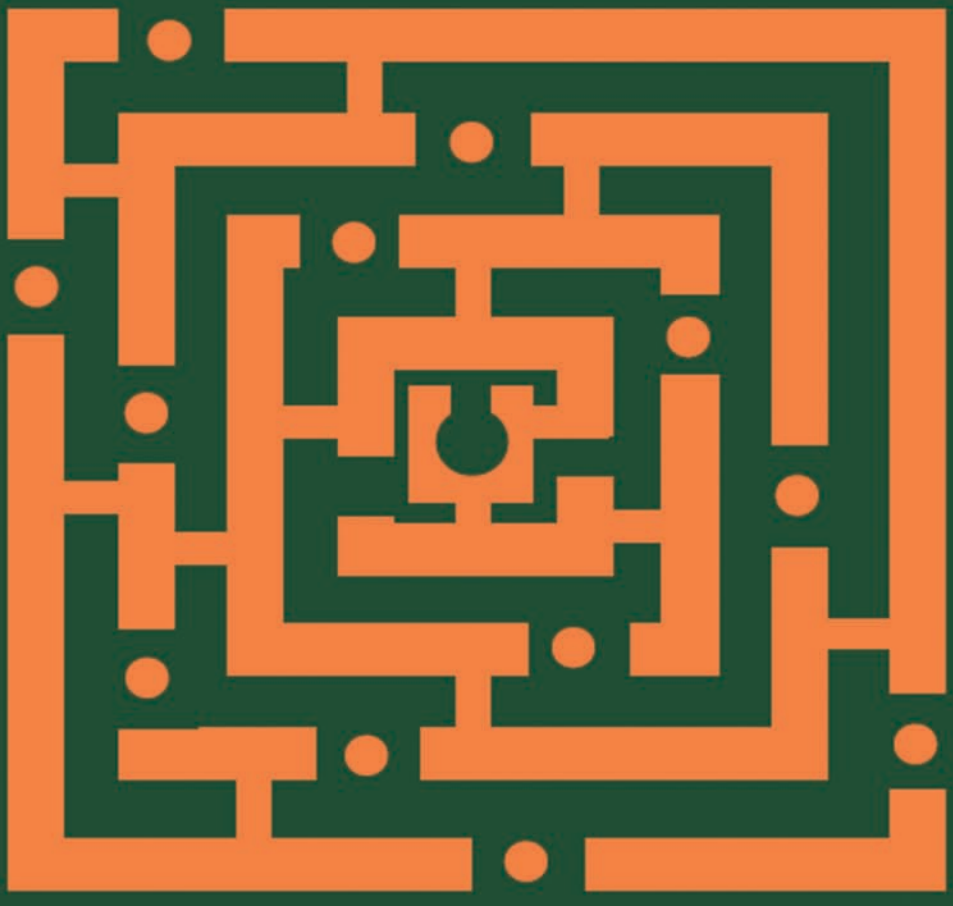
HANDBOOK of APPLIED CRYPTOGRAPHY



Alfred J. Menezes
Paul C. van Oorschot
Scott A. Vanstone

CRC Press
Taylor & Francis Group

HANDBOOK of APPLIED CRYPTOGRAPHY

DISCRETE MATHEMATICS AND ITS APPLICATIONS

Series Editor

Kenneth H. Rosen, Ph.D.

AT&T Laboratories
Middletown, New Jersey

Charles J. Colbourn and Jeffrey H. Dinitz, The CRC Handbook of Combinatorial Designs

Charalambos A. Charalambides, Enumerative Combinatorics

Steven Furino, Ying Miao, and Jianxing Yin, Frames and Resolvable Designs: Uses, Constructions, and Existence

Randy Goldberg and Lance Riek, A Practical Handbook of Speech Coders

Jacob E. Goodman and Joseph O'Rourke, Handbook of Discrete and Computational Geometry

Jonathan Gross and Jay Yellen, Graph Theory and Its Applications

Jonathan Gross and Jay Yellen, Handbook of Graph Theory

Darrel R. Hankerson, Greg A. Harris, and Peter D. Johnson, Introduction to Information Theory and Data Compression

Daryl D. Harms, Miroslav Kraetzl, Charles J. Colbourn, and John S. Devitt, Network Reliability: Experiments with a Symbolic Algebra Environment

David M. Jackson and Terry I. Visentin, An Atlas of Smaller Maps in Orientable and Nonorientable Surfaces

Richard E. Klima, Ernest Stitzinger, and Neil P. Sigmon, Abstract Algebra Applications with Maple

Patrick Knupp and Kambiz Salari, Verification of Computer Codes in Computational Science and Engineering

Donald L. Kreher and Douglas R. Stinson, Combinatorial Algorithms: Generation Enumeration and Search

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

Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, Handbook of Applied Cryptography

Richard A. Mollin, Algebraic Number Theory

Richard A. Mollin, Fundamental Number Theory with Applications

Richard A. Mollin, An Introduction to Cryptography

Richard A. Mollin, Quadratics

Richard A. Mollin, RSA and Public-Key Cryptography

Kenneth H. Rosen, Handbook of Discrete and Combinatorial Mathematics

Douglas R. Shier and K.T. Wallenius, Applied Mathematical Modeling: A Multidisciplinary Approach

Douglas R. Stinson, Cryptography: Theory and Practice, Second Edition

Roberto Togneri and Christopher J. deSilva, Fundamentals of Information Theory and Coding Design

Lawrence C. Washington, Elliptic Curves: Number Theory and Cryptography

Kun-Mao Chao and Bang Ye Wu, Spanning Trees and Optimization Problems

HANDBOOK of APPLIED CRYPTOGRAPHY

Alfred J. Menezes
Paul C. van Oorschot
Scott A. Vanstone

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

ISBN-13: 978-0-84-938523-0 (hbk)

Library of Congress Cataloging-in-Publication Data

Menezes, A. J. (Alfred J.), 1965–
Handbook of applied cryptography / Alfred Menezes, Paul van Oorschot, Scott Vanstone.
p. cm. -- (CRC Press series on discrete mathematics and its applications)
Includes bibliographical references and index.

1. Computers--Access control--Handbooks, manuals, etc.
2. Cryptography--Handbooks, manuals, etc. I. Van Oorschot, Paul C. II. Vanstone, Scott A. III. Title. IV. Series: Discrete mathematics and its applications.
QA76.9.A25M463 1996
0005.8'2--dc21 96-27609
CIP

To Archie and Lida Menezes

To Cornelis Henricus van Oorschot
and Maria Anna Buys van Vugt

To Margaret and Gordon Vanstone

Contents in Brief

Table of Contents

List of Tables

List of Figures

Foreword

by R.L. Rivest

As we draw near to closing out the twentieth century, we see quite clearly that the information-processing and telecommunications revolutions now underway will continue vigorously into the twenty-first. We interact and transact by directing flocks of digital packets towards each other through cyberspace, carrying love notes, digital cash, and secret corporate documents. Our personal and economic lives rely more and more on our ability to let such ethereal carrier pigeons mediate at a distance what we used to do with face-to-face meetings, paper documents, and a firm handshake. Unfortunately, the technical wizardry enabling remote collaborations is founded on broadcasting everything as sequences of zeros and ones that one's own dog wouldn't recognize. What is to distinguish a digital dollar when it is as easily reproducible as the spoken word? How do we converse privately when every syllable is bounced off a satellite and smeared over an entire continent? How should a bank know that it really *is* Bill Gates requesting from his laptop in Fiji a transfer of $10,000,000,000 to another bank? Fortunately, the magical mathematics of cryptography can help. Cryptography provides techniques for keeping information secret, for determining that information has not been tampered with, and for determining who authored pieces of information.

Cryptography is fascinating because of the close ties it forges between theory and practice, and because today's practical applications of cryptography are pervasive and critical components of our information-based society. Information-protection protocols designed on theoretical foundations one year appear in products and standards documents the next. Conversely, new theoretical developments sometimes mean that last year's proposal has a previously unsuspected weakness. While the theory is advancing vigorously, there are as yet few true guarantees; the security of many proposals depends on unproven (if plausible) assumptions. The theoretical work refines and improves the practice, while the practice challenges and inspires the theoretical work. When a system is "broken," our knowledge improves, and next year's system is improved to repair the defect. (One is reminded of the long and intriguing battle between the designers of bank vaults and their opponents.)

Cryptography is also fascinating because of its game-like adversarial nature. A good cryptographer rapidly changes sides back and forth in his or her thinking, from attacker to defender and back. Just as in a game of chess, sequences of moves and counter-moves must be considered until the current situation is understood. Unlike chess players, cryptographers must also consider all the ways an adversary might try to gain by breaking the rules or violating expectations. (Does it matter if she measures how long I am computing? Does it matter if her "random" number isn't one?)

The current volume is a major contribution to the field of cryptography. It is a rigorous encyclopedia of known techniques, with an emphasis on those that are both (believed to be) secure and practically useful. It presents in a coherent manner most of the important cryptographic tools one needs to implement secure cryptographic systems, and explains many of the cryptographic principles and protocols of existing systems. The topics covered range from low-level considerations such as random-number generation and efficient modular exponentiation algorithms and medium-level items such as public-key signature techniques, to higher-level topics such as zero-knowledge protocols. This book's excellent organization and style allow it to serve well as both a self-contained tutorial and an indispensable desk reference.

In documenting the state of a fast-moving field, the authors have done incredibly well at providing error-free comprehensive content that is up-to-date. Indeed, many of the chapters, such as those on hash functions or key-establishment protocols, break new ground in both their content and their unified presentations. In the trade-off between comprehensive coverage and exhaustive treatment of individual items, the authors have chosen to write simply and directly, and thus efficiently, allowing each element to be explained together with their important details, caveats, and comparisons.

