MATHEMATICAL WORLD VOLUME 29

The Mathematics of Encryption

An Elementary Introduction

Margaret Cozzens
Steven J. Miller

AMS
American Mathematical Society

The Mathematics of Encryption
An Elementary Introduction

http://dx.doi.org/10.1090/mawrld/029

MATHEMATICAL WORLD VOLUME 29

The Mathematics of Encryption
An Elementary Introduction

Margaret Cozzens
Steven J. Miller

Providence, Rhode Island

2010 *Mathematics Subject Classification.* Primary 94A60, 68P25, 01-01.

For additional information and updates on this book, visit
www.ams.org/bookpages/mawrld-29

Library of Congress Cataloging-in-Publication Data

Cozzens, Margaret B.

The mathematics of encryption : an elementary introduction / Margaret Cozzens, Steven J. Miller.

pages cm. — (Mathematical world ; 29)

Includes bibliographical references and index.

1. Coding theory–Textbooks. 2. Cryptography–Textbooks. 3. Cryptography–Mathematics–Textbooks. 4. Cryptography–History–Textbooks. 5. Data encryption (Computer science)–Textbooks. I. Miller, Steven J., 1974– II. Title.

QA268.C697 2013
652′.80151—dc23

2013016920

---

10 9 8 7 6 5 4 3 2 1 18 17 16 15 14 13

Margaret Cozzens dedicates to Tyler and Brad.

Steven Miller dedicates to Cameron and Kayla Miller, for their patience as the book was written and for hours of fun exploring the Caesar cipher.

This book is also dedicated to the men and women who have advanced freedom's cause through the centuries by devoting and sometimes giving up their lives to breaking codes and protecting these successes.

Contents

Preface xi

Acknowledgments xvii

Chapter 1. Historical Introduction 1
1.1. Ancient Times 2
1.2. Cryptography During the Two World Wars 8
1.3. Postwar Cryptography, Computers, and Security 12
1.4. Summary 14
1.5. Problems 15

Chapter 2. Classical Cryptology: Methods 19
2.1. Ancient Cryptography 20
2.2. Substitution Alphabet Ciphers 22
2.3. The Caesar Cipher 24
2.4. Modular Arithmetic 26
2.5. Number Theory Notation 28
2.6. The Affine Cipher 30
2.7. The Vigenère Cipher 33
2.8. The Permutation Cipher 36
2.9. The Hill Cipher 39
2.10. Summary 42
2.11. Problems 42

Chapter 3. Enigma and Ultra 51
3.1. Setting the Stage 51
3.2. Some Counting 54
3.3. Enigma's Security 60
3.4. Cracking the Enigma 67
3.5. Codes in World War II 70
3.6. Summary 72
3.7. Appendix: Proofs by Induction 73

3.8. Problems 75

Chapter 4. Classical Cryptography: Attacks I 81
4.1. Breaking the Caesar Cipher 81
4.2. Function Preliminaries 84
4.3. Modular Arithmetic and the Affine Cipher 86
4.4. Breaking the Affine Cipher 91
4.5. The Substitution Alphabet Cipher 94
4.6. Frequency Analysis and the Vigenère Cipher 99
4.7. The Kasiski Test 102
4.8. Summary 106
4.9. Problems 107

Chapter 5. Classical Cryptography: Attacks II 113
5.1. Breaking the Permutation Cipher 114
5.2. Breaking the Hill Cipher 115
5.3. Running Key Ciphers 120
5.4. One-Time Pads 122
5.5. Summary 127
5.6. Problems 128

Chapter 6. Modern Symmetric Encryption 133
6.1. Binary Numbers and Message Streams 133
6.2. Linear Feedback Shift Registers 138
6.3. Known-Plaintext Attack on LFSR Stream Ciphers 142
6.4. LFSRsum 145
6.5. BabyCSS 150
6.6. Breaking BabyCSS 152
6.7. BabyBlock 158
6.8. Security of BabyBlock 161
6.9. Meet-in-the-Middle Attacks 162
6.10. Summary 164
6.11. Problems 164

Chapter 7. Introduction to Public-Channel Cryptography 171
7.1. The Perfect Code Cryptography System 173
7.2. KidRSA 180
7.3. The Euclidean Algorithm 182
7.4. Binary Expansion and Fast Modular Exponentiation 188
7.5. Prime Numbers 192
7.6. Fermat's little Theorem 198
7.7. Summary 203
7.8. Problems 203

Chapter 8. Public-Channel Cryptography 213
8.1. RSA 214
8.2. RSA and Symmetric Encryption 218

8.3. Digital Signatures 219
8.4. Hash Functions 221
8.5. Diffie–Hellman Key Exchange 225
8.6. Why RSA Works 228
8.7. Summary 230
8.8. Problems 231

Chapter 9. Error Detecting and Correcting Codes 239
9.1. Introduction 240
9.2. Error Detection and Correction Riddles 241
9.3. Definitions and Setup 247
9.4. Examples of Error Detecting Codes 249
9.5. Error Correcting Codes 252
9.6. More on the Hamming $(7, 4)$ Code 255
9.7. From Parity to UPC Symbols 257
9.8. Summary and Further Topics 259
9.9. Problems 261

