

Includes Advanced Encryption Standard RIJNDAEL

RICHARD A. MOLLIN

An INTRODUCTION to

CRYPTOGRAPHY

An abstract, dark, and textured background image, possibly representing a map or a complex pattern, in shades of blue and black, occupying the lower half of the cover.

CHAPMAN & HALL/CRC

TN 918.2
M726

An INTRODUCTION to

CRYPTOGRAPHY

RICHARD A. MOLLIN



E200201068

CHAPMAN & HALL/CRC

Boca Raton London New York Washington, D.C.

Library of Congress Cataloging-in-Publication Data

Mollin, Richard A., 1947–

An introduction to cryptography / Richard A. Mollin.

p. cm.

Includes bibliographical references and index.

ISBN 1-58488-127-5

1. Coding theory. I. Title.

QA268 .M65 2000

003'.54—dc21

00-055482

CIP

This book contains information obtained from authentic and highly regarded sources. Reprinted material is quoted with permission, and sources are indicated. A wide variety of references are listed. Reasonable efforts have been made to publish reliable data and information, but the author and the publisher cannot assume responsibility for the validity of all materials or for the consequences of their use.

Neither this book nor any part may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, microfilming, and recording, or by any information storage or retrieval system, without prior permission in writing from the publisher.

The consent of CRC Press LLC does not extend to copying for general distribution, for promotion, for creating new works, or for resale. Specific permission must be obtained in writing from CRC Press LLC for such copying.

Direct all inquiries to CRC Press LLC, 2000 N.W. Corporate Blvd., Boca Raton, Florida 33431.

Trademark Notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation, without intent to infringe.

Visit the CRC Press Web site at www.crcpress.com

© 2001 by Chapman & Hall/CRC

No claim to original U.S. Government works

International Standard Book Number 1-58488-127-5

Library of Congress Card Number 00-055482

Printed in the United States of America 3 4 5 6 7 8 9 0

Printed on acid-free paper

An INTRODUCTION to

CRYPTOGRAPHY

The CRC Press Series on
**DISCRETE
MATHEMATICS
AND
ITS APPLICATIONS**

Series Editor

Kenneth H. Rosen, Ph.D.