While motivated by practical applications, the authors have clearly written a book that will be of as much interest to researchers and students as it is to practitioners, by including ample discussion of the underlying mathematics and associated theoretical considerations. The essential mathematical techniques and requisite notions are presented crisply and clearly, with illustrative examples. The insightful historical notes and extensive bibliography make this book a superb stepping-stone to the literature. (I was very pleasantly surprised to find an appendix with complete programs for the CRYPTO and EUROCRYPT conferences!)

It is a pleasure to have been asked to provide the foreword for this book. I am happy to congratulate the authors on their accomplishment, and to inform the reader that he/she is looking at a landmark in the development of the field.

Ronald L. Rivest
Webster Professor of Electrical Engineering and Computer Science
Massachusetts Institute of Technology
August 1996

Preface

This book is intended as a reference for professional cryptographers, presenting the techniques and algorithms of greatest interest to the current practitioner, along with the supporting motivation and background material. It also provides a comprehensive source from which to learn cryptography, serving both students and instructors. In addition, the rigorous treatment, breadth, and extensive bibliographic material should make it an important reference for research professionals.

Our goal was to assimilate the existing cryptographic knowledge of industrial interest into one consistent, self-contained volume accessible to engineers in practice, to computer scientists and mathematicians in academia, and to motivated non-specialists with a strong desire to learn cryptography. Such a task is beyond the scope of each of the following: research papers, which by nature focus on narrow topics using very specialized (and often non-standard) terminology; survey papers, which typically address, at most, a small number of major topics at a high level; and (regretably also) most books, due to the fact that many book authors lack either practical experience or familiarity with the research literature or both. Our intent was to provide a detailed presentation of those areas of cryptography which we have found to be of greatest practical utility in our own industrial experience, while maintaining a sufficiently formal approach to be suitable both as a trustworthy reference for those whose primary interest is further research, and to provide a solid foundation for students and others first learning the subject.

Throughout each chapter, we emphasize the relationship between various aspects of cryptography. Background sections commence most chapters, providing a framework and perspective for the techniques which follow. Computer source code (e.g. C code) for algorithms has been intentionally omitted, in favor of algorithms specified in sufficient detail to allow direct implementation without consulting secondary references. We believe this style of presentation allows a better understanding of how algorithms actually work, while at the same time avoiding low-level implementation-specific constructs (which some readers will invariably be unfamiliar with) of various currently-popular programming languages.

The presentation also strongly delineates what has been established as fact (by mathematical arguments) from what is simply current conjecture. To avoid obscuring the very applied nature of the subject, rigorous proofs of correctness are in most cases omitted; however, references given in the Notes section at the end of each chapter indicate the original or recommended sources for these results. The trailing Notes sections also provide information (quite detailed in places) on various additional techniques not addressed in the main text, and provide a survey of research activities and theoretical results; references again indicate where readers may pursue particular aspects in greater depth. Needless to say, many results, and indeed some entire research areas, have been given far less attention than they warrant, or have been omitted entirely due to lack of space; we apologize in advance for such major omissions, and hope that the most significant of these are brought to our attention.

To provide an integrated treatment of cryptography spanning foundational motivation through concrete implementation, it is useful to consider a hierarchy of thought ranging from conceptual ideas and end-user services, down to the tools necessary to complete actual implementations. Table 1 depicts the hierarchical structure around which this book is organized. Corresponding to this, Figure 1 illustrates how these hierarchical levels map

Information Security Objectives	
Confidentiality	
Data integrity	
Authentication (entity and data origin)	
Non-repudiation	
Cryptographic functions	
Encryption	Chapters 6, 7, 8
Message authentication and data integrity techniques	Chapter 9
Identification/entity authentication techniques	Chapter 10
Digital signatures	Chapter 11
Cryptographic building blocks	
Stream ciphers	Chapter 6
Block ciphers (symmetric-key)	Chapter 7
Public-key encryption	Chapter 8
One-way hash functions (unkeyed)	Chapter 9
Message authentication codes	Chapter 9
Signature schemes (public-key, symmetric-key)	Chapter 11
Utilities	
Public-key parameter generation	Chapter 4
Pseudorandom bit generation	Chapter 5
Efficient algorithms for discrete arithmetic	Chapter 14
Foundations	
Introduction to cryptography	Chapter 1
Mathematical background	Chapter 2
Complexity and analysis of underlying problems	Chapter 3
Infrastructure techniques and commercial aspects	
Key establishment protocols	Chapter 12
Key installation and key management	Chapter 13
Cryptographic patents	Chapter 15
Cryptographic standards	Chapter 15

Table 1: *Hierarchical levels of applied cryptography.*

onto the various chapters, and their inter-dependence.

Table 2 lists the chapters of the book, along with the primary author(s) of each who should be contacted by readers with comments on specific chapters. Each chapter was written to provide a self-contained treatment of one major topic. Collectively, however, the chapters have been designed and carefully integrated to be entirely complementary with respect to definitions, terminology, and notation. Furthermore, there is essentially no duplication of material across chapters; instead, appropriate cross-chapter references are provided where relevant.

While it is not intended that this book be read linearly from front to back, the material has been arranged so that doing so has some merit. Two primary goals motivated by the "handbook" nature of this project were to allow easy access to stand-alone results, and to allow results and algorithms to be easily referenced (e.g., for discussion or subsequent cross-reference). To facilitate the ease of accessing and referencing results, items have been categorized and numbered to a large extent, with the following classes of items jointly numbered consecutively in each chapter: *Definitions*, *Examples*, *Facts*, *Notes*, *Remarks*, *Algorithms*, *Protocols*, and *Mechanisms*. In more traditional treatments, *Facts* are usually identified as propositions, lemmas, or theorems. We use numbered *Notes* for additional technical points,

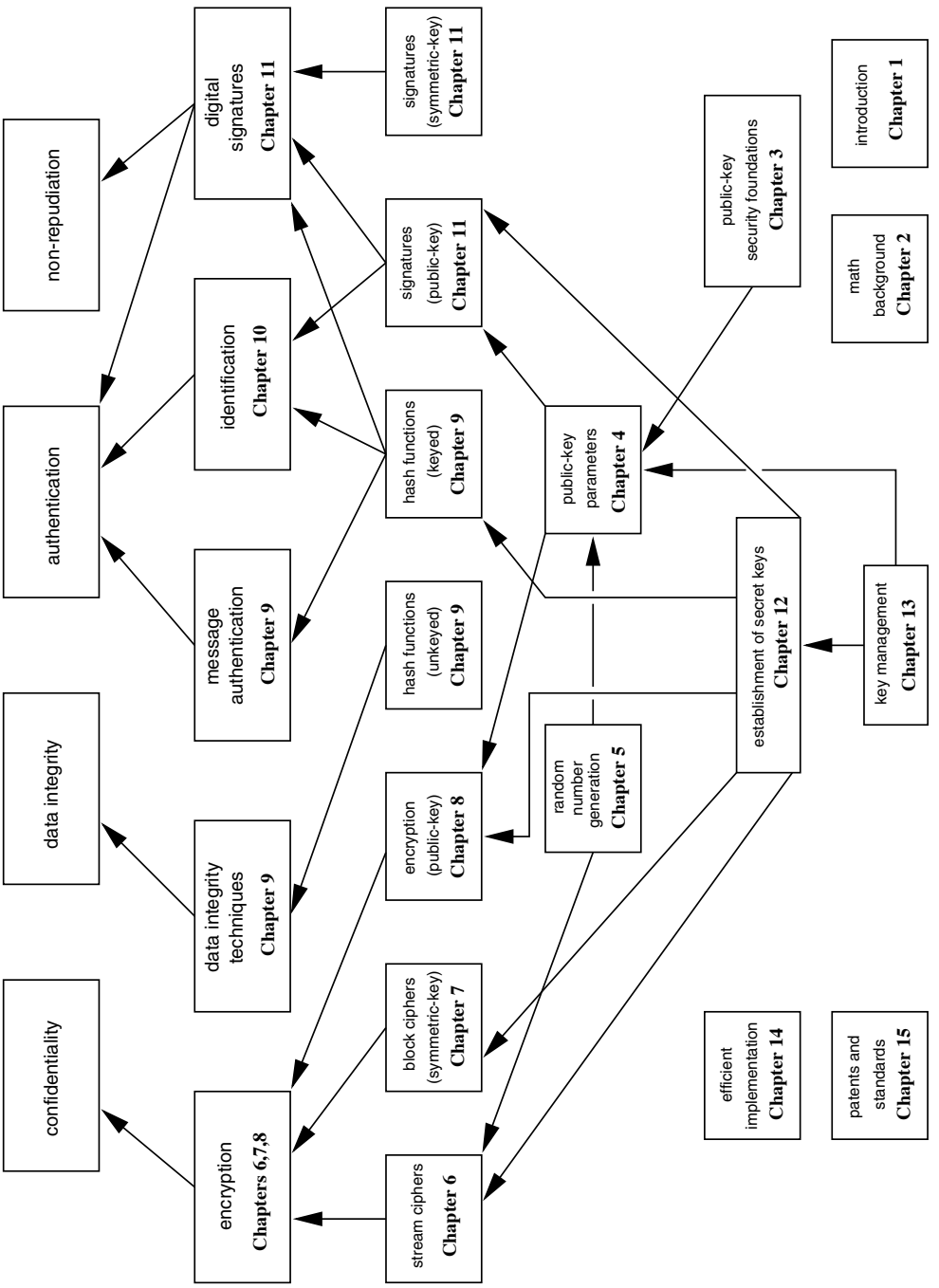


Figure 1: *Roadmap of the book.*

	Chapter	Primary Author		
		AJM	PVO	SAV
1.	Overview of Cryptography	*	*	*
2.	Mathematical Background	*		
3.	Number-Theoretic Reference Problems	*		
4.	Public-Key Parameters	*	*	
5.	Pseudorandom Bits and Sequences	*		
6.	Stream Ciphers	*		
7.	Block Ciphers		*	
8.	Public-Key Encryption	*		
9.	Hash Functions and Data Integrity		*	
10.	Identification and Entity Authentication		*	
11.	Digital Signatures			*
12.	Key Establishment Protocols		*	
13.	Key Management Techniques		*	
14.	Efficient Implementation			*
15.	Patents and Standards		*	
—	Overall organization	*	*	

Table 2: *Primary authors of each chapter.*

while numbered *Remarks* identify non-technical (often non-rigorous) comments, observations, and opinions. *Algorithms*, *Protocols* and *Mechanisms* refer to techniques involving a series of steps. *Examples*, *Notes*, and *Remarks* generally begin with parenthetical summary titles to allow faster access, by indicating the nature of the content so that the entire item itself need not be read in order to determine this. The use of a large number of small subsections is also intended to enhance the handbook nature and accessibility to results.