Chapter 10. Modern Cryptography 269
10.1. Steganography—Messages You Don't Know Exist 269
10.2. Steganography in the Computer Age 273
10.3. Quantum Cryptography 278
10.4. Cryptography and Terrorists at Home and Abroad 282
10.5. Summary 285
10.6. Problems 285

Chapter 11. Primality Testing and Factorization 289
11.1. Introduction 289
11.2. Brute Force Factoring 291
11.3. Fermat's Factoring Method 295
11.4. Monte Carlo Algorithms and FℓT Primality Test 299
11.5. Miller–Rabin Test 302
11.6. Agrawal–Kayal–Saxena Primality Test 305
11.7. Problems 310

Chapter 12. Solutions to Selected Problems 317
12.1. Chapter 1: Historical Introduction 317
12.2. Chapter 2: Classical Cryptography: Methods 317
12.3. Chapter 3: Enigma and Ultra 318
12.4. Chapter 4: Classical Cryptography: Attacks I 319
12.5. Chapter 5: Classical Cryptography: Attacks II 320
12.6. Chapter 6: Modern Symmetric Encryption 320
12.7. Chapter 7: Introduction to Public-Channel Cryptography 320
12.8. Chapter 8: Public-Channel Cryptography 321
12.9. Chapter 9: Error Detecting and Correcting Codes 321
12.10. Chapter 10: Modern Cryptography 322

12.11. Chapter 11: Primality Testing and Factorization 322

Bibliography 325

Index 329

Preface

Many of the challenges and opportunities facing citizens in the twenty-first century require some level of mathematical proficiency. Some obvious ones are optimization problems in business, managing your household's budget, weighing the economic policies and proposals of political candidates, and of course the ever-important quest to build the best fantasy sports team possible and, if not winning your local NCAA basketball pool, at least doing well enough to avoid embarrassment! As important as these are, there are many other applications of mathematics going on quietly around us all the time. In this book we concentrate on issues arising from cryptography, which we'll see is far more than soldiers and terrorists trying to communicate in secret. We use this as the vehicle to introduce you to a lot of good, applicable mathematics; for much of the book all you need is high school algebra and some patience. These are not cookbook problems to help you perfect your math skills, but rather the basis of modern commerce and security! Equally important, you'll gain valuable experience in how to think about and approach difficult problems. This is a highly transferable skill and will serve you well in the years to come.

Cryptography is one of the oldest studies, and one of the most active and important. The word **cryptography** comes from two Greek words: $\kappa\rho\upsilon\tau\tau\grave{o}\varsigma$ (kryptos), meaning secret, and $\gamma\rho\grave{\alpha}\varphi\omega$ (grapho), meaning to write. As these roots imply, it all began with the need for people to communicate securely. The basic setup is that there are two people, and they must be able to quickly, easily, and securely exchange information, often in the presence of an adversary who is actively attempting to intercept and decipher the messages.

In the public mind, the most commonly associated images involve the military. While war stories make for dramatic examples and are very important in both the development of the field and its applications, they are only part of the picture. It's not just a subject for soldiers on the battlefield. Whenever you make an online purchase, you're a player. This example has many of the key features.

The first issue is the most obvious. You need to authorize your credit card company or bank to transfer funds to the merchant; however, you're not face-to-face with the seller, and you have to send your information through a probably very insecure channel. It's imperative that no one is able to obtain your personal information and pretend to be you in future transactions!

There are, however, two other very important items. The process must be fast; people aren't willing to wait minutes to make sure an order has been confirmed. Also, there's always the problem of a message being corrupted. What if some of the message is mistransmitted or misread by the party on the other end? These questions lead us to the study of efficient algorithms and error detection and correction codes. These have found a wealth of applications not just in cryptography, but also in areas where the information is not secret.

Two great examples are streaming video and Universal Product Codes (UPC). In streaming video the information (everything from sports highlights to CSPAN debates) is often unprotected and deliberately meant to be freely available to all; what matters is being able to transmit it quickly and play it correctly on the other end. Fruits and vegetables are some of the few remaining items to resist getting a UPC barcode; these black and white patterns are on almost all products. It may shock you to realize how these are used. It's far more than helping the cashier charge you the proper amount; they're also used to help stores update their inventory in real time as well as correlate and analyze your purchases to better target you in the future! These are both wonderful examples of the need to detect and correct errors.

These examples illustrate that problems and solutions arising from cryptography often have applications in other disciplines. That's why we didn't title this book as an introduction to cryptography, but rather to encryption. Cryptography is of course important in the development of the field, but it's not the entire story.

The purpose of this book is to introduce just enough mathematics to explore these topics and to familiarize you with the issues and challenges of the field. Fortunately, basic algebra and some elementary number theory is enough to describe the systems and methods. This means you can read this book without knowing calculus or linear algebra; however, it's important to understand what "elementary" means. While we don't need to use powerful theorems from advanced mathematics, we do need to be very clever in combining our tools from algebra. Fortunately we're following the paths of giants, who have had numerous "aha moments" and have seen subtle connections between seemingly disparate subjects. We leisurely explore these paths, emphasizing the thought processes that led to these remarkable advances.