AT&T Bell Laboratories

The CRC Handbook of Combinatorial Designs,

Charles J. Colbourn and Jeffrey H. Dinitz

Frames and Resolvable Designs: Uses, Constructions, and Existence,

Steven Furino, Ying Miao, and Jianxing Yin

Handbook of Discrete and Computational Geometry,

Jacob E. Goodman and Joseph O'Rourke

Design Theory, Charles C. Lindner and Christopher A. Rodgers

Network Reliability: Experiments with a Symbolic Algebra Environment,

Daryl D. Harms, Miroslav Kraetzl, Charles J. Colbourn, and John S. Devitt

Handbook of Applied Cryptography, Alfred J. Menezes, Paul C. van Oorschot,

and Scott A. Vanstone

Quadratics, Richard A. Mollin,

Fundamental Number Theory with Applications, Richard A. Mollin

Cryptography: Theory and Practice, Douglas R. Stinson

Graph Theory and Its Applications, Jonathan Gross and Jay Yellen

Combinatorial Algorithms: Generation Enumeration, and Search,

Donald L. Kreher and Douglas R. Stinson

Introduction to Information Theory and Data Compression, Darrel R. Hankerson

Greg A. Harris, and Peter D. Johnson

Handbook of Discrete and Combinatorial Mathematics, Kenneth H. Rosen

Abstract Algebra Applications with Maple, Richard Klima, Ernest Stitzinger,

and Neil Sigmon

An Atlas of The Smaller Maps in Orientable and Nonorientable Surfaces,


David Jackson and Terry Visentin

Algebraic Number Theory, Richard A. Mollin

To Bridget — my muse

Preface

This book is intended for a one-semester introductory undergraduate course in cryptography. The text has been designed in such a way that the reader with little mathematical background can work through the text, and the reader with a firm mathematical background will encounter sufficient challenging material to sustain interest. Any mathematics required is presented herein in advance of the cryptographic material requiring it. The impetus for the writing of this text arose from this author's involvement in designing an undergraduate course in introductory cryptography for the Mathematics Department at the University of Calgary in 1998. No suitable text for that course was on the market, nor is there one at the time of this writing, hence the incarnation of this one. Essentially, the text is meant for *any* reader who wants an introduction to the area of cryptography. The core material is self-contained so that the reader may learn the basics of cryptography without having to go to another source. However, in the optional material sections, such as Section Two of Chapter Five, where the number field sieve is studied, the reader will require some knowledge of algebraic number theory such as that given in this author's previous book [145]. Also, for the advanced topics in optional Chapter Six, such as Section One on elliptic curve methods in primality testing, factoring, and cryptosystems, some algebraic background is required, but the basics of elliptic curves are developed in that section for the benefit of the reader.

For the instructor, a course outline is, simply put, the first four chapters (excluding the material in Section Three of Chapter Two on cryptanalysis of DES and the details of its AES successor — Rijndael) as the core material for a basic introduction to the area. Optional material (determined by the pointing hand symbol ) may be added at the discretion of the instructor, depending upon the needs and background of the students involved. The material in Section One of Chapter One is a motivator for the material in the text by giving an overview of the history of the subject, beginning with the first rumblings of cryptography in ancient Egypt four millennia ago and ending with our modern-day needs and challenges. There is sufficient historical data on various ciphers, such as the Caesar Cipher, the Playfair Cipher, the German World War I ADFGVX Field Cipher, and one of Edgar Allan Poe's famous cryptograms, to provide a novel set of challenging exercises at the end of this first section to motivate the reader further. Section Two of Chapter One is similarly a history, this time of factoring and primality testing. This may be seen as a precursor to the core material in Chapter Four and the optional material in Chapter Five. We begin with the notion of a prime defined in Euclid's Elements and proceed through several primality testing and factoring techniques introduced by Fibonacci and developed by Fermat, Euler, and numerous others up to Lucas at the end of the nineteenth century. We continue with Kraitichik, Lehmer, and others whose work ushered in the twentieth century, setting the groundwork for algorithms to be developed in the computer age. Section Three of Chapter One develops the basics of computer arithmetic, and sets the stage for Section Four which

explores complexity issues.

Section One of Chapter Two is an introduction to modular arithmetic. The language of congruences is developed from the basic definition through Wilson's Theorem, Fermat's Little Theorem, Euler's generalization, the Arithmetic of the Totient, the Chinese Remainder Theorem and its generalization together with numerous illustrations such as the Coconut Problem, the Egg Basket Problem, and the Units of Work Problem, culminating in a tool to be used in many of the cryptographic techniques developed in the text — the Repeated Squaring Method for Modular Exponentiation. Section Two of Chapter Two is devoted to the first of the two symmetric-key cryptosystems to be studied, namely block ciphers. From requisite definitions of the basic concepts such as enciphering and deciphering transformations, we provide detailed discussions, with examples and diagrams, of numerous block ciphers including: affine, substitution, running-key, as well as transposition and permutation ciphers; concluding with a complete, detailed description of the Data Encryption Standard, DES, together with many illustrative figures. Section Three of Chapter Two is optional, containing a discussion of modes of operation and cryptanalysis of block ciphers such as DES, and its AES successor — *Rijndael*. We give a complete, detailed, illustrated description of the Rijndael Cipher, which is preceded by a discussion of Feistel Ciphers of which DES is an example, and the reign of which Rijndael brought to an end. Section Four of Chapter Two deals with the other class of symmetric-key ciphers — stream ciphers. The reader is taken on a journey from the basic definition of a stream cipher through the notions of keystreams, seeds, generators, randomness, one-time pads, synchronous and self-synchronizing ciphers, linear feedback shift registers, and nonlinear combination generators, plus several illustrations and examples.

