufgaben zu lösen und sich dadurch kleine Erfolgserlebnisse zu gönnen.

Tippen Sie auch die Programmstücke ab und lassen Sie diese mit Ihren eigenen Zahlenbeispielen laufen! Abtippen ist zum Lernen besser als Copy and Paste – es ist wie zu Fuß zu gehen, man bekommt mehr mit als beim Autofahren.

Alice und Bob

In Büchern über Kryptografie tummeln sich immer wieder dieselben Leute: »Alice« und »Bob«, »Oscar« und »Eve«. Alice und Bob schicken sich geheime Botschaften, und Oscar oder Eve belauschen sie dabei.

Man verspricht sich größere Anschaulichkeit, wenn nicht *A* eine Nachricht an *B* schickt, sondern Alice an Bob. Wie aber sollen wir uns diese Personen vorstellen? Trägt Alice eine Brille? Ist Bob ein älterer Herr? Sind alle weiße Amerikaner?

Ich habe mich dazu entschlossen, in diesem Buch bewusst auf diese Personifizierung zu verzichten. Ich bleibe bei *A* und *B* und, wenn noch ein Dritter hinzukommt, bei *C*. Ein Dritter oder eine Dritte? Nun, wir wollen eben gerade nicht personifizieren. Auch wenn von »Sender« und »Empfänger« die Rede ist, sind die *Rollen* des Senders bzw. des Empfängers gemeint und keine männlichen Personen. Sender und Empfänger können auch technische Geräte sein, die miteinander kommunizieren. Und tatsächlich sind sie es normalerweise auch, nämlich Computer.

Moderne kryptografische Verfahren basieren auf mathematischen Berechnungen mit sehr großen Zahlen, und diese Berechnungen überlassen wir gerne Computern. Weder Alice noch Bob können 1000-stellige Zahlen potenzieren oder sich 500-stellige Primzahlen ausdenken ...

Also liebe Leserin und lieber Leser, und jetzt spreche ich Sie persönlich als Menschen an und nicht in Ihrer Rolle als Lesende, ich lade Sie ein, in den folgenden Kapiteln in die magische Welt der Kryptografie einzutauchen.

Ich wünsche Ihnen viel Freude beim Lesen und Lernen!

Bitte und danke sagen

Bitte senden Sie Kommentare, Lob und Kritik sowie Hinweise auf Fehler an mail@hwlang.de.

Danke sage ich allen, die mir beim Schreiben dieses Buches wertvolle Anregungen und Tipps gegeben haben, besonders Lennart Willrodt für die sehr eingehende Durchsicht einer ersten Version des Manuskripts, Arnold Willemer für viele hilfreiche Anmerkungen und Alexandra Dirksen für anregende Diskussionen. Ich danke auch dem Kollegen Reinhard Völler, der als Fachkorrektor mir zum Schluss noch wichtige Hinweise gegeben hat.

Zur zweiten Auflage

In den vier Jahren seit Erscheinen der ersten Auflage haben sich einige Sicherheitsanforderungen verschärft, bedingt durch Fortschritte in der Kryptoanalyse in Verbindung mit der inzwischen verfügbaren höheren Rechenleistung.

So werden etwa 160 Bit als Länge eines Hashwertes nicht mehr als ausreichend angesehen. Oder in Public-Key-Verfahren wird statt einer Blocklänge von 1024 Bit nunmehr eine Blocklänge von 2048 Bit empfohlen.

Die grundsätzliche Eignung der verwendeten Verfahren steht jedoch nicht in Frage. Gleichwohl haben einige neue Verfahren an Bedeutung gewonnen, so etwa der Hashalgorithmus SHA-256 (*Secure Hash Algorithm* mit 256 Bit), das Authentifizierungsverfahren GCM (*Galois Counter Mode*) oder das Signaturverfahren DSA (*Digital Signature Algorithm*).

Auf diese neueren Entwicklungen wird in der zweite Auflage dieses Buches eingegangen – passend auch zu mittlerweile häufig verwendeten neuen Sicherheitsverfahren im Web-Protokoll https (siehe Kapitel 1).

Alle Programmbeispiele sind einheitlich an die aktuelle Python-Version 3 angepasst. Auf die vor einiger Zeit noch gebräuchliche Version 2.7 wird nicht mehr eingegangen.

Last not least: Einige Fehler und Ungereimtheiten sind beseitigt, einige Dinge werden klarer und ausführlicher erklärt, und es gibt eine ganze Reihe zusätzlicher Aufgaben zum Üben.