Below is a quick summary of what is covered in this book, which we follow with outlines for semester-long courses. Each chapter ends with a collection of problems. Some problems are straightforward applications of

material from the text, while others are quite challenging and are introductions to more advanced topics. These problems are meant to supplement the text and to allow students of different levels and interests to explore the material in different ways. Instructors may contact the authors (either directly or through the AMS webpage) to request a complete solution key.

- Chapter 1 is a brief introduction to the history of cryptography. There is not much mathematics here. The purpose is to provide the exciting historical importance and background of cryptography, introduce the terminology, and describe some of the problems and uses.
- Chapter 2 deals with classical methods of encryption. For the most part we postpone the attacks and vulnerabilities of these methods for later chapters, concentrating instead on describing popular methods to encrypt and decrypt messages. Many of these methods involve procedures to replace the letters of a message with other letters. The main mathematical tool used here is modular arithmetic. This is a generalization of addition on a clock (if it's 10 o'clock now, then in five hours it's 3 o'clock), and this turns out to be a very convenient language for cryptography. The final section on the Hill cipher requires some basic linear algebra, but this section may safely be skipped or assigned as optional reading.
- Chapter 3 describes one of the most important encryption methods ever, the Enigma. It was used by the Germans in World War II and thought by them to be unbreakable due to the enormous number of possibilities provided. Fortunately for the Allies, through espionage and small mistakes by some operators, the Enigma was successfully broken. The analysis of the Enigma is a great introduction to some of the basic combinatorial functions and problems. We use these to completely analyze the Enigma's complexity, and we end with a brief discussion of Ultra, the Allied program that broke the unbreakable code.
- Chapters 4 and 5 are devoted to attacks on the classical ciphers. The most powerful of these is frequency analysis. We further develop the theory of modular arithmetic, generalizing a bit more operations on a clock. We end with a discussion of one-time pads. When used correctly, these offer perfect security; however, they require the correspondents to meet and securely exchange a secret. Exchanging a secret via insecure channels is one of the central problems of the subject, and that is the topic of Chapters 7 and 8.
- In Chapter 6 we begin our study of modern encryption methods. Several mathematical tools are developed, in particular binary expansions (which are similar to the more familiar decimal or base 10 expansions) and recurrence relations (which you may know from the Fibonacci numbers, which satisfy the recursion $F_{n+2} = F_{n+1} + F_n$).

We encounter a problem that we'll face again and again in later chapters: an encryption method which seems hard to break is actually vulnerable to a clever attack. All is not lost, however, as the very fast methods of this chapter can be used in tandem with the more powerful methods we discuss later.

- Chapters 7 and 8 bring us to the theoretical and practical high point of the book, a complete description of RSA (its name comes from the initials of the three people who described it publicly for the first time—Rivest, Shamir, and Aldeman). For years this was one of the most used encryption schemes. It allows two people who have never met to communicate quickly and securely. Before describing RSA, we first discuss several simpler methods. We dwell in detail on why they seem secure but are, alas, vulnerable to simple attacks. In the course of our analysis we'll see some ideas on how to improve these methods, which leads us to RSA. The mathematical content of these chapters is higher than earlier in the book. We first introduce some basic graph theory and then two gems of mathematics, the Euclidean algorithm and fast exponentiation. Both of these methods allow us to solve problems far faster than brute force suggests is possible, and they are the reason that RSA can be done in a reasonable amount of time. Our final needed mathematical ingredient is Fermat's little Theorem. Though it's usually encountered in a group theory course (as a special case of Lagrange's theorem), it's possible to prove it directly and elementarily. Fermat's result allows the recipient to decrypt the message efficiently; without it, we would be left with just a method for encryption, which of course is useless. In addition to describing how RSA works and proving why it works, we also explore some of the implementation issues. These range from transmitting messages quickly to verifying the identity of the sender.
- In Chapter 9 we discuss the need to detect and correct errors. Often the data is not encrypted, and we are just concerned with ensuring that we've updated our records correctly or received the correct file. We motivate these problems through some entertaining riddles. After exploring some natural candidates for error detecting and correcting codes, we see some elegant alternatives that are able to transmit a lot of information with enough redundancy to catch many errors. The general theory involves advanced group theory and lattices, but fortunately we can go quite far using elementary counting.
- We describe some of the complexities of modern cryptography in Chapter 10, such as quantum cryptography and steganography.
- Chapter 11 is on primality testing and factorization algorithms. In the RSA chapters we see the benefits of the mathematicalization of messages. To implement RSA, we need to be able to find two large

primes; for RSA to be secure, it should be very hard for someone to factor a given number (even if they're told it's just the product of two primes). Thus, this advanced chapter is a companion to the RSA chapter, but is not needed to understand the implementation of RSA. The mathematical requirements of the chapter grow as we progress further; the first algorithms are elementary, while the last is the only known modern, provably fast way to determine whether a number is prime. As there are many primality tests and factorization algorithms, there should be a compelling reason behind what we include and what we omit, and there is. For centuries people had unsuccessfully searched for a provably fast primality test; the mathematics community was shocked when Agrawal, Kayal, and Saxena found just such an algorithm. Our goal is not to prove why their algorithm works, but instead to explain the ideas and notation so that the interested reader can pick up the paper and follow the proof, as well as to remind the reader that just because a problem seems hard or impossible does not mean that it is! As much of cryptography is built around the assumption of the difficulty of solving certain problems, this is a lesson worth learning well.

