A Cryptography Primer

Cryptography has been employed in war and diplomacy from the time of Julius Caesar. In our Internet age, cryptography's most widespread application may be for commerce, from protecting the security of electronic transfers to guarding communication from industrial espionage.

This accessible introduction for undergraduates explains the cryptographic protocols for achieving privacy of communication and the use of digital signatures for certifying the validity, integrity, and origin of a message, document, or program. Rather than offering a how-to on configuring Web browsers and e-mail programs, the author provides a guide to the principles and elementary mathematics underlying modern cryptography, giving readers a look under the hood for security techniques and the reasons they are thought to be secure.

PHILIP N. KLEIN is Professor of Computer Science at Brown University. He was a recipient of the National Science Foundation's Presidential Young Investigator Award, and he has received multiple research grants from the National Science Foundation. He has been made an ACM Fellow in recognition of his contributions to research on graph algorithms. He is a recipient of Brown University's Award for Excellence in Teaching in the Sciences.

A CRYPTOGRAPHY PRIMER

Secrets and Promises

PHILIP N. KLEIN

Brown University, Providence, Rhode Island

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE
UNIVERSITY PRESS

Shaftesbury Road, Cambridge CB2 8EA, United Kingdom

One Liberty Plaza, 20th Floor, New York, NY 10006, USA

477 Williamstown Road, Port Melbourne, VIC 3207, Australia

314–321, 3rd Floor, Plot 3, Splendor Forum, Jasola District Centre, New Delhi – 110025, India

103 Penang Road, #05–06/07, Visioncrest Commercial, Singapore 238467

Cambridge University Press is part of Cambridge University Press & Assessment,
a department of the University of Cambridge.

We share the University's mission to contribute to society through the pursuit of
education, learning and research at the highest international levels of excellence.

www.cambridge.org
Information on this title: www.cambridge.org/9781107017887

First published 2014

A catalogue record for this publication is available from the British Library

Library of Congress Cataloging-in-Publication data
Klein, Philip N., author.
A cryptography primer : secrets and promises / Philip N. Klein,
Brown University, Providence, Rhode Island.
pages cm
Includes bibliographical references and index.
ISBN 978-1-107-01788-7 (hardback) – ISBN 978-1-107-60345-5 (paperback)
1. Computer security. 2. Data encryption (Computer science) 3. Digital signatures.
4. Telecommunication–Safety measures. I. Title.
QA76.9.A25K557 2014
005.8´2–dc23 2013046193

ISBN 978-1-107-01788-7 Hardback
ISBN 978-1-107-60345-5 Paperback

Contents

Preface

In his autobiography, *A Mathematician's Apology*, the number theorist and pacifist G. H. Hardy wrote

> . . . both Gauss and lesser mathematicians may be justified in rejoicing that there is one science [number theory] at any rate . . . whose very remoteness from ordinary human activities should keep it gentle and clean.

Hardy's book was published in 1940, toward the end of his career. If he had postponed his judgment for another 30 years, he might have come to a different conclusion, for number theory became the basis for an important technology long associated with war: cryptography, the use of secret codes.

Cryptography has been in use for at least several thousand years. It is listed in the *Kama Sutra* as one of the 64 arts to be mastered by women. One well-known elementary cryptosystem is attributed to Julius Caesar. Numerous anecdotes attest to the importance of cryptography in war and diplomacy over the years – and to that of cryptanalysis, the cracking of codes. For example, Britain's interception and deciphering of the Zimmerman telegram, a message from Germany's foreign minister to the government of Mexico (via the ambassador), helped speed the United States' entry into World War I, for the message promised Texas, New Mexico, and Arizona to Mexico in return for its help against the United States. Cryptanalysis has played a role in somewhat less momentous events as well; the following is excerpted from the autobiography of Casanova (1757):

> Five or six weeks later, she asked me if I had deciphered the manuscript . . . . I told her that I had.
>
> "Without the key, sir, excuse me if I believe the thing impossible."
>
> "Do you wish me to name your key, madame?" "If you please."

> I then told her the key-word which belonged to no language, and I saw her surprise. She told me that it was impossible, for she believed herself the only possessor of that word which she kept in her memory and which she had never written down.
>
> I could have told her the truth – that the same calculation which had served me for deciphering the manuscript had enabled me to learn the word – but on a caprice it struck me to tell her that a genie had revealed it to me. This false disclosure fettered Madame d'Urfe to me. That day I became the master of her soul, and I abused my power.

In the Information Age, however, cryptography's greatest contribution may be to commerce. Banks have long used cryptography to protect the security of electronic transfers. Geographically distributed corporations have used cryptography to protect their communication from industrial espionage. Perhaps the most exciting applications, however, involve securing communication between parties that have no previous connection and have therefore had no opportunity to agree on a key in advance. As commerce on the Internet grows, such applications will become ever more prevalent. Fortunately, technologies such as exponential key exchange and public-key cryptography exist to make such applications possible.