Regarding the partitioning of subject areas into chapters, we have used what we call a *functional organization* (based on functions of interest to end-users). For example, all items related to entity authentication are addressed in one chapter. An alternative would have been what may be called an *academic organization*, under which perhaps, all protocols based on zero-knowledge concepts (including both a subset of entity authentication protocols and signature schemes) might be covered in one chapter. We believe that a functional organization is more convenient to the practitioner, who is more likely to be interested in options available for an entity authentication protocol (Chapter 10) or a signature scheme (Chapter 11), than to be seeking a zero-knowledge protocol with unspecified end-purpose.

In the front matter, a top-level Table of Contents (giving chapter numbers and titles only) is provided, as well as a detailed Table of Contents (down to the level of subsections, e.g., §5.1.1). This is followed by a List of Figures, and a List of Tables. At the start of each chapter, a brief Table of Contents (specifying section number and titles only, e.g., §5.1, §5.2) is also given for convenience.

At the end of the book, we have included a list of papers presented at each of the Crypto, Eurocrypt, Asiacrypt/Auscrypt and Fast Software Encryption conferences to date, as well as a list of all papers published in the *Journal of Cryptology* up to Volume 9. These are in addition to the *References* section, each entry of which is cited at least once in the body of the handbook. Almost all of these references have been verified for correctness in their exact titles, volume and page numbers, etc. Finally, an extensive Index prepared by the authors is included. The Index begins with a List of Symbols.

Our intention was not to introduce a collection of new techniques and protocols, but rather to selectively present techniques from those currently available in the public domain. Such a consolidation of the literature is necessary from time to time. The fact that many good books in this field include essentially no more than what is covered here in Chapters 7, 8 and 11 (indeed, these might serve as an introductory course along with Chapter 1) illustrates that the field has grown tremendously in the past 15 years. The mathematical foundation presented in Chapters 2 and 3 is hard to find in one volume, and missing from most cryptography texts. The material in Chapter 4 on generation of public-key parameters, and in Chapter 14 on efficient implementations, while well-known to a small body of specialists and available in the scattered literature, has previously not been available in general texts. The material in Chapters 5 and 6 on pseudorandom number generation and stream ciphers is also often absent (many texts focus entirely on block ciphers), or approached only from a theoretical viewpoint. Hash functions (Chapter 9) and identification protocols (Chapter 10) have only recently been studied in depth as specialized topics on their own, and along with Chapter 12 on key establishment protocols, it is hard to find consolidated treatments of these now-mainstream topics. Key management techniques as presented in Chapter 13 have traditionally not been given much attention by cryptographers, but are of great importance in practice. A focused treatment of cryptographic patents and a concise summary of cryptographic standards, as presented in Chapter 15, are also long overdue.

In most cases (with some historical exceptions), where algorithms are known to be insecure, we have chosen to leave out specification of their details, because most such techniques are of little practical interest. Essentially all of the algorithms included have been verified for correctness by independent implementation, confirming the test vectors specified.

Acknowledgements

This project would not have been possible without the tremendous efforts put forth by our peers who have taken the time to read endless drafts and provide us with technical corrections, constructive feedback, and countless suggestions. In particular, the advice of our Advisory Editors has been invaluable, and it is impossible to attribute individual credit for their many suggestions throughout this book. Among our Advisory Editors, we would particularly like to thank:

Mihir Bellare	Don Coppersmith	Dorothy Denning	Walter Fumy
Burt Kaliski	Peter Landrock	Arjen Lenstra	Ueli Maurer
Chris Mitchell	Tatsuaki Okamoto	Bart Preneel	Ron Rivest
Gus Simmons	Miles Smid	Jacques Stern	Mike Wiener
Yacov Yacobi			

In addition, we gratefully acknowledge the exceptionally large number of additional individuals who have helped improve the quality of this volume, by providing highly appreciated feedback and guidance on various matters. These individuals include:

Carlisle Adams	Rich Ankney	Tom Berson
Simon Blackburn	Ian Blake	Antoon Bosselaers
Colin Boyd	Jørgen Brandt	Mike Burmester
Ed Dawson	Peter de Rooij	Yvo Desmedt
Whit Diffie	Hans Dobbertin	Carl Ellison
Luis Encinas	Warwick Ford	Amparo Fuster
Shuhong Gao	Will Gilbert	Marc Girault
Jovan Golić	Dieter Gollmann	Li Gong

Carrie Grant
Darrel Hankerson
Mike Just
Neal Koblitz
Evangelos Kranakis
Xuejia Lai
S. Mike Matyas
Peter Montgomery
Volker Müller
Kaisa Nyberg
Walter Penzhorn
Leon Pintsov
Matt Robshaw
Rainer Rueppel
Jeff Shallit
Andrea Vanstone
Jerry Veeh
Robert Zuccherato
Blake Greenlee
Anwar Hasan
Andy Klapper
Çetin Koç
David Kravitz
Charles Lam
Willi Meier
Mike Mosca
David Naccache
Andrew Odlyzko
Birgit Pfitzmann
Fred Piper
Peter Rodney
Mahmoud Salmasizadeh
Jon Sorenson
Serge Vaudenay
Fausto Vitini
Helen Gustafson
Don Johnson
Lars Knudsen
Judy Koeller
Hugo Krawczyk
Alan Ling
Serge Mister
Tim Moses
James Nechvatal
Richard Outerbridge
Kevin Phelps
Carl Pomerance
Phil Rogaway
Roger Schlafly
Doug Stinson
Klaus Vedder
Lisa Yin

We apologize to those whose names have inadvertently escaped this list. Special thanks are due to Carrie Grant, Darrel Hankerson, Judy Koeller, Charles Lam, and Andrea Vanstone. Their hard work contributed greatly to the quality of this book, and it was truly a pleasure working with them. Thanks also to the folks at CRC Press, including Tia Atchison, Gary Bennett, Susie Carlisle, Nora Konopka, Mary Kugler, Amy Morrell, Tim Pletscher, Bob Stern, and Wayne Yuhasz. The second author would like to thank his colleagues past and present at Nortel Secure Networks (Bell-Northern Research), many of whom are mentioned above, for their contributions on this project, and in particular Brian O'Higgins for his encouragement and support; all views expressed, however, are entirely that of the author. The third author would also like to acknowledge the support of the Natural Sciences and Engineering Research Council.

Any errors that remain are, of course, entirely our own. We would be grateful if readers who spot errors, missing references or credits, or incorrectly attributed results would contact us with details. It is our hope that this volume facilitates further advancement of the field, and that we have helped play a small part in this.

Alfred J. Menezes
Paul C. van Oorschot
Scott A. Vanstone

Preface to the 5th printing

The 5th printing includes corrections to all the editorial and technical errors that we are aware of as of June 2001. We thank everyone for the tremendous reception they have given to our book, and for those who have taken the time to draw errors to our attention.

Alfred J. Menezes
Paul C. van Oorschot
Scott A. Vanstone
June 2001

Chapter 1

Overview of Cryptography

Contents in Brief

1.1 Introduction

Cryptography has a long and fascinating history. The most complete non-technical account of the subject is Kahn's *The Codebreakers*. This book traces cryptography from its initial and limited use by the Egyptians some 4000 years ago, to the twentieth century where it played a crucial role in the outcome of both world wars. Completed in 1963, Kahn's book covers those aspects of the history which were most significant (up to that time) to the development of the subject. The predominant practitioners of the art were those associated with the military, the diplomatic service and government in general. Cryptography was used as a tool to protect national secrets and strategies.

The proliferation of computers and communications systems in the 1960s brought with it a demand from the private sector for means to protect information in digital form and to provide security services. Beginning with the work of Feistel at IBM in the early 1970s and culminating in 1977 with the adoption as a U.S. Federal Information Processing Standard for encrypting unclassified information, DES, the Data Encryption Standard, is the most well-known cryptographic mechanism in history. It remains the standard means for securing electronic commerce for many financial institutions around the world.

The most striking development in the history of cryptography came in 1976 when Diffie and Hellman published *New Directions in Cryptography*. This paper introduced the revolutionary concept of public-key cryptography and also provided a new and ingenious method

for key exchange, the security of which is based on the intractability of the discrete logarithm problem. Although the authors had no practical realization of a public-key encryption scheme at the time, the idea was clear and it generated extensive interest and activity in the cryptographic community. In 1978 Rivest, Shamir, and Adleman discovered the first practical public-key encryption and signature scheme, now referred to as RSA. The RSA scheme is based on another hard mathematical problem, the intractability of factoring large integers. This application of a hard mathematical problem to cryptography revitalized efforts to find more efficient methods to factor. The 1980s saw major advances in this area but none which rendered the RSA system insecure. Another class of powerful and practical public-key schemes was found by ElGamal in 1985. These are also based on the discrete logarithm problem.