Chapters 1–5 and 10 can be covered as a one semester course in mathematics for liberal arts or criminal justice majors, with little or no mathematics background. If time permits, parts of Chapters 9 and 11 can be included or sections from the RSA chapters (Chapters 7 and 8). For a semester course for mathematics, science, or engineering majors, most of the chapters can be covered in a week or two, which allows a variety of options to supplement the core material from the first few chapters.

A natural choice is to build the semester with the intention of describing RSA in complete detail and then supplementing as time allows with topics from Chapters 9 and 11. Depending on the length of the semester, some of the classical ciphers can safely be omitted (such as the permutation and the Hill ciphers), which shortens several of the first few chapters and lessens the mathematical prerequisites. Other options are to skip either the Enigma/Ultra chapter (Chapter 3) or the symmetric encryption chapter (Chapter 6) to have more time for other topics. Chapters 1 and 10 are less mathematical. These are meant to provide a broad overview of the past, present, and future of the subject and are thus good chapters for all to read.

Cryptography is a wonderful subject with lots of great applications. It's a terrific way to motivate some great mathematics. We hope you enjoy the journey ahead, and we end with some advice:

- `Wzr fdq nhhs d vhfuhw li rqh lv ghdg.`
- `Zh fdq idfwru wkh qxpehu iliwhhq zlwk txdqwxp frpsxwhuv. Zh fdq dovr idfwru wkh qxpehu iliwhhq zlwk d grj wudlqhg wr edun wkuhh wlphv.`
- `Jlyh xv wkh wrrov dqg zh zloo ilqlvk wkh mre.`

Acknowledgments

This book is the outgrowth of introductory cryptography courses for non-math majors taught at Rutgers University and Williams College. It is a pleasure to thank our colleagues and our students for many helpful conversations that have greatly improved the exposition and guided the emphasis, in particular Elliot Schrock (who helped write the Enigma chapter) and Zane Martin and Qiao Zhang (who were the TAs for the 2013 iteration at Williams College, Math 10: `Lqwurgxfwlrq wr Fubswrjudskb`, and who helped guide the class in writing the solutions manual for teachers).

We are especially grateful to Wesley Pegden, who generously shared his notes from versions he taught at Rutgers, and who provided numerous, detailed comments. We also thank our editor, Ed Dunne, for all his help, comments and advice throughout the project, Barbara Beeton and Jennifer Sharp at the AMS for their excellent work in creating the final version of the text, Teresa Levy for designing the cover, and the anonymous referees for their suggestions. We wish to thank a number of people who have read and commented on the book, including especially Katrina Palmer at Appalachian State University, Andrew Baxter at Penn State, and Robert Wilson at Rutgers University. Several members of the NSA community kindly shared general references as well as allowed one of the authors to use an Enigma machine.

Some of this book was inspired by work done with the CCICADA Center at Rutgers, a Department of Homeland Security University Center. Miller was partially supported by NSF grants DMS0600848 and DMS0970067 during the writing of this book, and gratefully acknowledges their support.

Bibliography

[1] W. R. Alford, A. Granville and C. Pomerance, *There are infinitely many Carmichael numbers*, Annals of Mathematics **139** (1994), 703–722. Available online at `http://www.math.dartmouth.edu/~carlp/PDF/paper95.pdf`.

[2] M. Agrawal, N. Kayal and N. Saxena, *PRIMES is in P*, Ann. of Math. (2) **160** (2004), no. 2, 781–793. Available online at `http://annals.math.princeton.edu/wp-content/uploads/annals-v160-n2-p12.pdf`.

[3] G. Ateniese, C. Blundo, A. de Santis, and D. Stinson, *Visual cryptography for general access structures*, Information and Computation **129** (1996), no. 2, 86–106.

[4] K. R. Babu, S. U. Kumar and A. V. Babu, *A survey on cryptography and steganography methods for information security*, International Journal of Computer Applications **12** (2010), no. 3, 13–17, published by the Foundation of Computer Science.

[5] W. Barker (editor), *The History of Codes and Cipher in the United States Prior to WWI*, Aegean Park Press, Laguna Hills, CA, 1978.

[6] W. Barker (editor), *The History of Codes and Cipher in the United States, Part II*, Aegean Park Press, Laguna Hills, CA, 1989.

[7] D. J. Baylis, *Error Correcting Codes: A Mathematical Introduction*, Chapman Hall/CRC Mathematics Series, 1997.

[8] M. Campbell, *Uncrackable codes: The Second World War's last Enigma*, New Scientist, magazine issue 2813, May 30, 2011.