Public-key cryptography, proposed by Diffie and Hellman in 1976, is the idea of having two separate keys, a public key for encryption of a message and a secret key for its decryption; a party can privately construct the two keys and then make the encryption key public without thereby revealing the decryption key. Subsequently, anyone can encrypt messages intended for the creator of the keys, but only the creator can decrypt. The first realization of this idea was due to Rivest, Shamir, and Adleman in 1978. The extent to which their scheme has captured the popular imagination is reflected by the following excerpt from a Harlequin romance, *Sunward Journey:*

> "I'm really not into computers, Jay. I don't know much. I do know the key to the code was the product of two long prime numbers, each about a hundred digits, right?"
>
> "Yes, that's correct. It's called the RSA cryptosystem."
>
> "Right, for Rivest, Shamir, and Adleman from MIT. That much I know. I also understand that even using a sophisticated computer to decipher the code it would take forever," she recalled. "Something like three point eight billion years for a two-hundred-digit key, right?" "That's exactly correct. All of the stolen information was apparently tapped from the phone lines running from the company offices to your house. Supposedly no one except Mike had the decoding key, and no one could figure it out unless he passed it along, but there has to be a bug in that logic somewhere," he said, loosening his dark green silk tie. "Vee, it's much warmer than I thought. Would you mind if I removed my jacket?"
>
> "Of course not. You're so formal," she remarked . . . .

As our heroine, Vee, states, RSA is based on properties of the product of two prime numbers. Thus it harnesses Hardy's favorite area of "pure" mathematics, number theory. The basis of this cryptosystem (like most) is the dichotomy between easy and hard. Creating the public and secret keys is roughly as easy as selecting and multiplying the two hundred-digit prime numbers. As Vee asserts, cracking the system (using currently known methods) requires an exorbitant amount of time; it seems to require one to determine the two prime numbers from their product, a problem called integer factorization. Though progress on this problem continues, known algorithms (recipes) to solve it are not fast enough to seriously threaten the security of RSA – not yet, anyway. To quote a man known more for marketing skill than expertise in number theory,

> Because both the system's privacy and the security of digital money depend on encryption, a breakthrough in mathematics or computer science that defeats the cryptographic system could be a disaster. The obvious mathematical breakthrough would be development of an easy way to factor large prime numbers. – Bill Gates, *The Road Ahead*, first edition, p. 265

(To factor a number is to determine the prime numbers that when multiplied together form the number; if a number is prime then factoring yields just the number itself.)

But RSA has uses other than encryption. As Diffie and Hellman realized, the flip side of public-key cryptography is digital signatures. Using a method such as RSA, the creator of the two keys can construct a *signature* for a document, a number derived from the document in such a way that anyone who knows the public key can verify the signature is consistent with that document. Furthermore, only someone who knows the secret key can construct a valid signature for a given document, so a valid signature associated with a document is strong evidence that the creator of the keys was responsible for producing the signature. If someone tampers with the document, the signature will no longer bear the same mathematical relation to the document, so the document will be deemed invalid. Digital signatures can thus be used to authenticate messages sent over the Internet, guarding against undetected tampering and forged messages. They can be used for creating unforgeable certificates, such as an electronic version of a credit card or passport. They can also be used to detect unauthorized changes to a computer program, such as the introduction of a virus.

Other technologies for computer security have been developed, including methods for securely authenticating a party (the secure analogue of reciting a phone card number or credit card number or mother's maiden name over the telephone), methods for committing to a document without revealing it (the secure analogue of a sealed envelope), and methods for time-stamping a document (the secure analogue of mailing oneself a letter in order to get it postmarked).

The technology of cryptography rests on the science of computation in that it crucially relies on the fundamental premise of that science, the dichotomy between computationally easy problems and computationally difficult problems: codes should be easy to decrypt if you know the key, hard if you don't. Cryptography is thus a concrete realization of this intellectual pursuit.

In order to expose a broader audience to the excitement of this fun, increasingly important, and intellectually challenging field, I have developed a course, "Secrets and Promises: An Introduction to Digital Security." I have written this book for that course. The word "secrets" in the title refers to the use of cryptography for achieving privacy of communication; the word "promises" refers to the use of digital signatures for certifying the validity, integrity, and origin of a message, document, or program. This text is intended as a gentle introduction to the principles and elementary mathematics underlying modern cryptography. It is not a practical, "how-to" text; it will not instruct readers in the use of present-day computer programs (such as web browsers and e-mail programs) that employ digital security. Such programs are forever evolving; moreover, they will be successful in the marketplace only if using them does not depend on knowledge of the underlying security techniques. In this text, we will look under the hood; we will study the security techniques and the reasons they are thought to be secure.

For some of the fundamental cryptographic schemes, such as AES and SHA, the details are rather unenlightening. In this text, we will omit detailed discussion of these schemes. The roles these schemes play will instead be filled by schemes based on elementary number theory. These number-theoretic schemes are a bit too slow to be used in practice, but they are considered secure and they fit better into the curriculum of this text. Thus we make some sacrifice in adherence to practice in order to achieve greater uniformity and readability. Those readers hungry for details on AES, etc., can easily find them in other texts.

Acknowledgments

Many thanks to Sarah Finney, Peter Galea, Kevin Ingersoll, and Mark Weaver, who have helped shape the course on which this text is based. Thanks also to the National Science Foundation, which helped to sponsor the course's development. Thanks to Michael Yanagisawa, who helped in proofreading. Thanks, finally, to Alice, Bob, Eve, and the other characters that frequent the literature of modern cryptography.