David Wong

Kryptografie in der Praxis

Eine Einführung in die bewährten Tools, Frameworks und Protokolle

dpunkt.verlag

David Wong

Kryptografie in der Praxis

Eine Einführung in die bewährten Tools, Frameworks und Protokolle

dpunkt.verlag

David Wong

Übersetzung: Frank Langenau
Lektorat: Sandra Bollenbacher
Copy-Editing: Petra Heubach-Erdmann, Düsseldorf
Satz: inpunkt[w]o, *www.inpunktwo.de*
Herstellung: Stefanie Weidner
Umschlaggestaltung: Helmut Kraus, *www.exclam.de*
Druckerei: mediaprint solutions GmbH, 33100 Paderborn

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über *http://dnb.d-nb.de* abrufbar.

ISBN:
Print 978-3-86490-939-9
PDF 978-3-98890-006-7
ePub 978-3-98890-007-4
mobi 978-3-98890-008-1

1. Auflage 2023

Wieblinger Weg 17
69123 Heidelberg

Hinweis:
Dieses Buch wurde mit mineralölfreien Farben auf PEFC-zertifiziertem Papier aus nachhaltiger Waldwirtschaft gedruckt. Der Umwelt zuliebe verzichten wir zusätzlich auf die Einschweißfolie. Hergestellt in Deutschland.

Schreiben Sie uns:
Falls Sie Anregungen, Wünsche und Kommentare haben, lassen Sie es uns wissen: *hallo@dpunkt.de*.

5 4 3 2 1 0

Meinen Eltern, Anne Cerclet und Henry Wong, die meine Neugierde geweckt haben. Meiner Frau, Felicia Lupu, die mich auf dieser Reise unterstützt hat.

Inhalt

Vorwort

Wenn Sie dieses Buch in die Hand nehmen, fragen Sie sich vielleicht: »Warum noch ein Buch über Kryptografie?« oder sogar: »Warum sollte ich dieses Buch lesen?« Um diese Frage zu beantworten, müssen Sie verstehen, wie alles begann.

Ein Buch – seit Jahren im Entstehen

Wenn Sie heutzutage etwas über irgendeine Sache erfahren wollen, suchen Sie danach mit Google oder Bing oder Baidu – das Prinzip dürfte klar sein. Was Kryptografie angeht und je nachdem, wonach Sie suchen, fallen die Quellen möglicherweise recht spärlich aus. Auf dieses Phänomen bin ich schon vor langer Zeit gestoßen und es hat mich seither immer wieder frustriert.

An der Uni musste ich für einen Kurs einen Angriff per Differential Power Analysis (DPA) implementieren. Dieser Angriff war zu dieser Zeit ein Durchbruch in der Kryptoanalyse, denn es war der erste Seitenkanalangriff, der veröffentlicht wurde. Ein Angriff per Differential Power Analysis ist etwas Magisches: Indem man den Stromverbrauch eines Geräts misst, während es etwas ver- oder entschlüsselt, ist man in der Lage, seine Geheimnisse herauszufinden. Mir war klar, dass herausragende Papers großartige Ideen vermitteln können, wobei man nur wenig Aufwand in Klarheit und Verständlichkeit investieren muss. Ich erinnere mich, wie ich mir das Hirn zermarterte, um zu ergründen, was der Autor zu sagen versuchte. Schlimmer noch, ich konnte keine guten Online-Quellen finden, die das Paper erklärten. Also habe ich mir weiter den Kopf zerbrochen, und schließlich habe ich es verstanden. Und dann dachte ich, vielleicht könnte ich anderen helfen, die wie ich diese Tortur durchmachen müssen.

Hoch motiviert zeichnete ich einige Diagramme, animierte sie und nahm mich dabei auf, wie ich sie durchging. Das war mein erstes YouTube-Video über Kryptografie: *https://www.youtube.com/watch?v=gbqNCgVcXsM*.

Jahre später, nachdem ich das Video hochgeladen hatte, bekomme ich immer noch Lob von verschiedenen Leuten im Internet. Gerade gestern, als ich an diesem Vorwort schrieb, postete jemand: »Danke, wirklich eine tolle Erklärung, die mir wahrscheinlich Stunden erspart hat, dieses Paper zu verstehen.«

Was für eine Auszeichnung! Dieser winzige Schritt, mich auf die andere Seite der Bildungslandschaft zu wagen, genügte, um mir Lust auf mehr zu machen. Ich begann, weitere Videos aufzunehmen, und rief dann einen Blog ins Leben, um über Kryptografie zu schreiben. Zu finden ist der Blog hier: *https://cryptologie.net*.