Chapter Three addresses public-key cryptosystems, beginning in Section One with exponentiation, discrete logarithms, and protocols. In particular, we present the Pohlig-Hellman Symmetric Key Exponentiation Cipher, one-way functions, coin flipping via both exponentiation and one-way functions, bit commitment protocols, the Pohlig-Hellman Algorithm for computing discrete logarithms, hash functions, message authentication codes, and the Diffie-Hellman Key-exchange Protocol. The latter motivates the discussion in Section Two where we look at public-key cryptosystems, beginning with the definition of trapdoor one-way functions, which leads to a discussion of the RSA Public-Key Cryptosystem. Then a definition of modular roots and power residues fleshes out our knowledge of congruences sufficiently to describe the Rabin and ElGamal Public-key Ciphers. Section Three deals with issues surrounding authentication, the need for which is motivated by an illustrated discussion of impersonation attacks on public-key cryptosystems. This leads into a definition of the notions surrounding digital signatures. As illustrations, we present the RSA, Rabin, and ElGamal Public-key Signature schemes. Section Four studies the Knapsack Problem. Once the basics are set up, we provide a definition of superincreasing sequences, illustrated by the Merkle-Hellman and Chor-Rivest Knapsack Cryptosystems. Chapter Three concludes with a comparison and a contrasting of symmetric-key and public-key ciphers, with a description of the

modern approach using combinations of both types of ciphers for a more secure cryptographic envelope.

Chapter Four deals with primality testing, starting in Section One with an introduction to primitive roots, moving from the definition to a discussion of Gauss's Algorithm for computing primitive roots, Artin's Conjecture, and the fundamental primitive root theorem. We then engage in a development of the index calculus, leading to Euler's Criterion for power residue congruences. Our knowledge of quadratic residues is then advanced by the introduction of the Legendre Symbol and its properties, which allows us to prove Gauss's Quadratic Reciprocity Law. Another step up is taken with a definition of the Jacobi Symbol and its properties, which we need later in the chapter. Section Two inspects true primality tests including the Lucas-Lehmer Test, the Pocklington Theorem, Proth's Theorem, and Pepin's Test. The section concludes with a discussion of complexity of primality testing, including the introduction of the notion of a certificate. Probabilistic primality tests are the topic of Section Three, starting with the definitions of Euler Liars, pseudoprimes, and witnesses. Then we work through and illustrate the Solovay-Strassen Probabilistic Primality Test. Once the concept of strong pseudoprimes, liars, and witnesses are introduced, we are in a position to present the Miller-Rabin-Selfridge (strong pseudoprime) Test. The section concludes with a general discussion of Monte Carlo Algorithms, of which the latter two algorithms are examples.

Chapter Five on factoring is the first of two optional chapters. Section One involves an illustrated description of three factoring algorithms: Pollard's $p - 1$ Method, the Brillhart-Morrison Continued Fraction Algorithm, and the quadratic sieve. A brief history of how the work of Legendre, Euler, Kraitchik, and Lehmer led to the development of these algorithms is also provided, as is a discussion of how the notions can be generalized. This motivates the topic of Section Two, which begins with an illustration of how Pollard's original idea for factoring with cubic integers led to the development of the number field sieve. Then a detailed description of the special number field sieve is given (with the factorization of the ninth Fermat Number as an illustration) along with a discussion of its complexity in relation to the general number field sieve.

Chapter Six contains advanced topics. The first section introduces elliptic curves from the basic definition and leads the reader through the development of the elliptic curve group structure with several figures to illustrate the geometry in relation to the algebraic development. Once the basics are established, we state (without proof) some deep results needed for the cryptography, including the Nagell-Lutz Theorem, Mazur's Theorem, Mordell's Theorem, Siegel's Theorem, and Hasse's Theorem. We then present, and illustrate with worked examples, Lenstra's Elliptic Curve Factoring Method as well as the Elliptic Curve Primality Test and some generalizations thereof. To prepare for the cryptosystems, we generalize the notion of discrete logs to elliptic curves, and describe both the ElGamal and Menezes-Vanstone Public-key Elliptic Curve Cryptosystems. The section concludes with a discussion of the security of elliptic curve ciphers. The next section takes a look at the concept of Zero-knowledge Proofs in its various formats. We illustrate with the Feige-Fiat-Shamir Identification