[9] R. D. Carmichael, *Note on a new number theory function*, Bull. Amer. Math. Soc. **16** (1910), no. 5, 232–238.

[10] J. H. Conway and N. J. A. Sloane, *Lexicographic codes: error-correcting codes from game theory*, IEEE Trans. Inform. Theory **32** (1986), no. 3, 337–348.

[11] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, third edition, Springer-Verlag, New York, 1998.

[12] A. D'Agapeyeff, *Codes and Ciphers—A History of Cryptography*, Blackfriars Press, 1949.

[13] H. Davenport, *Multiplicative Number Theory*, 3rd edition, revised by H. Montgomery, Graduate Texts in Mathematics, Vol. 74, Springer-Verlag, New York, 2000.

[14] Daily Mail Online, *Al-Qaeda planned to hijack cruise ships and execute passengers, reveals "treasure trove of intelligence" embedded in PORN video*, retrieved 5/1/2012: `http://www.dailymail.co.uk/news/article-2137848/Porn-video-reveals-Al-Qaeda-planns-hijack-cruise-ships-execute-passengers.html`

[15] S. Droste, *New results on visual cryptography*, In Advances in Cryptology—CRYPTO '96, pp. 401–415, Springer, 1996.

[16] A. Ekert and R. Jozsa, Richard, *Quantum computation and Shor's factoring algorithm*, Rev. Modern Phys. **68** (1996), no. 3, 733–753.
[17] P. Erdős, *On pseudoprimes and Carmichael numbers*, Publ. Math. Debrecen **4** (1956), 201–206. Available online at `http://www.renyi.hu/~p_erdos/ 1956-10.pdf`.
[18] W. F. Friedman, *History of the Use of Codes*, Aegean Park Press, Laguna Hills, CA, 1977.
[19] J. Gallian, *Contemporary Abstract Algebra*, seventh edition, Brooks Cole, Belmont, CA, 2009.
[20] M. J. E. Golay, *Notes on digital coding*, Proc. I.R.E. **37** (1949), 657.
[21] A. Granville, *It is easy to determine whether a given integer is prime*, Bull. Amer. Math. Soc. (N.S.) **42** (2005), no. 1, 3–38. Available online at `http://www.dms.umontreal.ca/~andrew/PDF/Bulletin04.pdf`.
[22] M. Kanemasu, *Golay codes*, MIT Undergraduate Journal of Mathematics **1** (1999), no. 1, 95–99. Available online at `http://www.math.mit.edu/ phase2/UJM/vol1/MKANEM~1.PDF`
[23] Klagenfurt University, *The Breakthrough of Frequency Analysis*, Universitat Klagenfurt, Aug. 2005.
[24] A. Korselt, *Probléme chinois*, L'intermédiaire des mathématiciens **6** (1899), 142–143.
[25] J. Leech and N. J. A. Sloane, *Sphere packings and error-correcting codes*, Canad. J. Math. **23** (1971), 718–745. Available online at `http://cms.math.ca/cjm/v23/cjm1971v23.0718-0745.pdf`.
[26] R. Lewin, *Ultra Goes to War*, Pen and Sword, Barnsley, United Kingdom, 2008.
[27] S. Loepp and W. K. Wootters, *Protecting Information: From classical error correction to quantum cryptography*, Cambridge University Press, 2006.
[28] M. Marayati, Y. Alam and M. H. at-Tayyan, *Al-Kindi's Treatise on Cryptanalysis*, vol. 1, Riyadh, KFCRIS & KACST, 2003. Print. Ser. on Arabic Origins of Cryptology.
[29] R. McCoy, *Navajo code talkers of World War II*, American West **18** (1981), no. 6, 67–74.
[30] W. C. Meadows, *They Had a Chance to Talk to One Another...: The Role of Incidence in Native American Code Talking*, Ethnohistory **56** (2009), no. 2, 269–284.
[31] W. C. Meadows, *The Comanche code talkers of World War II*, University of Texas Press, Austin, 2002.
[32] A. R. Miller, *The Cryptographic Mathematics of Enigma*, NSA Pamphlet, 2001. `http://www.nsa.gov/about/\_files/cryptologic\_heritage/publications/wwii/engima\_cryptographic\_mathematics.pdf`
[33] S. J. Miller, *The Probability Lifesaver*, Princeton University Press, to appear.
[34] S. J. Miller and C. E. Silva, *If a prime divides a product...*, preprint. `http://arxiv.org/abs/1012.5866`
[35] S. J. Miller and R. Takloo-Bighash, *An Invitation to Modern Number Theory*, Princeton University Press, Princeton, NJ, 2006, 503 pages.
[36] M. Naor and A. Shamir, *Visual cryptography, advances in cryptology*, Eurocrypt '94 Proceeding LNCS (1995), 950, 1–12.
[37] National Science and Technology Council, *Federal Plan for Cyber Security and Information Assurance Research and Development*, April 2006. `http://www.cyber.st.dhs.gov/docs/Federal%20R&D%20Plan%202006.pdf`
[38] T. Nicely, *The pentium bug*, `http://www.trnicely.net/pentbug/pentbug.html`.
[39] T. Nicely, *Enumeration to* 10^{14} *of the twin primes and Brun's constant*, Virginia J. Sci. **46** (1996), 195–204.
[40] D. Nicholas, *Lucky break*, History Today **57** (2007) no. 9, 56–57.