Bevor ich mit diesem Buch begann, hatte ich fast 500 Artikel angehäuft, in denen die vielen Konzepte erklärt wurden, die über diese Einführung hinausgehen. Das war alles nur Übung. In meinem Hinterkopf reifte die Idee, ein Buch zu schreiben, langsam heran, Jahre bevor Manning Publications sich mit einem Buchvorschlag an mich wenden würde.

Der Lehrplan eines Kryptografen in der Praxis

Ich hatte meinen Bachelor in theoretischer Mathematik abgeschlossen und wusste nicht, was als Nächstes auf mich zukam. Außerdem hatte ich mein ganzes Leben lang programmiert und wollte beides unter einen Hut bringen. Natürlich wurde ich neugierig auf die Kryptografie, die das Beste aus beiden Welten zu vereinen schien, und ich begann, die verschiedenen Bücher zu lesen, die mir zur Verfügung standen. Schnell erkannte ich meine Berufung.

Dennoch störte mich etwas: Insbesondere die langen Einführungen, die mit dem geschichtlichen Hintergrund beginnen, denn ich interessierte mich nur für die technischen Einzelheiten und das war schon immer so. Ich schwor mir, wenn ich jemals ein Buch über Kryptografie schreiben würde, dann sollte es sich gänzlich über Vigenère-Chiffren, Cäsar-Chiffren und andere Überbleibsel der Geschichte ausschweigen. Nachdem ich also an der Universität Bordeaux einen Master in Kryptografie erworben hatte, war ich der Auffassung, für die reale Welt bereit zu sein. Doch was wusste ich schon ...

Ich glaubte, mein Abschluss würde ausreichen, doch in meiner Ausbildung fehlte eine Menge Wissen über die eigentlichen Protokolle, die ich angreifen wollte. Ich hatte viel Zeit damit verbracht, etwas über die Mathematik elliptischer Kurven zu lernen, doch nichts darüber, wie diese in kryptografischen Algorithmen verwendet werden. Ich hatte etwas über LFSRs, ElGamal, DES und eine Reihe anderer kryptografischer Primitive gelernt, die ich nie wiedersehen würde.

Mein erster Auftrag zu Beginn meiner Arbeit in der Industrie bei Matasano, der späteren NCC Group, bestand darin, OpenSSL, die beliebteste SSL/TLS-Implementierung zu kontrollieren – d. h. den Code, der im Grunde das gesamte Internet verschlüsselt. Oh Mann, hat mir das Kopfzerbrechen bereitet. Ich weiß noch, wie ich jeden Tag mit starken Kopfschmerzen nach Hause kam. Was für eine katastrophale Bibliothek und ein ebensolches Protokoll! Damals hatte ich keine Ahnung, dass ich Jahre später Mitautor von TLS 1.3, der neuesten Version des Protokolls, werden würde.

Doch zu diesem Zeitpunkt dachte ich bereits: »Das hätte ich in der Uni lernen sollen. Das Wissen, das ich mir jetzt aneigne, wäre nützlich gewesen, um mich auf die Praxis vorzubereiten!« Schließlich war ich jetzt ein spezialisierter Sicherheits-

experte für Kryptografie. Ich überprüfte reale kryptografische Anwendungen. Ich hatte den Job, den man sich nach dem Abschluss eines Kryptografie-Studiums nur wünschen kann. Ich implementierte, verifizierte, verwendete und empfahl, welche kryptografischen Algorithmen infrage kämen. Das ist der Grund, warum ich der erste Leser des Buches bin, das ich schreibe. Das ist es, was ich meinem früheren Ich geschrieben hätte, um es auf die reale Welt vorzubereiten.

Wo sich die meisten Fehler verstecken

Im Rahmen meiner Beratertätigkeit habe ich viele reale kryptografische Anwendungen überprüft, wie zum Beispiel OpenSSL, das verschlüsselte Backup-System von Google, die TLS-1.3-Implementierung von Cloudflare, das Protokoll der Zertifizierungsstelle von Let's Encrypt, das Sapling-Protokoll der Kryptowährung Zcash, das Schwellenwert-Proxy-Wiederverschlüsselungsschema von NuCypher und Dutzende anderer realer kryptografischer Anwendungen, die ich leider nicht öffentlich nennen darf.