Protocol, the cut and choose protocol, and Hamiltonian Circuits. The section is concluded with a study of noninteractive zero-knowledge protocols and zero-knowledge proofs of discrete log. Section Three, the last section of the main text of the book, takes us into the realm of quantum cryptography. The basis upon which the latter rests is the Heisenberg Uncertainty Principle that we discuss at length. We demonstrate how this principle can be used to generate a secret key for a quantum cryptosystem, called quantum key generation. The amazing properties of both quantum computers and quantum cryptography are considered, including the proposals for nuclear magnetic resonance-based quantum computers. The latter are closer to the proposed DNA-based computers, which would be several orders of magnitude faster than the fastest supercomputers known today. To take the reader to the edge of the fantastic, we also look at quantum teleportation and all that implies. The building of a quantum computer (a prototype of which already exists) would have dramatic consequences, not the least of which would be the breaking of public-key cryptography, such as RSA cryptosystems.

The following highlights other aspects and special features of the text.

◆ Features of This Text

- The book is ideal for the student since it offers a wealth of exercises with nearly 300 problems. The more challenging exercises are marked with a ☆. Also, complete and detailed solutions to all of the *odd-numbered exercises* are provided at the back of the text. Complete and detailed solutions of the *even-numbered exercises* are included in a *Solutions Manual*, which is available from the publisher for the instructor who adopts the text for a course. The exercises marked with two stars are to be considered only by the reader who requires an *exceptional challenge*, or for the instructor to extract from the solutions manual to present to students as an additional feature.

- The text is *accessible* to anyone from the beginning undergraduate to the research scientist. Appendix A, described below, contains a review of all of the requisite background material. Essentially, the reader can work through the book without any serious impediment or need to seek another source in order to learn the core material.

- There are *more than 50 biographies* of the individuals who helped develop cryptographic concepts. These are given in the footnotes woven throughout the text, to give a human face to the cryptography being presented. A knowledge of the lives of these individuals can only deepen our appreciation of the material at hand. The footnote presentation of their lives allows the reader to have immediate information at will, or to treat them as digressions, and access them later without significantly interfering with the main mathematical text at hand. The *footnotes* contain not only the bibliographical information cited above, but also historical data of interest, as well as other information which the discerning reader may want to explore at leisure.

- There are *optional topics*, denoted by ☞, which add additional material

for the more advanced reader or the reader requiring more challenging material which goes beyond the basics presented in the core data.

- There are more than 80 *examples* throughout the text to illustrate the concepts presented, as well as in excess of 60 diagrams, figures, and tables.

- *Appendix A* contains fundamental facts for the uninitiated reader or the reader requiring a quick finger-tip reference for a reminder of the underlying background used in the text. We begin with the basic notions surrounding set theory, binary relations and operations, functions, the basic laws of arithmetic, as well as notions surrounding divisibility including the Euclidean Algorithm and its generalization, properties of the gcd and lcm, the fundamental theorem of arithmetic, the principle of induction, and properties of the binomial coefficient including the binomial theorem. Then we turn to some basic concepts in matrix theory, the fundamentals surrounding polynomials and polynomial rings (having already introduced the basic notions of groups, rings, and fields in Section One of Chapter Two), morphisms of rings, vector spaces, and sequences. We close with fundamental concepts needed in the text concerning continued fractions.

- For ease of search, the reader will find consecutive numbering, namely object $N.m$ is the m^{th} object in Chapter N (or Appendix N), exclusive of footnotes and exercises, which are numbered separately and consecutively unto themselves. Thus, for instance, Diagram 2.76 is the 76th numbered object in Chapter Two; exclusive of footnotes and exercises; Exercise 3.36 is the 36th exercise in Chapter Three; and Footnote 4.9 is the ninth footnote in Chapter Four.

- The *bibliography* contains more than 200 references for further reading.