One of the most significant contributions provided by public-key cryptography is the digital signature. In 1991 the first international standard for digital signatures (ISO/IEC 9796) was adopted. It is based on the RSA public-key scheme. In 1994 the U.S. Government adopted the Digital Signature Standard, a mechanism based on the ElGamal public-key scheme.

The search for new public-key schemes, improvements to existing cryptographic mechanisms, and proofs of security continues at a rapid pace. Various standards and infrastructures involving cryptography are being put in place. Security products are being developed to address the security needs of an information intensive society.

The purpose of this book is to give an up-to-date treatise of the principles, techniques, and algorithms of interest in cryptographic practice. Emphasis has been placed on those aspects which are most practical and applied. The reader will be made aware of the basic issues and pointed to specific related research in the literature where more indepth discussions can be found. Due to the volume of material which is covered, most results will be stated without proofs. This also serves the purpose of not obscuring the very applied nature of the subject. This book is intended for both implementers and researchers. It describes algorithms, systems, and their interactions.

Chapter 1 is a tutorial on the many and various aspects of cryptography. It does not attempt to convey all of the details and subtleties inherent to the subject. Its purpose is to introduce the basic issues and principles and to point the reader to appropriate chapters in the book for more comprehensive treatments. Specific techniques are avoided in this chapter.

1.2 Information security and cryptography

The concept of *information* will be taken to be an understood quantity. To introduce cryptography, an understanding of issues related to information security in general is necessary. Information security manifests itself in many ways according to the situation and requirement. Regardless of who is involved, to one degree or another, all parties to a transaction must have confidence that certain objectives associated with information security have been met. Some of these objectives are listed in Table 1.1.

Over the centuries, an elaborate set of protocols and mechanisms has been created to deal with information security issues when the information is conveyed by physical documents. Often the objectives of information security cannot solely be achieved through mathematical algorithms and protocols alone, but require procedural techniques and abidance of laws to achieve the desired result. For example, privacy of letters is provided by sealed envelopes delivered by an accepted mail service. The physical security of the envelope is, for practical necessity, limited and so laws are enacted which make it a criminal

privacy or confidentiality	keeping information secret from all but those who are authorized to see it.
data integrity	ensuring information has not been altered by unauthorized or unknown means.
entity authentication or identification	corroboration of the identity of an entity (e.g., a person, a computer terminal, a credit card, etc.).
message authentication	corroborating the source of information; also known as data origin authentication.
signature	a means to bind information to an entity.
authorization	conveyance, to another entity, of official sanction to do or be something.
validation	a means to provide timeliness of authorization to use or manipulate information or resources.
access control	restricting access to resources to privileged entities.
certification	endorsement of information by a trusted entity.
timestamping	recording the time of creation or existence of information.
witnessing	verifying the creation or existence of information by an entity other than the creator.
receipt	acknowledgement that information has been received.
confirmation	acknowledgement that services have been provided.
ownership	a means to provide an entity with the legal right to use or transfer a resource to others.
anonymity	concealing the identity of an entity involved in some process.
non-repudiation	preventing the denial of previous commitments or actions.
revocation	retraction of certification or authorization.

Table 1.1: *Some information security objectives.*

offense to open mail for which one is not authorized. It is sometimes the case that security is achieved not through the information itself but through the physical document recording it. For example, paper currency requires special inks and material to prevent counterfeiting.

Conceptually, the way information is recorded has not changed dramatically over time. Whereas information was typically stored and transmitted on paper, much of it now resides on magnetic media and is transmitted via telecommunications systems, some wireless. What has changed dramatically is the ability to copy and alter information. One can make thousands of identical copies of a piece of information stored electronically and each is indistinguishable from the original. With information on paper, this is much more difficult. What is needed then for a society where information is mostly stored and transmitted in electronic form is a means to ensure information security which is independent of the physical medium recording or conveying it and such that the objectives of information security rely solely on digital information itself.

One of the fundamental tools used in information security is the signature. It is a building block for many other services such as non-repudiation, data origin authentication, identification, and witnessing, to mention a few. Having learned the basics in writing, an individual is taught how to produce a handwritten signature for the purpose of identification. At contract age the signature evolves to take on a very integral part of the person's identity. This signature is intended to be unique to the individual and serve as a means to identify, authorize, and validate. With electronic information the concept of a signature needs to be

redressed; it cannot simply be something unique to the signer and independent of the information signed. Electronic replication of it is so simple that appending a signature to a document not signed by the originator of the signature is almost a triviality.

Analogues of the "paper protocols" currently in use are required. Hopefully these new electronic based protocols are at least as good as those they replace. There is a unique opportunity for society to introduce new and more efficient ways of ensuring information security. Much can be learned from the evolution of the paper based system, mimicking those aspects which have served us well and removing the inefficiencies.

Achieving information security in an electronic society requires a vast array of technical and legal skills. There is, however, no guarantee that all of the information security objectives deemed necessary can be adequately met. The technical means is provided through cryptography.

1.1 Definition *Cryptography* is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication.

Cryptography is not the only means of providing information security, but rather one set of techniques.

Cryptographic goals

Of all the information security objectives listed in Table 1.1, the following four form a framework upon which the others will be derived: (1) privacy or confidentiality (§1.5, §1.8); (2) data integrity (§1.9); (3) authentication (§1.7); and (4) non-repudiation (§1.6).

1. *Confidentiality* is a service used to keep the content of information from all but those authorized to have it. *Secrecy* is a term synonymous with confidentiality and privacy. There are numerous approaches to providing confidentiality, ranging from physical protection to mathematical algorithms which render data unintelligible.
2. *Data integrity* is a service which addresses the unauthorized alteration of data. To assure data integrity, one must have the ability to detect data manipulation by unauthorized parties. Data manipulation includes such things as insertion, deletion, and substitution.
3. *Authentication* is a service related to identification. This function applies to both entities and information itself. Two parties entering into a communication should identify each other. Information delivered over a channel should be authenticated as to origin, date of origin, data content, time sent, etc. For these reasons this aspect of cryptography is usually subdivided into two major classes: *entity authentication* and *data origin authentication*. Data origin authentication implicitly provides data integrity (for if a message is modified, the source has changed).
4. *Non-repudiation* is a service which prevents an entity from denying previous commitments or actions. When disputes arise due to an entity denying that certain actions were taken, a means to resolve the situation is necessary. For example, one entity may authorize the purchase of property by another entity and later deny such authorization was granted. A procedure involving a trusted third party is needed to resolve the dispute.

A fundamental goal of cryptography is to adequately address these four areas in both theory and practice. Cryptography is about the prevention and detection of cheating and other malicious activities.

This book describes a number of basic *cryptographic tools* (*primitives*) used to provide information security. Examples of primitives include encryption schemes (§1.5 and §1.8),

hash functions (§1.9), and digital signature schemes (§1.6). Figure 1.1 provides a schematic listing of the primitives considered and how they relate. Many of these will be briefly introduced in this chapter, with detailed discussion left to later chapters. These primitives should

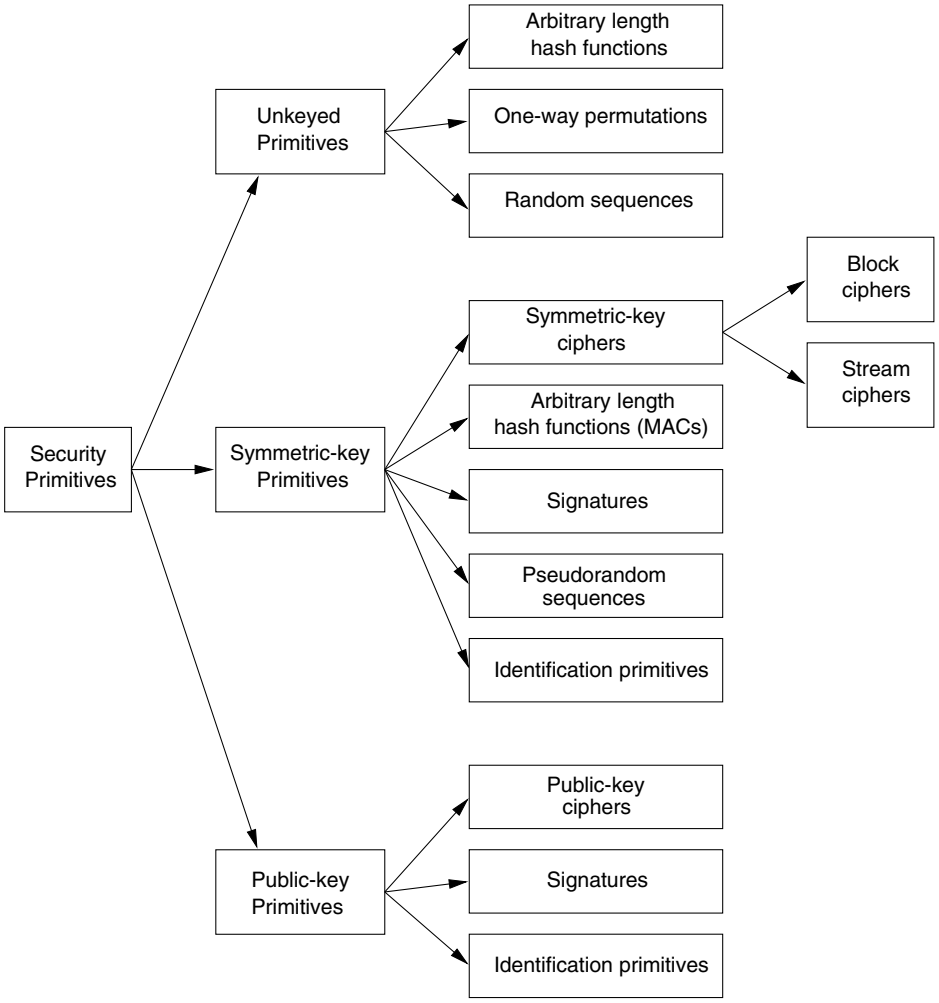


Figure 1.1: *A taxonomy of cryptographic primitives.*

be evaluated with respect to various criteria such as:

1. *level of security.* This is usually difficult to quantify. Often it is given in terms of the number of operations required (using the best methods currently known) to defeat the intended objective. Typically the level of security is defined by an upper bound on the amount of work necessary to defeat the objective. This is sometimes called the work factor (see §1.13.4).
2. *functionality.* Primitives will need to be combined to meet various information security objectives. Which primitives are most effective for a given objective will be determined by the basic properties of the primitives.
3. *methods of operation.* Primitives, when applied in various ways and with various inputs, will typically exhibit different characteristics; thus, one primitive could provide

very different functionality depending on its mode of operation or usage.