Zu Beginn meiner Tätigkeit sollte ich das benutzerdefinierte Protokoll prüfen, das ein bekanntes Unternehmen zur Verschlüsselung seiner Kommunikation geschrieben hatte. Es stellte sich heraus, dass es Signaturen für fast alles verwendete, außer für die ephemeren Schlüssel, was das gesamte Protokoll zum Scheitern brachte, da man diese Schlüssel hätte leicht ersetzen können – ein Anfängerfehler von jemandem mit etwas Erfahrung bei sicheren Transportprotokollen, was aber Leuten fehlt, die dachten, ihre Expertise genügt, um eine eigene Kryptografie zu entwickeln. Ich erinnere mich, wie ich am Ende des Engagements die Schwachstelle erklärte und ein Raum voller Ingenieure für gut 30 Sekunden verstummte.

Diese Geschichte wiederholte sich in meiner beruflichen Laufbahn viele Male. Einmal habe ich bei der Prüfung einer Kryptowährung für einen Kunden einen Weg gefunden, Transaktionen aus bereits bestehenden Transaktionen zu fälschen, weil nicht klar war, was signiert wurde. Als ich mir TLS-Implementierungen für einen anderen Kunden ansah, fand ich einige subtile Möglichkeiten, um eine RSA-Implementierung zu knacken. Das daraus resultierende Whitepaper mit einem der Erfinder von RSA mündete schließlich in einer Reihe von CVEs (Common Vulnerabilities and Exposures), die an ein Dutzend Open-Source-Projekte gemeldet wurden. Als ich mich kürzlich im Rahmen von Recherchen für mein Buch mit dem neueren Matrix-Chat-Protokoll befasst habe, stellte ich fest, dass das Authentifizierungsprotokoll gebrochen war, was zu einem Bruch der Ende-zu-Ende-Verschlüsselung führte. Es gibt so viele Details, die Ihnen entgleiten können, wenn Sie Kryptografie einsetzen. An diesem Punkt war mir klar, dass ich etwas darüber schreiben musste. Deshalb enthält mein Buch viele dieser Anekdoten.

In meinem Job geht es unter anderem darum, Kryptografie-Bibliotheken und -Anwendungen in einer Vielzahl von Programmiersprachen zu überprüfen. Ich habe Fehler entdeckt (zum Beispiel CVE-2016-3959 in der Standardbibliothek von Golang), Möglichkeiten untersucht, wie Bibliotheken dazu verleiten können,

sie zu missbrauchen (zum Beispiel in meinem Paper »How to Backdoor Diffie-Hellman«), und Ratschläge gegeben, welche Bibliotheken verwendet werden sollten. Die Entwickler wussten nie, welche Bibliotheken sie verwenden sollten, und die Antwort fand ich auch immer ziemlich knifflig.

Ich machte mich daran, das Disco-Protokoll zu entwickeln (*https://discocrypto.com*; *https://embeddeddisco.com*), und schrieb dessen umfangreiche Kryptografie-Bibliothek in weniger als 1000 Zeilen Code, noch dazu in mehreren Sprachen. Disco stützte sich auf nur zwei kryptografische Primitive: die Permutation von SHA-3 und Curve25519. Ja, allein mit diesen beiden Dingen, die in 1000 Zeilen Code implementiert wurden, konnte ein Entwickler jede Art von authentifizierendem Schlüsselaustausch, Signaturen, Verschlüsselung, MACs, Hashing, Schlüsselableitung usw. realisieren. Dies gab mir eine einzigartige Sichtweise auf das, was eine gute kryptografische Bibliothek ausmachen sollte.

Da ich in meinem Buch derartige praktische Einsichten darstellen wollte, enthalten natürlich die verschiedenen Kapitel Beispiele, wie man »Krypto« in verschiedenen Programmiersprachen anwendet, wobei renommierte kryptografische Bibliotheken zum Einsatz kommen.

Wozu noch ein neues Buch?

Als ich eine meiner jährlichen Kryptografie-Schulungen bei Black Hat (einer bekannten Sicherheitskonferenz) abhielt, kam ein Student zu mir und fragte, ob ich ein gutes Buch oder einen Online-Kurs über Kryptografie empfehlen könne. Ich erinnere mich, dass ich dem Studenten empfahl, ein Buch von Boneh und Shoup zu lesen und den Kurs Cryptography I von Boneh auf Coursera zu besuchen. (Diese beiden Quellen empfehle ich auch am Ende dieses Buches.)

Der Student sagte mir: »Okay, ich habe es versucht, aber es ist zu theoretisch!« Diese Antwort gab mir zu denken. Zuerst war ich anderer Meinung, aber langsam wurde mir klar, dass er recht hatte. Die meisten Quellen sind ziemlich mathematiklastig und die meisten Entwickler, die sich mit Kryptografie beschäftigen, haben mit Mathematik nicht viel am Hut. Welche Alternativen gab es denn für sie?