- The *list of symbols* is designed so that the reader may determine, at a glance, on which page the first defining occurrence of a desired notation exists, and the symbols are all contained on page 346.

- The *index* has more than 2,400 entries, and has been devised in such a way to ensure that there is maximum ease in getting information from the text.

- The webpage cited in the penultimate line of page xiv will contain a file for comments, and any typos/errors that are found. Furthermore, comments via the e-mail address on the bottom line of page xiv are also welcome.

◆ **Acknowledgments** The author is grateful for the proofreading done by the following people, each of whom lent their own (largely non-intersecting) expertise and valuable time: John Brillhart (U.S.A.), John Burke (U.S.A.), Kell Cheng (my graduate student), Jacek Fabrykowski (U.S.A.), Bart Goddard (U.S.A.), Franz Lemmermeyer (Germany), Renate Scheidler (U.S.A.), Peter Shiue (U.S.A.), Michel Spira (Brazil), Nikos Tzanakis (Greece), and Thomas Zaplachinski (Canada), a former student, now cryptographer.

Richard Mollin, Calgary, July 11, 2000

Preface for the Third Printing

The announcement on October 2, 2000 of the selection of the AES, *Rijndael*, as successor to DES, came swiftly upon the heels of the publication of this text in late August of 2000, and the second printing of this text also went quickly to press. Hence, this printing presented the first opportunity to include an update. Essentially the basic changes, aside from some corrections of minor typos, has been the elimination of the description of the Twofish Cipher, and a replacement with a complete description of the Rijndael Cipher as well as the attendant changes, which that generated, such as an update of the Index and Table of Contents. We have also added an Appendix **A₀** on pages 269–270, which contains a detailed description with examples of the means by which the Rijndael S-Box was constructed, as well as the complete S-Box itself.

Richard Mollin, Calgary, January 6, 2001

website: <http://www.math.ucalgary.ca/~ramollin/>

e-mail: ramollin@math.ucalgary.ca

Contents

Preface.....	ix
Preface for the third printing.....	xiv
1 Origins, Computer Arithmetic, & Complexity	1
1.1 What is Cryptography & Why Study it? — A History .	1
1.2 A History of Factoring & Primality Testing	18
1.3 Computer Arithmetic	32
1.4 Complexity	47
2 Symmetric-Key Cryptosystems	57
2.1 An Introduction to Congruences	57
2.2 Block Ciphers	76
2.3 DES Cryptanalysis & Successor AES	102
2.4 Stream Ciphers	113
3 Public-Key Cryptosystems	127
3.1 Exponentiation, Discrete Logs, & Protocols	127
3.2 Public-Key Cryptography	137
3.3 Authentication	146
3.4 Knapsack	153
4 Primality Testing	161
4.1 An Introduction to Primitive Roots	161
4.2 True Primality Tests	180
4.3 Probabilistic Primality Tests	188
5 Factoring	195
5.1 Three Algorithms	195
5.2 The Number Field Sieve	207
6 Advanced Topics	221
6.1 Elliptic Curves & Cryptography	221
6.2 Zero-Knowledge	252
6.3 Quantum Cryptography	262

Appendix A₀: The Rijndael S-Box	269
Appendix A: Fundamental Facts	271
Solutions to Odd-Numbered Exercises	303
Bibliography	331
List of Symbols	346
Index	347
About the Author	373

Chapter 1

Origins, Computer Arithmetic, & Complexity

1.1 What is Cryptography & Why Study it? — A History

Every area of study has its own language, which includes specific terms that facilitate an understanding of the objects being investigated. The science^{1.1} of *cryptography* refers to the study of methods for sending messages in *secret* (namely, in *enciphered* or *disguised* form) so that only the intended recipient can remove the disguise and read the message (or *decipher* it). The original message is called the *plaintext*, and the disguised message is called the *ciphertext*. The final message, encapsulated and sent, is called a *cryptogram*. The process of transforming plaintext into ciphertext is called *encryption* or *enciphering*. The reverse process of turning ciphertext into plaintext, which is accomplished by the recipient who has the knowledge to remove the disguise, is called *decryption*^{1.2} or *deciphering*. Anyone who engages in cryptography is called a *cryptographer*. On the other hand, the study of mathematical techniques for attempting to defeat