4. *performance*. This refers to the efficiency of a primitive in a particular mode of operation. (For example, an encryption algorithm may be rated by the number of bits per second which it can encrypt.)
5. *ease of implementation*. This refers to the difficulty of realizing the primitive in a practical instantiation. This might include the complexity of implementing the primitive in either a software or hardware environment.

The relative importance of various criteria is very much dependent on the application and resources available. For example, in an environment where computing power is limited one may have to trade off a very high level of security for better performance of the system as a whole.

Cryptography, over the ages, has been an art practised by many who have devised ad hoc techniques to meet some of the information security requirements. The last twenty years have been a period of transition as the discipline moved from an art to a science. There are now several international scientific conferences devoted exclusively to cryptography and also an international scientific organization, the International Association for Cryptologic Research (IACR), aimed at fostering research in the area.

This book is about cryptography: the theory, the practice, and the standards.

1.3 Background on functions

While this book is not a treatise on abstract mathematics, a familiarity with basic mathematical concepts will prove to be useful. One concept which is absolutely fundamental to cryptography is that of a *function* in the mathematical sense. A function is alternately referred to as a *mapping* or a *transformation*.

1.3.1 Functions (1-1, one-way, trapdoor one-way)

A *set* consists of distinct objects which are called *elements* of the set. For example, a set X might consist of the elements a, b, c, and this is denoted $X = \{a, b, c\}$.

1.2 Definition A *function* is defined by two sets X and Y and a *rule* f which assigns to each element in X precisely one element in Y. The set X is called the *domain* of the function and Y the *codomain*. If x is an element of X (usually written $x \in X$) the *image* of x is the element in Y which the rule f associates with x; the image y of x is denoted by $y = f(x)$. Standard notation for a function f from set X to set Y is $f\colon X \longrightarrow Y$. If $y \in Y$, then a *preimage* of y is an element $x \in X$ for which $f(x) = y$. The set of all elements in Y which have at least one preimage is called the *image* of f, denoted $\mathrm{Im}(f)$.

1.3 Example (*function*) Consider the sets $X = \{a, b, c\}$, $Y = \{1, 2, 3, 4\}$, and the rule f from X to Y defined as $f(a) = 2$, $f(b) = 4$, $f(c) = 1$. Figure 1.2 shows a schematic of the sets X, Y and the function f. The preimage of the element 2 is a. The image of f is $\{1, 2, 4\}$. □

Thinking of a function in terms of the schematic (sometimes called a *functional diagram*) given in Figure 1.2, each element in the domain X has precisely one arrowed line originating from it. Each element in the codomain Y can have any number of arrowed lines incident to it (including zero lines).

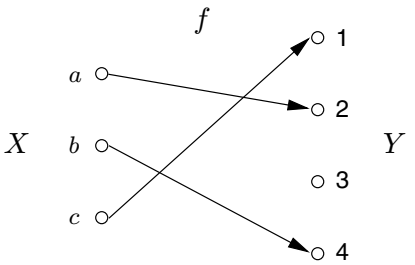


Figure 1.2: *A function f from a set X of three elements to a set Y of four elements.*

Often only the domain X and the rule f are given and the codomain is assumed to be the image of f. This point is illustrated with two examples.

1.4 Example (*function*) Take $X = \{1, 2, 3, \ldots, 10\}$ and let f be the rule that for each $x \in X$, $f(x) = r_x$, where r_x is the remainder when x^2 is divided by 11. Explicitly then

$$\begin{array}{lllll} f(1) = 1 & f(2) = 4 & f(3) = 9 & f(4) = 5 & f(5) = 3 \\ f(6) = 3 & f(7) = 5 & f(8) = 9 & f(9) = 4 & f(10) = 1. \end{array}$$

The image of f is the set $Y = \{1, 3, 4, 5, 9\}$. □

1.5 Example (*function*) Take $X = \{1, 2, 3, \ldots, 10^{50}\}$ and let f be the rule $f(x) = r_x$, where r_x is the remainder when x^2 is divided by $10^{50} + 1$ for all $x \in X$. Here it is not feasible to write down f explicitly as in Example 1.4, but nonetheless the function is completely specified by the domain and the mathematical description of the rule f. □

(i) 1-1 functions

1.6 Definition A function (or transformation) is $1-1$ *(one-to-one)* if each element in the codomain Y is the image of at most one element in the domain X.

1.7 Definition A function (or transformation) is *onto* if each element in the codomain Y is the image of at least one element in the domain. Equivalently, a function $f\colon X \longrightarrow Y$ is onto if $\mathrm{Im}(f) = Y$.

1.8 Definition If a function $f\colon X \longrightarrow Y$ is $1-1$ and $\mathrm{Im}(f) = Y$, then f is called a *bijection*.

1.9 Fact If $f\colon X \longrightarrow Y$ is $1-1$ then $f\colon X \longrightarrow \mathrm{Im}(f)$ is a bijection. In particular, if $f\colon X \longrightarrow Y$ is $1-1$, and X and Y are finite sets of the same size, then f is a bijection.

In terms of the schematic representation, if f is a bijection, then each element in Y has exactly one arrowed line incident with it. The functions described in Examples 1.3 and 1.4 are not bijections. In Example 1.3 the element 3 is not the image of any element in the domain. In Example 1.4 each element in the codomain has two preimages.

1.10 Definition If f is a bijection from X to Y then it is a simple matter to define a bijection g from Y to X as follows: for each $y \in Y$ define $g(y) = x$ where $x \in X$ and $f(x) = y$. This function g obtained from f is called the *inverse function* of f and is denoted by $g = f^{-1}$.

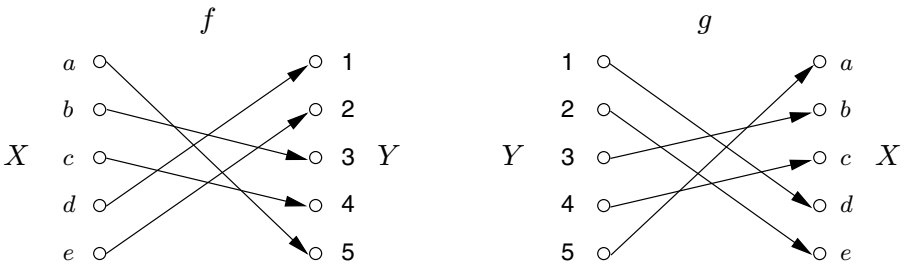


Figure 1.3: *A bijection f and its inverse $g = f^{-1}$.*

1.11 Example (*inverse function*) Let $X = \{a, b, c, d, e\}$, and $Y = \{1, 2, 3, 4, 5\}$, and consider the rule f given by the arrowed edges in Figure 1.3. f is a bijection and its inverse g is formed simply by reversing the arrows on the edges. The domain of g is Y and the codomain is X. □

Note that if f is a bijection, then so is f^{-1}. In cryptography bijections are used as the tool for encrypting messages and the inverse transformations are used to decrypt. This will be made clearer in §1.4 when some basic terminology is introduced. Notice that if the transformations were not bijections then it would not be possible to always decrypt to a unique message.

(ii) One-way functions

There are certain types of functions which play significant roles in cryptography. At the expense of rigor, an intuitive definition of a one-way function is given.

1.12 Definition A function f from a set X to a set Y is called a *one-way function* if $f(x)$ is "easy" to compute for all $x \in X$ but for "essentially all" elements $y \in \mathrm{Im}(f)$ it is "computationally infeasible" to find any $x \in X$ such that $f(x) = y$.

1.13 Note (*clarification of terms in Definition 1.12*)

(i) A rigorous definition of the terms "easy" and "computationally infeasible" is necessary but would detract from the simple idea that is being conveyed. For the purpose of this chapter, the intuitive meaning will suffice.

(ii) The phrase "for essentially all elements in Y" refers to the fact that there are a few values $y \in Y$ for which it is easy to find an $x \in X$ such that $y = f(x)$. For example, one may compute $y = f(x)$ for a small number of x values and then for these, the inverse is known by table look-up. An alternate way to describe this property of a one-way function is the following: for a random $y \in \mathrm{Im}(f)$ it is computationally infeasible to find any $x \in X$ such that $f(x) = y$.

The concept of a one-way function is illustrated through the following examples.

1.14 Example (*one-way function*) Take $X = \{1, 2, 3, \ldots, 16\}$ and define $f(x) = r_x$ for all $x \in X$ where r_x is the remainder when 3^x is divided by 17. Explicitly,

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$f(x)$	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1

Given a number between 1 and 16, it is relatively easy to find the image of it under f. However, given a number such as 7, without having the table in front of you, it is harder to find

x given that $f(x) = 7$. Of course, if the number you are given is 3 then it is clear that $x = 1$ is what you need; but for most of the elements in the codomain it is not that easy. □

One must keep in mind that this is an example which uses very small numbers; the important point here is that there is a difference in the amount of work to compute $f(x)$ and the amount of work to find x given $f(x)$. Even for very large numbers, $f(x)$ can be computed efficiently using the repeated square-and-multiply algorithm (Algorithm 2.143), whereas the process of finding x from $f(x)$ is much harder.