Die anderen beiden einigermaßen renommierten Quellen zu dieser Zeit waren *Applied Cryptography* und *Cryptography Engineering* (beide Bücher von Bruce Schneier). Doch spiegelten diese Bücher nicht mehr den neuesten Stand wider. *Applied Cryptography* widmete vier Kapitel den Blockchiffren und ein ganzes Kapitel der Funktionsweise von Chiffren, aber es gab kein einziges Kapitel über authentifizierte Verschlüsselung. Im neueren *Cryptography Engineering* wurde die Kryptografie mit elliptischen Kurven nur in einer Fußnote erwähnt. Andererseits wurden viele meiner Videos oder Blogbeiträge zu erstklassigen Quellen für bestimmte kryptografische Konzepte. Ich wusste, dass ich etwas Wertvolles beisteuern kann.

Nach und nach interessierten sich viele meiner Studenten für Kryptowährungen und stellten immer mehr Fragen zu diesem Thema. Gleichzeitig begann ich, immer mehr Anwendungen für Kryptowährungen zu überprüfen. Später wechselte ich zu

Facebook und war für die Sicherheit der Kryptowährung Libra (heute als Diem bekannt) verantwortlich. Zu jener Zeit waren Kryptowährungen eines der heißesten Arbeitsgebiete, die eine Vielzahl äußerst interessanter kryptografischer Primitive zusammenbrachten, die bis dahin in der realen Welt wenig bis gar keine Anwendung gefunden hatten (Null-Wissen-Beweise, aggregierte Signaturen, Schwellenwertkryptografie, Mehrparteienberechnungen, Konsensprotokolle, kryptografische Akkumulatoren, verifizierbare Zufallsfunktionen, verifizierbare Verzögerungsfunktionen, ... die Liste geht noch weiter). Und dennoch enthielt kein Krypto-Buch ein Kapitel über Kryptowährungen. Meine Ziele waren damit klar.

Ich konnte also etwas schreiben, das Studenten, Entwicklern, Beratern, Sicherheitsingenieuren und anderen vermitteln würde, worum es in der modernen angewandten Kryptografie geht. Es sollte ein Buch mit wenigen Formeln, dafür aber mit vielen Diagrammen werden. Auf die geschichtlichen Hintergründe wollte ich weitgehend verzichten, dafür aber von kryptografischen Fehlern, mit denen ich selbst zu tun hatte, erzählen. Die veralteten Algorithmen sollten nur eine untergeordnete Rolle spielen, aber Kryptografie, die ich aus eigener Erfahrung kannte, sollte breiten Raum einnehmen: TLS, das Noise-Protokoll-Framework, das Signal-Protokoll, Kryptowährungen, HSMs, Schwellenwert-Kryptografie usw. Das Buch sollte weniger die theoretische Kryptografie beleuchten, sondern vor allem das enthalten, was relevant werden könnte: PAKE (Password-Authenticated Key Exchange), Null-Wissen-Beweise, Post-Quanten-Kryptografie usw.

Als sich Manning Publications 2018 bei mir meldete und mich fragte, ob ich ein Buch über Kryptografie schreiben möchte, kannte ich die Antwort bereits. Was ich schreiben wollte, wusste ich. Ich hatte nur darauf gewartet, dass mir jemand die Gelegenheit und einen Vorwand gab, meine Zeit damit zu verbringen, das Buch zu schreiben, das ich im Sinn hatte. Es trifft sich gut, dass Manning eine Reihe von Büchern über die »reale Welt« im Programm hat, und so schlug ich natürlich vor, dass mein Buch sie erweitern sollte. Was Sie hier vor sich haben, ist das Ergebnis von mehr als zwei Jahren harter Arbeit und viel Hingabe. Ich hoffe, es gefällt Ihnen!

Danksagungen

Vielen Dank an Marina Michaels für ihre kontinuierliche Hilfe und ihre Einblicke, ohne die dieses Buch wahrscheinlich nicht zustande gekommen wäre.