^{1.1}Some would call it an *art*, or an art *and* a science (for instance see [173, p. 1]). However, herein we are concerned with the mathematical techniques that are embraced by this study, and the computational tools used to implement them. Hence, the term “science” is apt. Moreover, if we (broadly) define art as *creative skill or its application*, and science as *a systematized branch of knowledge operating upon objective principles*, then we will see in the following historical perspective that cryptography may be viewed as having begun as an *art* in the course of human development, but is very seriously a *science* in our modern world. Cryptography has, as its etymology, *kryptos* from the Greek, meaning *hidden*, and *graphein*, meaning *to write*. The (English) term *cryptography* was coined in 1658 by Thomas Browne, a British physician and writer.

^{1.2}Some people (if not entire cultures) find the terms *encrypt* and *decrypt* to be repugnant since the terms may be interpreted as referring to dead bodies. Thus, *encipher* and *decipher* are becoming the standard in usage. Also, some sources call the process of turning ciphertext into plaintext *exploitation* (see [64, p. 92]).

cryptographic methods is called *cryptanalysis*. Those practicing cryptanalysis (usually termed the “enemy”) are called *cryptanalysts*. The term *cryptology* is used to embody the study of both cryptography and cryptanalysis, and the practitioners of cryptology are *cryptologists*.^{1.3} We will be primarily concerned in this text with cryptography, and not cryptanalysis.^{1.4}

Cryptography may be viewed as *overt secret writing* in the sense that the writing is clearly seen to be disguised. This is different from *steganography*,^{1.5} which conceals the very *existence* of the message, namely *covert secret writing*. For instance, *invisible ink* would be called a *technical* steganographic method as would suitcases with false bottoms containing a secret message. One of the most famous such methods, employed by the Germans during World War II, was the use of the microdot (invented by Emanuel Goldberg in the 1920’s) as a period in typewritten documents. An example of *linguistic* steganography, the other branch of steganography, is the use of two typefaces to convey a secret message, a technique used by Francis Bacon,^{1.6} which is described in his publication of 1623: *De Augmentis Scientiarum*. Today, hiding (subliminal)^{1.7} messages in television commercials would also qualify. Generally speaking, steganography involves the hiding of secret messages in other messages or devices. The modern convention is to break cryptography into two parts: *cryptography proper* or *overt secret writing*, and *steganography* or *covert secret writing*. The term *steganography* first appeared in the work *Steganographia*, by Johannes Trithemius (1462–1516) which he began writing in 1499. Trithemius’s manuscript was circulated for over a century, and not published until 1606. In 1609, the Roman Catholic Church

^{1.3}The term *cryptology* was coined by James Howell in 1645. However, John Wilkins (1614–72) in his book *Mercury, or the Secret and Swift Messenger*, introduced into the English language the terms *cryptologia* or *secrecy in speech*, and *cryptographia* or *secrecy in writing*. He also used *cryptomeneses* as a general term for any secret communications. Wilkins, who was a cofounder of the Royal Society along with John Wallis (1616–1703) later married Oliver Cromwell’s sister, and became Bishop of Chester. The modern incarnation of the use of the word *cryptology* is probably due to the advent of Kahn’s encyclopedic book [100], *The Codebreakers* published in 1967, after which the term became accepted and established as that area of study embracing both cryptography and cryptanalysis. The etymology of cryptology is the greek *kryptos* meaning *hidden* and *logos* meaning *word*.

^{1.4}Examples of contemporary (research) cryptanalysis may be found in research publications such as the *Journal of Cryptology*, as well as in the proceedings of various regularly held conferences such as the annual American conference, *Crypto*, held in late August in Santa Barbara, California. Historical data on cryptology may be found in the journal *Cryptologia*.

^{1.5}The etymology is *steganos* from the Greek meaning *impenetrable*.