[41] R. Nichols, *Lanaki's Classical Cryptography Course*, Lecture 6, Part II: "Arabian Contributions to Cryptology", American Cryptogram Association, Jan. 1996. Accessed from the web February 9, 2013. http://www.threaded. com/cryptography6.htm.

[42] L. Savu, *Cryptography role in information security*, in Proceedings of the 5th WSEAS international conference on Communications and information technology (CIT11), N. Mastorakis, V. Mladenov, Z. Bojkovic, F. Topalis and K. Psarris editors. World Scientific and Engineering Academy and Society (WSEAS), Stevens Point, Wisconsin, USA, pp. 36–41.

[43] B. R. Roshan Shetty, J. Rohith, V. Mukund, R. Honwade and S. Rangaswamy, *Steganography Using Sudoku Puzzle* (2009), 623–626. doi:10.1109/ARTCom.2009.116.

[44] J. Silverman, *A friendly introduction to number theory*, Pearson Prentice Hall, 2006.

[45] S. Singh, *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*, Anchor Books (a division of Random House), New York, 1999.

[46] S. Singh, *Arab Code Breakers*, SimonSingh.net, 2012, accessed February 14, 2013. http://simonsingh.net/media/articles/maths-and-science/arab-code-breakers.

[47] A. Stiglic, *The PRIMES is in P little FAQ*, September 22, 2008, http://www. instantlogic.net/publications/PRIMES\%20is\%20in\%20P\%20little\%20FAQ.htm

[48] T. M. Thompson, *From error-correcting codes through sphere packings to simple groups*, The Carus Mathematical Monographs, Number 21, the Mathematical Association of America, 1983.

[49] United States Department of Justice, *Criminal complaint by Special Agent Ricci against alleged Russian agents*, June 2010. http://www.justice.gov/opa/documents/062810complaint2.pdf.

[50] University Klagenfurt, *People behind information*, node on "The Breakthrough of Frequency Analysis" in Virtual Exhibitions Informatics, accessed February 27, 2013. http://cs-exhibitions.uni-klu.ac.at/index.php?id=279.

[51] E. R. Verheul and H. C. A. van Tilborg, *Constructions and properties of k out of n visual secret sharing schemes*, Design Codes and Cryptography **11** (1997), no. 2, 179–196.

[52] B. Watson, *Jaysho, moasi, dibeh, ayeshi, hasclishnih, beshlo, shush, gini*, Smithsonian (1993), 2434.

[53] Wikipedia, User 'SilverMaple', *Al-Kindi*, Wikimedia Foundation, accessed February 14, 2013. http://en.wikipedia.org/wiki/Al-Kindi.

[54] J. Wilcox, *Solving the Enigma—History of the Cryptanalytic Bombe*, NSA Pamphlet, 2001. http://www.nsa.gov/about/_files/cryptologicvheritage/publications/wwii/solving_enigma.pdf

[55] W. R. Wilson, *Code talkers*, American History **31** (Jan/Feb 97), no. 6, 16–21.

[56] F. W. Winterbotham, *The Ultra Secret*, Dell, 1975.

[57] F. B. Wrixon, *Codes, Ciphers, Secrets, and Cryptic Communication*, Black Dog and Leventhal Publishers, New York, 1998.

Index

$(\mathbb{Z}/n\mathbb{Z})^*$, 306
$\binom{n}{k}$, 307
$\oplus$, 137
d-regular, 204
k error detecting, 248

adjacency matrix, 205
adjacent, 173
Advanced Encryption Standard (AES), 158, 171
affine cipher, 32
AKS primality test, 308
alphabet, 247
ASCII, 135
attack
  ciphertext-only, 127
  known-plaintext, 127
authenticity, 21
avatar, 278

BabyBlock cipher, 158
BabyCSS, 151
base, 315
base B expansions, 189
bigrams, 116
binary code, 247
binary expansion, 189
binary number system, 134
Binet's formula, 74, 233
binomial coefficient, 58, 59, 307
binomial theorem, 199
birthday attacks, 235
birthday problem, 235
bit, 135, 279
Bletchley Park, 11
block cipher, 158
book code, 7
box principle, 224, 234