1.15 Example (*one-way function*) A *prime number* is a positive integer greater than 1 whose only positive integer divisors are 1 and itself. Select primes $p = 48611$, $q = 53993$, form $n = pq = 2624653723$, and let $X = \{1, 2, 3, \ldots, n-1\}$. Define a function f on X by $f(x) = r_x$ for each $x \in X$, where r_x is the remainder when x^3 is divided by n. For instance, $f(2489991) = 1981394214$ since $2489991^3 = 5881949859 \cdot n + 1981394214$. Computing $f(x)$ is a relatively simple thing to do, but to reverse the procedure is much more difficult; that is, given a remainder to find the value x which was originally cubed (raised to the third power). This procedure is referred to as the computation of a modular cube root with modulus n. If the factors of n are unknown and large, this is a difficult problem; however, if the factors p and q of n are known then there is an efficient algorithm for computing modular cube roots. (See §8.2.2(i) for details.) □

Example 1.15 leads one to consider another type of function which will prove to be fundamental in later developments.

(iii) Trapdoor one-way functions

1.16 Definition A *trapdoor one-way function* is a one-way function $f\colon X \longrightarrow Y$ with the additional property that given some extra information (called the *trapdoor information*) it becomes feasible to find for any given $y \in \mathrm{Im}(f)$, an $x \in X$ such that $f(x) = y$.

Example 1.15 illustrates the concept of a trapdoor one-way function. With the additional information of the factors of $n = 2624653723$ (namely, $p = 48611$ and $q = 53993$, each of which is five decimal digits long) it becomes much easier to invert the function. The factors of 2624653723 are large enough that finding them by hand computation would be difficult. Of course, any reasonable computer program could find the factors relatively quickly. If, on the other hand, one selects p and q to be very large distinct prime numbers (each having about 100 decimal digits) then, by today's standards, it is a difficult problem, even with the most powerful computers, to deduce p and q simply from n. This is the well-known *integer factorization problem* (see §3.2) and a source of many trapdoor one-way functions.

It remains to be rigorously established whether there actually are any (true) one-way functions. That is to say, no one has yet definitively proved the existence of such functions under reasonable (and rigorous) definitions of "easy" and "computationally infeasible". Since the existence of one-way functions is still unknown, the existence of trapdoor one-way functions is also unknown. However, there are a number of good candidates for one-way and trapdoor one-way functions. Many of these are discussed in this book, with emphasis given to those which are practical.

One-way and trapdoor one-way functions are the basis for public-key cryptography (discussed in §1.8). The importance of these concepts will become clearer when their application to cryptographic techniques is considered. It will be worthwhile to keep the abstract concepts of this section in mind as concrete methods are presented.

1.3.2 Permutations

Permutations are functions which are often used in various cryptographic constructs.

1.17 Definition Let $\mathcal{S}$ be a finite set of elements. A *permutation* p on $\mathcal{S}$ is a bijection (Definition 1.8) from $\mathcal{S}$ to itself (i.e., $p\colon \mathcal{S} \longrightarrow \mathcal{S}$).

1.18 Example (*permutation*) Let $\mathcal{S} = \{1, 2, 3, 4, 5\}$. A permutation $p\colon \mathcal{S} \longrightarrow \mathcal{S}$ is defined as follows:

$$p(1) = 3,\ p(2) = 5,\ p(3) = 4,\ p(4) = 2,\ p(5) = 1.$$

A permutation can be described in various ways. It can be displayed as above or as an array:

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix}, \tag{1.1}$$

where the top row in the array is the domain and the bottom row is the image under the mapping p. Of course, other representations are possible. □

Since permutations are bijections, they have inverses. If a permutation is written as an array (see 1.1), its inverse is easily found by interchanging the rows in the array and reordering the elements in the new top row if desired (the bottom row would have to be reordered correspondingly). The inverse of p in Example 1.18 is $p^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 3 & 2 \end{pmatrix}$.

1.19 Example (*permutation*) Let X be the set of integers $\{0, 1, 2, \ldots, pq - 1\}$ where p and q are distinct *large* primes (for example, p and q are each about 100 decimal digits long), and suppose that neither $p-1$ nor $q-1$ is divisible by 3. Then the function $p(x) = r_x$, where r_x is the remainder when x^3 is divided by pq, can be shown to be a permutation. Determining the inverse permutation is computationally infeasible by today's standards unless p and q are known (cf. Example 1.15). □

1.3.3 Involutions

Another type of function which will be referred to in §1.5.3 is an involution. Involutions have the property that they are their own inverses.

1.20 Definition Let $\mathcal{S}$ be a finite set and let f be a bijection from $\mathcal{S}$ to $\mathcal{S}$ (i.e., $f\colon \mathcal{S} \longrightarrow \mathcal{S}$). The function f is called an *involution* if $f = f^{-1}$. An equivalent way of stating this is $f(f(x)) = x$ for all $x \in \mathcal{S}$.

1.21 Example (*involution*) Figure 1.4 is an example of an involution. In the diagram of an involution, note that if j is the image of i then i is the image of j. □

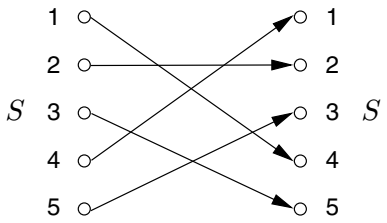


Figure 1.4: *An involution on a set S of 5 elements.*

1.4 Basic terminology and concepts

The scientific study of any discipline must be built upon rigorous definitions arising from fundamental concepts. What follows is a list of terms and basic concepts used throughout this book. Where appropriate, rigor has been sacrificed (here in Chapter 1) for the sake of clarity.

Encryption domains and codomains

- $\mathcal{A}$ denotes a finite set called the *alphabet of definition*. For example, $\mathcal{A} = \{0, 1\}$, the *binary alphabet*, is a frequently used alphabet of definition. Note that any alphabet can be encoded in terms of the binary alphabet. For example, since there are 32 binary strings of length five, each letter of the English alphabet can be assigned a unique binary string of length five.
- $\mathcal{M}$ denotes a set called the *message space*. $\mathcal{M}$ consists of strings of symbols from an alphabet of definition. An element of $\mathcal{M}$ is called a *plaintext message* or simply a *plaintext*. For example, $\mathcal{M}$ may consist of binary strings, English text, computer code, etc.
- $\mathcal{C}$ denotes a set called the *ciphertext space*. $\mathcal{C}$ consists of strings of symbols from an alphabet of definition, which may differ from the alphabet of definition for $\mathcal{M}$. An element of $\mathcal{C}$ is called a *ciphertext*.

Encryption and decryption transformations

- $\mathcal{K}$ denotes a set called the *key space*. An element of $\mathcal{K}$ is called a *key*.
- Each element $e \in \mathcal{K}$ uniquely determines a bijection from $\mathcal{M}$ to $\mathcal{C}$, denoted by E_e. E_e is called an *encryption function* or an *encryption transformation*. Note that E_e must be a bijection if the process is to be reversed and a unique plaintext message recovered for each distinct ciphertext.[1]
- For each $d \in \mathcal{K}$, D_d denotes a bijection from $\mathcal{C}$ to $\mathcal{M}$ (i.e., $D_d \colon \mathcal{C} \longrightarrow \mathcal{M}$). D_d is called a *decryption function* or *decryption transformation*.
- The process of applying the transformation E_e to a message $m \in \mathcal{M}$ is usually referred to as *encrypting* m or the *encryption* of m.
- The process of applying the transformation D_d to a ciphertext c is usually referred to as *decrypting* c or the *decryption* of c.

[1] More generality is obtained if E_e is simply defined as a $1 - 1$ transformation from $\mathcal{M}$ to $\mathcal{C}$. That is to say, E_e is a bijection from $\mathcal{M}$ to $\mathrm{Im}(E_e)$ where $\mathrm{Im}(E_e)$ is a subset of $\mathcal{C}$.

- An *encryption scheme* consists of a set $\{E_e : e \in \mathcal{K}\}$ of encryption transformations and a corresponding set $\{D_d : d \in \mathcal{K}\}$ of decryption transformations with the property that for each $e \in \mathcal{K}$ there is a unique key $d \in \mathcal{K}$ such that $D_d = E_e^{-1}$; that is, $D_d(E_e(m)) = m$ for all $m \in \mathcal{M}$. An encryption scheme is sometimes referred to as a *cipher*.
- The keys e and d in the preceding definition are referred to as a *key pair* and sometimes denoted by (e, d). Note that e and d could be the same.
- To *construct* an encryption scheme requires one to select a message space $\mathcal{M}$, a ciphertext space $\mathcal{C}$, a key space $\mathcal{K}$, a set of encryption transformations $\{E_e : e \in \mathcal{K}\}$, and a corresponding set of decryption transformations $\{D_d : d \in \mathcal{K}\}$.

Achieving confidentiality

An encryption scheme may be used as follows for the purpose of achieving confidentiality. Two parties Alice and Bob first secretly choose or secretly exchange a key pair (e, d). At a subsequent point in time, if Alice wishes to send a message $m \in \mathcal{M}$ to Bob, she computes $c = E_e(m)$ and transmits this to Bob. Upon receiving c, Bob computes $D_d(c) = m$ and hence recovers the original message m.