^{1.6}Francis Bacon (1561–1626) was born on January 22, 1561 in London, England. He was educated at Trinity College in Cambridge, and ultimately became a lawyer in 1582. After a brief unsuccessful stint in politics, he became Queen Elizabeth’s counsel. In that capacity, he helped to convict Robert Devereux (1566–1601) the second earl of Essex, for treason, after which Essex was executed. After James I assumed the throne, Bacon again went the political route. Then after a sequence of subsequent legal positions, he was appointed lord chancellor and Baron Verulam in 1618, and by 1621, he was made Viscount St. Albans. In the intervening years 1608–1620, he wrote numerous philosophical works, and wrote several versions of his best-known scientific work, *Novum Organum*. In 1621, Bacon was accused of bribery and fell from power. He spent his final years writing his most valuable and respected works. He died on April 9, 1626 in London.

^{1.7}...if indeed such messages exist. For instance, see <http://www.reall.org/letters/1997-05-16-usnwr-subliminal-messages.html>.

placed it on its index of Prohibited Books, where it remained for over two centuries. Nevertheless, it was reprinted numerous times, including as late as 1721. During Trithemius's lifetime, his *Steganographia* caused him to be known as a sorcerer, which did not sit well since he was an abbot at the abbey of Saint Martin at Spanheim, Germany. In fact, his fellow monks were so incensed that Trithemius was transferred to the monastery of Saint Jacob in Wurzburg, where he remained (writing and studying) until his death on December 15, 1516. Beyond these comments, we will not be concerned in this text with steganography, but rather with cryptography proper. (See [12] for more details on *Steganographia*.)

The first recorded instance of a cryptographic technique was literally written in stone almost four millennia ago. This was done by an Egyptian scribe who used hieroglyphic symbol substitution^{1.8} (albeit at the time not well-developed) in his writing on a rock wall in the tomb of a nobleman of the time, *Khnumhotep*. It is unlikely that the scribe was actually trying to disguise the inscription, but rather was trying to impart some increased prestige (cache) to his inscription of the nobleman's deeds, which included the erection of several monuments for the reigning Pharaoh *Amenemhet* II. In other words, the scribe was attempting to impress the reader, and perhaps impart some authority to his writing, somewhat in a fashion similar to the use of flowery or legalistic language in a modern-day formal document. Although the scribe's intent was not secrecy (the primary goal of modern cryptography) his method of *symbol substitution* was one of the elements of cryptography that we recognize today.^{1.9} Subsequent scribes actually added the essential element of secrecy to their hieroglyphic substitutions (on various tombs), but the end-goal here seems to have been to provide a *riddle* or *puzzle* (and therefore an enticement to read the epitaph) which most readers could relatively easily unravel. Therefore, although the cryptanalysis required was trivial, and the cryptography of hieroglyphic symbol substitution not fully developed, one may reasonably say that the seeds of cryptology were planted in ancient Egypt. Given that cryptology was born quite early, it did not mature rapidly or continuously. It had several incarnations in various cultures, with probably fewer methods extant than the number lost in antiquity.

The oldest extant cryptography from ancient Mesopotamia is an enciphered cuneiform tablet, which has a formula for making pottery glazes, and dates from around 1500 B.C., found on the site of Seleucia on the banks of the Tigris river. Also, the Babylonian and Assyrian scribes occasionally used exceptional or unusual cuneiform symbols on their clay tablets to "sign-off" the message with a date and signature, called *colophons*. However, again, these substitution techniques were not intended to disguise, but rather to display the knowledge of cuneiform held by the individual scribe for later generations to see and admire.

In the Hebrew literature, there is also evidence of letter substitution. The most common is a technique called *atbash*, in which the last and the first letters of the Hebrew alphabet are interchanged, and the remaining letters similarly

^{1.8}By a *substitution*, at this early juncture, we mean a permutation of the plaintext letters. We will give a rigorous mathematical definition later.

^{1.9}The use of substitutions *without* the element of secrecy is called *protocryptography*.