Caesar cipher, 22, 24
  key, 25
Carmichael numbers, 201, 299
carrier, 270
ceiling, 189
chaff, 277
chaffing and winnowing, 277
check digit
  Verhoeff, 259
check digit, 258
Chinese Remainder Theorem, 237
Choctaw Indians, 8
cipher, 4
  affine, 32
  Caesar, 22, 24
    key, 25
  Hill, 39, 40
  multiplication, 109
  one-time pad, 122
  running key, 120
  stream, 138
  substitution alphabet, 22
  symmetric, 171
  Vigenère, 34
ciphertext, 22, 24
ciphertext-only attack, 127
clock arithmetic, 27
clumping, 177, 178
code, 4, 240, 247
  k error detecting, 248
  binary, 247
  exactly k error detecting, 249
  fixed length, 247
  Hamming $(7, 4)$, 253
code talkers, 9

codeword, 240, 247
codex, 4
collision, 223
composite, 29, 192
composition, 85
congruent, 27
connected, 205
cover image, 270
crib, 70
cryptanalysis, 1
cryptography, xi, 1, 20
cryptology, 1

decimal expansion, 189
decimal number system, 133
decipher, 21
decode, 21
decryption, 1
degree, 173
Demon, 13
DES, 275
deterministic, 305
Diffie–Hellman, 225, 227
digital signatures, 220
digits, 189
Dirichlet's pigeon-hole principle, 224, 234
disconnected, 205
discrete logarithm problem, 228
divisors, 29
  greatest common, 29
  nontrivial proper, 29
  proper, 29
double factorial, 63
DoubleBabyBlock cipher, 162

edges, 173
encrypt, 21
encryption, 1
Enigma, 11, 51, 52
  notches, 65
  plugboard, 60
  reflector, 65
  rotors, 64
equivalent, 27
Euclid's proof of the infinitude of primes, 290
Euclidean algorithm, 183
  extended, 184, 187
Euler totient function, 215, 236, 305
Euler's theorem, 211, 237
extended Euclidean algorithm, 184, 187

factorial
  double, 63
factorial function, 23, 56
factorization
  brute force, 291, 292
  Fermat's method, 295, 297
factors, 29
fast exponentiation, 191
feature coding, 272
Ferguson, 261
Fermat
  Fermat's Last Theorem (FLT), 210
  Fermat's little Theorem (FℓT), 198
  method, 295, 297
  primality test, 200, 299
  test for $\mathcal{PC}$, 300
  witness, 201
Fibonacci, 207
Fibonacci numbers, 74, 233
filtering, 275
fixed length code, 247
floor, 183, 188
frequency analysis, 82
function
  Euler totient, 305
  factorial, 23
  inverse, 85
functions, 85
Fundamental Theorem of Arithmetic, 29, 291

Gaussian elimination, 149
Germain prime, 232
graph, 173
  adjacent, 173
  degree, 173
  edges, 173
  loop, 173
  vertices, 173
greatest common divisor (gcd), 29, 182, 183

Hales, 261
Hamming code, 253
Hamming distance, 248
hash functions, 222
  ToyHash algorithm, 222
Heisenberg Uncertainty Principle, 278
hieroglyphs, 2
Hill cipher, 39, 40
horizontal line shift coding, 272
Horner's algorithm, 232

induction, 63
inverse
  modular, 85
inverse function, 85, 108
invertible, 40

Jewels, 12
Jigsaw, 285

Kasiski test, 102
Kepler conjecture, 261
key, 270
key escrow, 13
keystream, 34
KidRSA, 181
known-plaintext attack, 127

lattice, 260
least significant bit, 273
LEDs, 279
letter swap, 19
LFSRsum, 145
Linear Feedback Shift Register (LFSR), 139
links, 173
log laws, 315
logarithm, 315
loops, 173
LSB, 273
Lucifer, 13

MAC, 277
masking, 275
matrices, 40
maximum distance, 248
meet-in-the-middle, 163
microdots, 276
Miller–Rabin
  primality test, 304
  test, 302, 304
minimum distance, 248
modular inverse, 85
modulo, 27
modulo arithmetic, 27
modulus, 27
Monster group, 261
Monte Carlo algorithm, 300, 302
muddle, 159
multiplication cipher, 109
multiplicativity of combinations, 54

Navajo Indians, 9
nodes, 173
nomenclators, 5
nontrivial proper divisor, 29
notches, 65
null ciphers, 272

odd part, 303
one-time pad, 122
Operation Torch, 51
order
  element, 307

package, 270
parity, 244
Patton, George S., 51
payload, 270
perfect code, 174
perfect code cryptosystem, 177
  clumping, 177
  private key, 177
perfect security, 123
perfect squares, 198
permutation, 37
PGP, 13
pigeon-hole principle, 224, 234
plaintext, 24
PNT, 197
polynomial-time algorithm, 305
Pretty Good Privacy, 13
primality test
  AKS, 308
  Fermat's little Theorem, 299, 300
  Miller–Rabin, 304
prime, 29, 192
prime number theorem, 197, 293
proof by contradiction, 193, 195
proofs by induction, 73
  base case, 73
  inductive step, 73
proper divisor, 29
property $\mathcal{PC}$, 300
Purple, 11

quantum computing, 285
quantum cryptography, 14
quantum key distribution, 14
qubits, 279

recursion, 23
recursive, 23
reduces, 27
reduction, 27
reflector, 65
Rejewski, Marion, 68

relatively prime, 29, 90
Room 40, 8
rotors, 64
RSA, 13, 214, 216
  problem, 230
  theorem, 229
running key cipher, 120