Mein Dank geht auch an Jean-Philippe Aumasson, Fabian Becker, Daniel Li, Jeff Lau, Filipe Casal, Curtis Light, Vincent Herbert, Donald Piret, Dan Cashman, Ricky Han, Tshaka Lekholoane, Frances Buran, Sam Zaydel, Michael Rosenberg, Pascal Knecht, Seth David Schoen, Eyal Ronen, Saralynn Chick, Robert Seacord, Eloi Manuel, Rob Wood, Hunter Monk, Jean-Christophe Forest, Liviu Bartha, Mattia Reggiani, Olivier Guerra, Andrey Labunov, Carl Littke, Yan Ivnitskiy, Keller Fuchs, Roman Zabicki, M K Saravanan, Sarah Zennou, Daniel Bourdrez, Jason Noll, Ilias Cherkaoui, Felipe De Lima, Raul Siles, Matteo Bocchi, John Woods, Kostas Chalkias, Yolan Romailler, Gerardo Di Giacomo, Gregory Naza-

rio, Rob Stubbs, Ján Jančár, Gabe Pike, Kiran Tummala, Stephen Singam, Jeremy O'Donoghue, Jeremy Boone, Thomas Duboucher, Charles Guillemet, Ryan Sleevi, Lionel Rivière, Benjamin Larsen, Gabriel Giono, Daan Sprenkels, Andreas Krogen, Vadim Lyubashevsky, Samuel Neves, Steven (Dongze) Yue, Tony Patti, Graham Steel und alle Livebook-Kommentatoren für die vielen Diskussionen und Korrekturen sowie das fachliche und redaktionelle Feedback.

An alle Rezensenten: Adhir Ramjiawan, Al Pezewski, Al Rahimi, Alessandro Campeis, Bobby Lin, Chad Davis, David T Kerns, Domingo Salazar, Eddy Vluggen, Gábor László Hajba, Geert Van Laethem, Grzegorz Bernaś, Harald Kuhn, Hugo Durana, Jan Pieter Herweijer, Jeff Smith, Jim Karabatsos, Joel Kotarski, John Paraskevopoulos, Matt Van Winkle, Michal Rutka, Paul Grebenc, Richard Lebel, Ruslan Shevchenko, Sanjeev Jaiswal, Shawn P Bolan, Thomas Doylend, William Rudenmalm – eure Vorschläge haben dem Buch wirklich gutgetan.

Über dieses Buch

An *Kryptografie in der Praxis* schreibe ich nun seit mehr als zwei Jahren. Ursprünglich war es gedacht als Einführung in alles, was man über die Art von Kryptografie wissen muss, die in der realen Welt verwendet wird. Aber das ist natürlich eine unmögliche Aufgabe. Kein Gebiet lässt sich in einem einzigen Buch zusammenfassen. Deshalb musste ich ein Gleichgewicht finden zwischen dem Umfang an Details, die ich dem Leser vermitteln möchte, und der Größe des abzudeckenden Gebiets. Ich hoffe, Sie sehen das genauso wie ich. Wenn Sie nach einem praktischen Buch suchen, das Ihnen die Kryptografie so, wie sie in Unternehmen und Produkten implementiert und verwendet wird, nahebringt, und wenn Sie neugierig darauf sind, wie Kryptografie in der realen Welt hinter den Kulissen funktioniert, aber nicht auf ein Nachschlagewerk aus sind, dann ist dieses Buch genau das richtige für Sie.

Wer dieses Buch lesen sollte

Im Folgenden habe ich den Leserkreis aufgelistet, der meiner Meinung nach von diesem Buch profitieren wird (doch lassen Sie sich deshalb bitte nicht in eine Schublade stecken).

Studenten

Wenn Sie Informatik, Sicherheit oder Kryptografie studieren und etwas über Kryptografie in der realen Welt lernen möchten (weil Sie entweder einen Job in der Industrie anstreben oder an angewandten Themen in der Wissenschaft arbeiten möchten), dann dürfte dieses Buch meiner Ansicht nach für Sie genau richtig sein. Warum? Weil ich, wie ich im Vorwort schrieb, selbst einmal Student war und ein Buch verfasst habe, das ich damals selber gern gehabt hätte.

Sicherheitspraktiker

Pentester, Sicherheitsberater, Sicherheitsingenieure, Sicherheitsarchitekten und andere Experten im Sicherheitsbereich haben den Großteil meiner Studenten ausgemacht, als ich angewandte Kryptografie unterrichtet habe. Deshalb habe ich diesen Stoff durch die vielen Fragen verfeinert, die mir gestellt wurden, als ich komplizierte kryptografische Konzepte für Nicht-Kryptografen zu erklären versuchte. Da ich selbst als Sicherheitspraktiker tätig bin, ist dieses Buch auch von der Kryptografie geprägt, die ich für große Unternehmen geprüft habe, und von den Bugs, die ich im Rahmen dieser Arbeit kennengelernt und gefunden habe.