The question arises as to why keys are necessary. (Why not just choose one encryption function and its corresponding decryption function?) Having transformations which are very similar but characterized by keys means that if some particular encryption/decryption transformation is revealed then one does not have to redesign the entire scheme but simply change the key. It is sound cryptographic practice to change the key (encryption/decryption transformation) frequently. As a physical analogue, consider an ordinary resettable combination lock. The structure of the lock is available to anyone who wishes to purchase one but the combination is chosen and set by the owner. If the owner suspects that the combination has been revealed he can easily reset it without replacing the physical mechanism.

1.22 Example (*encryption scheme*) Let $\mathcal{M} = \{m_1, m_2, m_3\}$ and $\mathcal{C} = \{c_1, c_2, c_3\}$. There are precisely $3! = 6$ bijections from $\mathcal{M}$ to $\mathcal{C}$. The key space $\mathcal{K} = \{1, 2, 3, 4, 5, 6\}$ has six elements in it, each specifying one of the transformations. Figure 1.5 illustrates the six encryption functions which are denoted by $E_i, 1 \leq i \leq 6$. Alice and Bob agree on a trans-

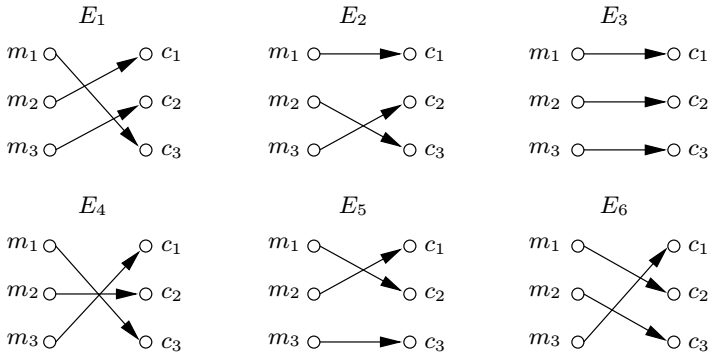


Figure 1.5: *Schematic of a simple encryption scheme.*

formation, say E_1. To encrypt the message m_1, Alice computes $E_1(m_1) = c_3$ and sends c_3 to Bob. Bob decrypts c_3 by reversing the arrows on the diagram for E_1 and observing that c_3 points to m_1.

When $\mathcal{M}$ is a small set, the functional diagram is a simple visual means to describe the mapping. In cryptography, the set $\mathcal{M}$ is typically of astronomical proportions and, as such, the visual description is infeasible. What is required, in these cases, is some other simple means to describe the encryption and decryption transformations, such as mathematical algorithms. □

Figure 1.6 provides a simple model of a two-party communication using encryption.

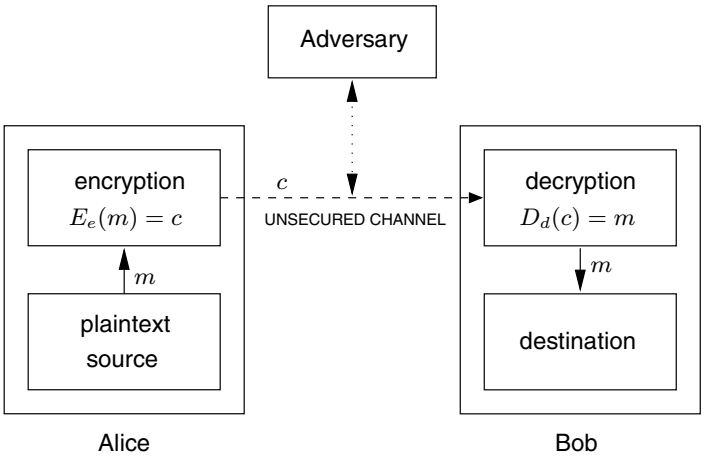


Figure 1.6: *Schematic of a two-party communication using encryption.*

Communication participants

Referring to Figure 1.6, the following terminology is defined.

- An *entity* or *party* is someone or something which sends, receives, or manipulates information. Alice and Bob are entities in Example 1.22. An entity may be a person, a computer terminal, etc.
- A *sender* is an entity in a two-party communication which is the legitimate transmitter of information. In Figure 1.6, the sender is Alice.
- A *receiver* is an entity in a two-party communication which is the intended recipient of information. In Figure 1.6, the receiver is Bob.
- An *adversary* is an entity in a two-party communication which is neither the sender nor receiver, and which tries to defeat the information security service being provided between the sender and receiver. Various other names are synonymous with adversary such as enemy, attacker, opponent, tapper, eavesdropper, intruder, and interloper. An adversary will often attempt to play the role of either the legitimate sender or the legitimate receiver.

Channels

- A *channel* is a means of conveying information from one entity to another.
- A *physically secure channel* or *secure channel* is one which is not physically accessible to the adversary.
- An *unsecured channel* is one from which parties other than those for which the information is intended can reorder, delete, insert, or read.
- A *secured channel* is one from which an adversary does not have the ability to reorder, delete, insert, or read.

One should note the subtle difference between a physically secure channel and a secured channel – a secured channel may be secured by physical or cryptographic techniques, the latter being the topic of this book. Certain channels are assumed to be physically secure. These include trusted couriers, personal contact between communicating parties, and a dedicated communication link, to name a few.

Security

A fundamental premise in cryptography is that the sets $\mathcal{M}, \mathcal{C}, \mathcal{K}, \{E_e : e \in \mathcal{K}\}, \{D_d : d \in \mathcal{K}\}$ are public knowledge. When two parties wish to communicate securely using an encryption scheme, the only thing that they keep secret is the particular key pair (e, d) which they are using, and which they must select. One can gain additional security by keeping the class of encryption and decryption transformations secret but one should not base the security of the entire scheme on this approach. History has shown that maintaining the secrecy of the transformations is very difficult indeed.

1.23 Definition An encryption scheme is said to be *breakable* if a third party, without prior knowledge of the key pair (e, d), can systematically recover plaintext from corresponding ciphertext within some appropriate time frame.

An appropriate time frame will be a function of the useful lifespan of the data being protected. For example, an instruction to buy a certain stock may only need to be kept secret for a few minutes whereas state secrets may need to remain confidential indefinitely.

An encryption scheme can be broken by trying all possible keys to see which one the communicating parties are using (assuming that the class of encryption functions is public knowledge). This is called an *exhaustive search* of the key space. It follows then that the number of keys (i.e., the size of the key space) should be large enough to make this approach computationally infeasible. It is the objective of a designer of an encryption scheme that this be the best approach to break the system.

Frequently cited in the literature are *Kerckhoffs' desiderata*, a set of requirements for cipher systems. They are given here essentially as Kerckhoffs originally stated them:

1. the system should be, if not theoretically unbreakable, unbreakable in practice;
2. compromise of the system details should not inconvenience the correspondents;
3. the key should be rememberable without notes and easily changed;
4. the cryptogram should be transmissible by telegraph;
5. the encryption apparatus should be portable and operable by a single person; and
6. the system should be easy, requiring neither the knowledge of a long list of rules nor mental strain.

This list of requirements was articulated in 1883 and, for the most part, remains useful today. Point 2 allows that the class of encryption transformations being used be publicly known and that the security of the system should reside only in the key chosen.

Information security in general

So far the terminology has been restricted to encryption and decryption with the goal of privacy in mind. Information security is much broader, encompassing such things as authentication and data integrity. A few more general definitions, pertinent to discussions later in the book, are given next.

- An *information security service* is a method to provide some specific aspect of security. For example, integrity of transmitted data is a security objective, and a method to ensure this aspect is an information security service.

- *Breaking* an information security service (which often involves more than simply encryption) implies defeating the objective of the intended service.
- A *passive adversary* is an adversary who is capable only of reading information from an unsecured channel.
- An *active adversary* is an adversary who may also transmit, alter, or delete information on an unsecured channel.

Cryptology

- *Cryptanalysis* is the study of mathematical techniques for attempting to defeat cryptographic techniques, and, more generally, information security services.
- A *cryptanalyst* is someone who engages in cryptanalysis.
- *Cryptology* is the study of cryptography (Definition 1.1) and cryptanalysis.
- A *cryptosystem* is a general term referring to a set of cryptographic primitives used to provide information security services. Most often the term is used in conjunction with primitives providing confidentiality, i.e., encryption.

Cryptographic techniques are typically divided into two generic types: *symmetric-key* and *public-key*. Encryption methods of these types will be discussed separately in §1.5 and §1.8. Other definitions and terminology will be introduced as required.

1.5 Symmetric-key encryption

§1.5 considers symmetric-key encryption. Public-key encryption is the topic of §1.8.

1.5.1 Overview of block ciphers and stream ciphers

1.24 Definition Consider an encryption scheme consisting of the sets of encryption and decryption transformations $\{E_e : e \in \mathcal{K}\}$ and $\{D_d : d \in \mathcal{K}\}$, respectively, where $\mathcal{K}$ is the key space. The encryption scheme is said to be *symmetric-key* if for each associated encryption/decryption key pair (e, d), it is computationally "easy" to determine d knowing only e, and to determine e from d.

Since $e = d$ in most practical symmetric-key encryption schemes, the term symmetric-key becomes appropriate. Other terms used in the literature are *single-key*, *one-key*, *private-key*,[2] and *conventional* encryption. Example 1.25 illustrates the idea of symmetric-key encryption.