S-box, 160
Secure Hash Algorithm (SHA)
  SHA-1, 225
seed, 140
self-loops, 204
sifr, 4
signature, 21
signatures, 220
simple, 204
sphere packings, 260
Stager cipher, 7
steganography, 13, 20, 269
stego-function, 270
stego-object, 270
still images, 273
Strassen algorithm, 208, 233
stream ciphers, 138
substitution alphabet ciphers, 22
Sudoku puzzles, 275
symmetric ciphers, 171

text extraction, 285
totient function, 215, 236, 305
ToyHash, 222
transmit, 21
transparencies, 283
transposition, 48
trap-door functions, 294
triangle inequality, 253
Turing, Alan, 70
twin primes, 197

Ultra, 11, 52
unit, 29, 192
Universal Product Code (UPC)
  symbols, 257

valid encryption scheme, 21, 22
Verhoeff, Jacobus, 259
vertical line shift coding, 272
vertices, 173
Vigenère cipher, 34
  Kasiski test, 102
  keystream, 34

winnowing, 277

XOR, 137

Zimmerman telegram, 8

Published Titles in This Series

29 **Margaret Cozzens and Steven J. Miller,** The Mathematics of Encryption, 2013
28 **David Wright,** Mathematics and Music, 2009
27 **Jacques Sesiano,** An Introduction to the History of Algebra, 2009
26 **A. V. Akopyan and A. A. Zaslavsky,** Geometry of Conics, 2007
25 **Anne L. Young,** Mathematical Ciphers, 2006
24 **Burkard Polster,** The Shoelace Book, 2006
23 **Koji Shiga and Toshikazu Sunada,** A Mathematical Gift, III, 2005
22 **Jonathan K. Hodge and Richard E. Klima,** The Mathematics of Voting and Elections: A Hands-On Approach, 2005
21 **Gilles Godefroy,** The Adventure of Numbers, 2004
20 **Kenji Ueno, Koji Shiga, and Shigeyuki Morita,** A Mathematical Gift, II, 2004
19 **Kenji Ueno, Koji Shiga, and Shigeyuki Morita,** A Mathematical Gift, I, 2003
18 **Timothy G. Feeman,** Portraits of the Earth, 2002
17 **Serge Tabachnikov, Editor,** Kvant Selecta: Combinatorics, I, 2002
16 **V. V. Prasolov,** Essays on Numbers and Figures, 2000
15 **Serge Tabachnikov, Editor,** Kvant Selecta: Algebra and Analysis, II, 1999
14 **Serge Tabachnikov, Editor,** Kvant Selecta: Algebra and Analysis, I, 1999
13 **Saul Stahl,** A Gentle Introduction to Game Theory, 1999
12 **V. S. Varadarajan,** Algebra in Ancient and Modern Times, 1998
11 **Kunihiko Kodaira, Editor,** Basic Analysis: Japanese Grade 11, 1996
10 **Kunihiko Kodaira, Editor,** Algebra and Geometry: Japanese Grade 11, 1996
9 **Kunihiko Kodaira, Editor,** Mathematics 2: Japanese Grade 11, 1997
8 **Kunihiko Kodaira, Editor,** Mathematics 1: Japanese Grade 10, 1996
7 **Dmitri Fomin, Sergey Genkin, and Ilia V. Itenberg,** Mathematical Circles, 1996
6 **David W. Farmer and Theodore B. Stanford,** Knots and Surfaces, 1996
5 **David W. Farmer,** Groups and Symmetry: A Guide to Discovering Mathematics, 1996
4 **V. V. Prasolov,** Intuitive Topology, 1994
3 **L. E. Sadovskiĭ and A. L. Sadovskiĭ,** Mathematics and Sports, 1993
2 **Yu. A. Shashkin,** Fixed Points, 1991
1 **V.M. Tikhomirov,** Stories about Maxima and Minima, 1991

How quickly can you compute the remainder when dividing 109837^{97} by 120143? Why would you even want to compute this? And what does this have to do with cryptography?

Photo courtesy of Walter Morris

Photo courtesy of Cesar E. Silva

Modern cryptography lies at the intersection of mathematics and computer science, involving number theory, algebra, computational complexity, fast algorithms, and even quantum mechanics. Many people think of codes in terms of spies, but in the information age, highly mathematical codes are used every day by almost everyone, whether at the bank ATM, at the grocery checkout, or at the keyboard when you access your email or purchase products online.

This book provides a historical and mathematical tour of cryptography, from classical ciphers to quantum cryptography. The authors introduce just enough mathematics to explore modern encryption methods, with nothing more than basic algebra and some elementary number theory being necessary. Complete expositions are given of the classical ciphers and the attacks on them, along with a detailed description of the famous Enigma system. The public-key system RSA is described, including a complete mathematical proof that it works. Numerous related topics are covered, such as efficiencies of algorithms, detecting and correcting errors, primality testing and digital signatures. The topics and exposition are carefully chosen to highlight mathematical thinking and problem solving. Each chapter ends with a collection of problems, ranging from straightforward applications to more challenging exercises that introduce advanced topics. Unlike many books in the field, this book is aimed at a general liberal arts student, but without losing mathematical completeness.

ISBN: 978-0-8218-8321-1

9 780821 883211

MAWRLD/29

For additional information and updates on this book, visit

www.ams.org/bookpages/mawrld-29