Entwickler, die Kryptografie direkt oder indirekt verwenden

Diese Arbeit ist auch von vielen Diskussionen geprägt worden, die ich mit Kunden und Mitarbeitern geführt habe, die im Großen und Ganzen weder Sicherheitsexperten noch Kryptografen waren. Heutzutage wird es immer schwieriger, Code zu schreiben, der gänzlich ohne Kryptografie auskommt, und deshalb muss man ein gewisses Verständnis für die Verfahren haben, auf die man setzt. Dieses Buch vermittelt Ihnen unter anderem dieses Verständnis anhand von Programmbeispielen in verschiedenen Programmiersprachen.

Kryptografen, die sich für andere Gebiete interessieren

Dieses Buch ist eine Einführung in angewandte Kryptografie, die für Leute wie mich nützlich ist. Wie schon erwähnt, habe ich es zuerst für mich selbst geschrieben. Wenn ich es geschafft habe, gute Arbeit zu leisten, sollte ein theoretischer Kryptograf in der Lage sein, die Welt der angewandten Kryptografie schnell zu erfassen; ein anderer, der an symmetrischer Verschlüsselung arbeitet, sollte schnell erfassen können, wie der kennwortgeschützte Schlüsselaustausch funktioniert, wenn er das entsprechende Kapitel liest; und ein Dritter, der sich mit Protokollen beschäftigt, sollte schnell ein gutes Verständnis für Quantenkryptografie bekommen; und so weiter.

Ingenieure und Produktmanager, die mehr wissen möchten

Dieses Buch versucht auch, Fragen zu beantworten, die für mich eher produktorientiert sind: Was sind die Kompromisse und Beschränkungen dieser Ansätze? Welches Risiko gehe ich ein? Würde mir dieser Weg helfen, die Vorschriften einzuhalten? Was muss ich tun, um mit einer Regierung zusammenzuarbeiten?

Neugierige, die wissen wollen, worum es in der Welt der realen Kryptografie geht

Um dieses Buch zu lesen, müssen Sie keiner der oben genannten Typen sein. Es genügt, wenn Sie ein wenig neugierig sind, was Kryptografie ist und wie man sie in der realen Welt verwendet. Denken Sie daran, dass ich weder die Geschichte

der Kryptografie noch die Grundlagen der Informatik lehre. Deshalb sollten Sie zumindest schon einmal von Kryptografie gehört haben, bevor Sie sich auf ein Buch wie dieses einlassen.

Vorausgesetztes Wissen, die lange Version

Was brauchen Sie, um dieses Buch optimal nutzen zu können? Zunächst einmal setzt dieses Buch voraus, dass Sie ein gewisses Grundverständnis davon haben, wie Ihr Laptop oder das Internet funktioniert, und zumindest sollten Sie von Verschlüsselung schon mal gehört haben. Da es in diesem Buch um Kryptografie in der realen Welt geht, wird es schwierig sein, die Dinge in den richtigen Zusammenhang zu bringen, wenn Sie sich mit Computern gar nicht auskennen oder noch nie etwas von *Verschlüsselung* gehört haben.

Wenn Sie einigermaßen wissen, worauf Sie sich einlassen, ist es von großem Vorteil, wenn Ihnen Bits und Bytes geläufig sind und wenn Sie bitweise Operationen wie XOR, Linksschieben und derartige Dinge schon einmal gesehen oder sogar verwendet haben. Ist es andernfalls ein K.-o.-Kriterium? Nein, aber es kann bedeuten, dass Sie hier und da einige Minuten ins Stocken geraten, um etwas zu googeln, bevor Sie weiterlesen können.

Doch ganz gleich, wie qualifiziert Sie sind, müssen Sie wahrscheinlich von Zeit zu Zeit eine Pause einlegen, um sich weitere Informationen aus dem Internet zu holen. Entweder (Asche auf mein Haupt) weil ich vergessen habe, einen Begriff zu erklären, bevor ich ihn verwende, oder weil ich irrtümlich davon ausgegangen bin, dass Sie ihn bereits kennen. In jedem Fall sollte dies kein Problem darstellen, da ich versuche, die verschiedenen Konzepte, die ich einführe, in möglichst einfachen Worten zu erklären.

Wenn Sie schließlich das Wort *Kryptografie* verwenden, denken Sie möglicherweise an Mathematik. Falls Sie nicht nur daran denken, sondern auch noch das Gesicht verziehen, wird es Sie erfreuen zu hören, dass Sie sich darüber keine Sorgen machen müssen. In *Kryptografie in der Praxis* geht es darum, Einblicke zu vermitteln, damit Sie ein Gespür dafür bekommen, wie das Ganze funktioniert. Zudem wird versucht, mathematische Details möglichst zu vermeiden.

Natürlich würde ich lügen, wenn ich behaupte, dass dieses Buch gänzlich ohne Mathematik auskommt. Es gibt keinen Kryptografieunterricht ohne Mathematik. Daher formuliere ich es so: Es ist hilfreich, wenn Sie ein gutes Niveau in Mathematik erreicht haben, aber auch, wenn das nicht der Fall ist, sollte Sie das nicht davon abhalten, den größten Teil dieses Buches zu lesen. Einige Kapitel werden Ihnen vielleicht nicht so liegen, es sei denn, Sie haben ein weitergehendes Verständnis von Mathematik, was insbesondere die letzten Kapitel (14 und 15) zur Quantenkryptografie und Kryptografie der nächsten Generation betrifft. Doch nichts ist unmöglich und Sie können diese Kapitel mit Willenskraft und durch Googeln zu Matrixmultiplikationen und anderen Dingen, die Sie vielleicht nicht kennen, meistern. Wenn Sie diese Kapitel überspringen möchten, sollten Sie aber auf keinen Fall Kapitel 16 auslassen, denn das ist das Sahnehäubchen auf dem Kuchen.

Wegweiser durch das Buch

Kryptografie in der Praxis ist in zwei Teile gegliedert. Den ersten Teil sollten Sie von der ersten bis zur letzten Seite lesen. Er deckt die meisten Bausteine der Kryptografie ab: nämlich die Elemente, aus denen Sie am Ende wie mit LEGO-Steinen komplexere Systeme und Protokolle konstruieren.

- Kapitel 1 ist eine Einführung in praktische Kryptografie, die Ihnen eine Vorstellung davon vermittelt, was Sie lernen werden.
- In Kapitel 2 geht es um Hashfunktionen, einen fundamentalen Algorithmus der Kryptografie, mit dem sich aus Bytestrings eindeutige Bezeichner erstellen lassen.
- Kapitel 3 erläutert, was Datenauthentifizierung ist und wie Sie sicherstellen können, dass niemand Ihre Nachrichten verändert.
- Kapitel 4 befasst sich mit Verschlüsselung, die es zwei Teilnehmern ermöglicht, ihre Kommunikation vor Beobachtern zu verbergen.
- Kapitel 5 stellt den Schlüsselaustausch vor, der es Ihnen ermöglicht, interaktiv ein gemeinsames Geheimnis mit einer anderen Person auszuhandeln.
- Kapitel 6 beschreibt die asymmetrische Verschlüsselung, die es mehreren Personen ermöglicht, Nachrichten an eine einzige Person zu verschlüsseln.
- Thema von Kapitel 7 sind Signaturen, die kryptografischen Entsprechungen von Unterschriften mit Stift auf Papier.
- In Kapitel 8 geht es um Zufälligkeit und darum, wie Sie Ihre Geheimnisse verwalten.

Der zweite Teil dieses Buches enthält die Systeme, die aus diesen Elementen aufgebaut sind.

- In Kapitel 9 erfahren Sie, wie Sie die Verbindungen zwischen Computern mit Verschlüsselung und Authentifizierung (über das SSL/TLS-Protokoll) sichern.
- Kapitel 10 beschreibt die Ende-zu-Ende-Verschlüsselung, bei der es im Grunde darum geht, wie Menschen wie Sie und ich einander vertrauen können.
- Kapitel 11 zeigt, wie Computer Personen authentifizieren und wie Personen dabei helfen können, dass sich Computer miteinander synchronisieren.
- Kapitel 12 ist dem aufstrebenden Gebiet der Kryptowährungen gewidmet.
- Kapitel 13 konzentriert sich auf Hardware-Kryptografie, d. h. auf die Geräte, mit denen Sie verhindern können, dass Ihre Schlüssel entwendet werden.

Es gibt zwei Bonuskapitel: Kapitel 14 über Post-Quanten-Kryptografie und Kapitel 15 über Kryptografie der nächsten Generation. Diese beiden Gebiete finden allmählich Eingang in Produkte und Unternehmen, entweder weil sie an Relevanz gewinnen oder weil sie immer praktischer und effizienter werden. Ich bin Ihnen nicht böse, wenn Sie diese beiden letzten Kapitel auslassen, aber Sie sollten unbe-

dingt Kapitel 16 mit abschließenden Bemerkungen lesen, bevor Sie dieses Buch ins Regal stellen. Kapitel 16 fasst die verschiedenen Herausforderungen und die verschiedenen Lektionen zusammen, die ein Kryptografie-Praktiker (also Sie, wenn Sie dieses Buch durchgearbeitet haben) im Kopf behalten muss. Wie sagte doch Spidermans Onkel Ben Parker: »Aus großer Kraft folgt große Verantwortung.«

Über den Code

Dieses Buch enthält viele Beispiele von Quellcode sowohl in nummerierten Listings als auch im laufenden Text. In beiden Fällen ist der Quellcode in `Schreibmaschinenschrift` formatiert, um ihn vom normalen Text zu unterscheiden. Manchmal ist der Code auch **`fett gedruckt`**, um Code hervorzuheben, der sich gegenüber früheren Schritten im Kapitel geändert hat, zum Beispiel wenn eine neue Funktion zu einer bestehenden Codezeile hinzukommt.

In vielen Fällen wurde der ursprüngliche Quellcode neu formatiert; wir haben Zeilenumbrüche hinzugefügt und die Einrückungen bearbeitet, um dem verfügbaren Platz auf den Buchseiten zu entsprechen. Hat das in seltenen Fällen nicht ausgereicht, wurden Zeilenfortsetzungszeichen (➥) in die Listings eingefügt. Außerdem wurden oftmals die Kommentare aus den Quellcode-Listings entfernt, wenn der Code ohnehin im Text beschrieben wird. In vielen Listings heben begleitende Codeanmerkungen wichtige Konzepte hervor.

Über den Autor

David Wong ist leitender Kryptografie-Ingenieur bei O(1) Labs und arbeitet an der Kryptowährung Mina. Davor war er Sicherheitsverantwortlicher für die Kryptowährung Diem (vormals bekannt als Libra) bei Novi, Facebook, und davor Sicherheitsberater bei der NCC Group im Bereich Kryptografiedienste.

Im Laufe seiner Karriere hat David Wong an mehreren öffentlich finanzierten Open-Source-Audits teilgenommen, beispielsweise an OpenSSL und Let's Encrypt. Er war Sprecher auf verschiedenen Konferenzen, einschließlich Black Hat und DEF CON, und hat in einem regelmäßig stattfindenden Kryptografiekurs bei Black Hat unterrichtet. Hervorzuheben sind seine Beiträge zu Standards wie TLS 1.3 und zum Noise Protocol Framework. Er hat Schwachstellen in vielen Systemen gefunden, einschließlich CVE-2016-3959 in der Golang-Standardbibliothek, CVE-2018-12404, CVE-2018-19608, CVE-2018-16868, CVE-2018-16869 und CVE-2018-16870 in verschiedenen TLS-Bibliotheken.

Unter anderem ist er Autor des Disco-Protokolls (*www.discocrypto.com* und *www.embeddeddisco.com*) und des Decentralized Application Security Project für Smart Contracts (*www.dasp.co*). Zu seinen Forschungen gehören Cache-Angriffe auf RSA (*http://cat.eyalro.net*), ein auf QUIC basierendes Protokoll (*https://eprint.iacr.org/2019/028*), Timing-Angriffe auf ECDSA (*https://eprint.iacr.org/2015/839*) oder Hintertüren in Diffie-Hellman (*https://eprint.iacr.org/2016/644*). Aktuell finden Sie ihn in seinem Blog unter *www.cryptologie.net*.

Teil A

Primitive: Die Elemente der Kryptografie

Willkommen in der Welt der Kryptografie! Das Buch, das Sie in den Händen halten (falls Sie sich für die gedruckte Version entschieden haben), ist in zwei gleiche Teile mit jeweils acht Kapiteln aufgeteilt. Wenn Sie es ganz durcharbeiten, lernen Sie (fast) alles, was es über Kryptografie in der Praxis zu wissen gibt – und zwar in der Welt, in der Sie sich befinden.

Beachten Sie, dass der erste Teil des Buches so geschrieben wurde, dass Sie die Kapitel der Reihe nach lesen sollten. Allerdings nennt Ihnen jedes Kapitel, was vorausgesetzt wird, sodass dies nicht als obligatorische Einschränkung gedacht ist. Die ersten acht Kapitel führen Sie durch die Grundlagen – die Bausteine der Kryptografie. Jedes Kapitel führt ein neues Element ein und erläutert, was es bewirkt, wie es arbeitet und wie es zusammen mit anderen Elementen verwendet werden kann. In diesem ersten Teil geht es vor allem darum, Ihnen gute Abstraktionen und Einblicke zu vermitteln, bevor wir im zweiten Teil alle beschriebenen Elemente praktisch einsetzen.

Viel Erfolg!