1.25 Example (*symmetric-key encryption*) Let $\mathcal{A} = \{\mathrm{A}, \mathrm{B}, \mathrm{C}, \ldots, \mathrm{X}, \mathrm{Y}, \mathrm{Z}\}$ be the English alphabet. Let $\mathcal{M}$ and $\mathcal{C}$ be the set of all strings of length five over $\mathcal{A}$. The key e is chosen to be a permutation on $\mathcal{A}$. To encrypt, an English message is broken up into groups each having five letters (with appropriate padding if the length of the message is not a multiple of five) and a permutation e is applied to each letter one at a time. To decrypt, the inverse permutation $d = e^{-1}$ is applied to each letter of the ciphertext. For instance, suppose that the key e is chosen to be the permutation which maps each letter to the one which is three positions to its right, as shown below

$$e = \begin{pmatrix} \mathrm{A}\ \mathrm{B}\ \mathrm{C}\ \mathrm{D}\ \mathrm{E}\ \mathrm{F}\ \mathrm{G}\ \mathrm{H}\ \mathrm{I}\ \mathrm{J}\ \mathrm{K}\ \mathrm{L}\ \mathrm{M}\ \mathrm{N}\ \mathrm{O}\ \mathrm{P}\ \mathrm{Q}\ \mathrm{R}\ \mathrm{S}\ \mathrm{T}\ \mathrm{U}\ \mathrm{V}\ \mathrm{W}\ \mathrm{X}\ \mathrm{Y}\ \mathrm{Z} \\ \mathrm{D}\ \mathrm{E}\ \mathrm{F}\ \mathrm{G}\ \mathrm{H}\ \mathrm{I}\ \mathrm{J}\ \mathrm{K}\ \mathrm{L}\ \mathrm{M}\ \mathrm{N}\ \mathrm{O}\ \mathrm{P}\ \mathrm{Q}\ \mathrm{R}\ \mathrm{S}\ \mathrm{T}\ \mathrm{U}\ \mathrm{V}\ \mathrm{W}\ \mathrm{X}\ \mathrm{Y}\ \mathrm{Z}\ \mathrm{A}\ \mathrm{B}\ \mathrm{C} \end{pmatrix}$$

[2] Private key is a term also used in quite a different context (see §1.8). The term will be reserved for the latter usage in this book.

A message

$$m = \text{THISC IPHER ISCER TAINL YNOTS ECURE}$$

is encrypted to

$$c = E_e(m) = \text{WKLVF LSKHU LVFHU WDLQO BQRWV HFXUH.} \quad \square$$

A two-party communication using symmetric-key encryption can be described by the block diagram of Figure 1.7, which is Figure 1.6 with the addition of the secure (both con-

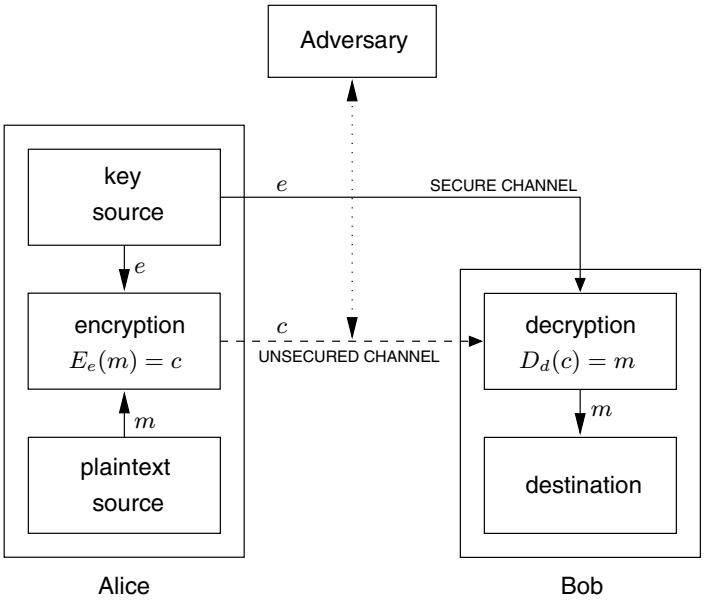


Figure 1.7: *Two-party communication using encryption, with a secure channel for key exchange. The decryption key d can be efficiently computed from the encryption key e.*

fidential and authentic) channel. One of the major issues with symmetric-key systems is to find an efficient method to agree upon and exchange keys securely. This problem is referred to as the *key distribution problem* (see Chapters 12 and 13).

It is assumed that all parties know the set of encryption/decryption transformations (i.e., they all know the encryption scheme). As has been emphasized several times the only information which should be required to be kept secret is the key d. However, in symmetric-key encryption, this means that the key e must also be kept secret, as d can be deduced from e. In Figure 1.7 the encryption key e is transported from one entity to the other with the understanding that both can construct the decryption key d.

There are two classes of symmetric-key encryption schemes which are commonly distinguished: *block ciphers* and *stream ciphers*.

1.26 Definition A *block cipher* is an encryption scheme which breaks up the plaintext messages to be transmitted into strings (called *blocks*) of a fixed length t over an alphabet $\mathcal{A}$, and encrypts one block at a time.

Most well-known symmetric-key encryption techniques are block ciphers. A number of examples of these are given in Chapter 7. Two important classes of block ciphers are *substitution ciphers* and *transposition ciphers* (§1.5.2). Product ciphers (§1.5.3) combine

these. Stream ciphers are considered in §1.5.4, while comments on the key space follow in §1.5.5.

1.5.2 Substitution ciphers and transposition ciphers

Substitution ciphers are block ciphers which replace symbols (or groups of symbols) by other symbols or groups of symbols.

Simple substitution ciphers

1.27 Definition Let $\mathcal{A}$ be an alphabet of q symbols and $\mathcal{M}$ be the set of all strings of length t over $\mathcal{A}$. Let $\mathcal{K}$ be the set of all permutations on the set $\mathcal{A}$. Define for each $e \in \mathcal{K}$ an encryption transformation E_e as:

$$E_e(m) = (e(m_1)e(m_2)\cdots e(m_t)) = (c_1c_2\cdots c_t) = c,$$

where $m = (m_1m_2\cdots m_t) \in \mathcal{M}$. In other words, for each symbol in a t-tuple, replace (substitute) it by another symbol from $\mathcal{A}$ according to some fixed permutation e. To decrypt $c = (c_1c_2\cdots c_t)$ compute the inverse permutation $d = e^{-1}$ and

$$D_d(c) = (d(c_1)d(c_2)\cdots d(c_t)) = (m_1m_2\cdots m_t) = m.$$

E_e is called a *simple substitution cipher* or a *mono-alphabetic substitution cipher*.

The number of distinct substitution ciphers is $q!$ and is independent of the block size in the cipher. Example 1.25 is an example of a simple substitution cipher of block length five.

Simple substitution ciphers over small block sizes provide inadequate security even when the key space is extremely large. If the alphabet is the English alphabet as in Example 1.25, then the size of the key space is $26! \approx 4 \times 10^{26}$, yet the key being used can be determined quite easily by examining a modest amount of ciphertext. This follows from the simple observation that the distribution of letter frequencies is preserved in the ciphertext. For example, the letter E occurs more frequently than the other letters in ordinary English text. Hence the letter occurring most frequently in a sequence of ciphertext blocks is most likely to correspond to the letter E in the plaintext. By observing a modest quantity of ciphertext blocks, a cryptanalyst can determine the key.

Homophonic substitution ciphers

1.28 Definition To each symbol $a \in \mathcal{A}$, associate a set $H(a)$ of strings of t symbols, with the restriction that the sets $H(a)$, $a \in \mathcal{A}$, be pairwise disjoint. A *homophonic substitution cipher* replaces each symbol a in a plaintext message block with a randomly chosen string from $H(a)$. To decrypt a string c of t symbols, one must determine an $a \in \mathcal{A}$ such that $c \in H(a)$. The key for the cipher consists of the sets $H(a)$.

1.29 Example (*homophonic substitution cipher*) Consider $\mathcal{A} = \{a, b\}$, $H(a) = \{00, 10\}$, and $H(b) = \{01, 11\}$. The plaintext message block ab encrypts to one of the following: 0001, 0011, 1001, 1011. Observe that the codomain of the encryption function (for messages of length two) consists of the following pairwise disjoint sets of four-element bitstrings:

$$\begin{aligned} aa &\longrightarrow \{0000, 0010, 1000, 1010\} \\ ab &\longrightarrow \{0001, 0011, 1001, 1011\} \\ ba &\longrightarrow \{0100, 0110, 1100, 1110\} \\ bb &\longrightarrow \{0101, 0111, 1101, 1111\} \end{aligned}$$

Any 4-bitstring uniquely identifies a codomain element, and hence a plaintext message. □

Often the symbols do not occur with equal frequency in plaintext messages. With a simple substitution cipher this non-uniform frequency property is reflected in the ciphertext as illustrated in Example 1.25. A homophonic cipher can be used to make the frequency of occurrence of ciphertext symbols more uniform, at the expense of data expansion. Decryption is not as easily performed as it is for simple substitution ciphers.

Polyalphabetic substitution ciphers

1.30 Definition A *polyalphabetic substitution cipher* is a block cipher with block length t over an alphabet $\mathcal{A}$ having the following properties:

(i) the key space $\mathcal{K}$ consists of all ordered sets of t permutations $(p_1, p_2, \ldots, p_t)$, where each permutation p_i is defined on the set $\mathcal{A}$;
(ii) encryption of the message $m = (m_1 m_2 \cdots m_t)$ under the key $e = (p_1, p_2, \ldots, p_t)$ is given by $E_e(m) = (p_1(m_1)p_2(m_2) \cdots p_t(m_t))$; and
(iii) the decryption key associated with $e = (p_1, p_2, \ldots, p_t)$ is $d = (p_1^{-1}, p_2^{-1}, \ldots, p_t^{-1})$.

1.31 Example (*Vigenère cipher*) Let $\mathcal{A} = \{\mathrm{A}, \mathrm{B}, \mathrm{C}, \ldots, \mathrm{X}, \mathrm{Y}, \mathrm{Z}\}$ and $t = 3$. Choose $e = (p_1, p_2, p_3)$, where p_1 maps each letter to the letter three positions to its right in the alphabet, p_2 to the one seven positions to its right, and p_3 ten positions to its right. If

$$m = \text{THI SCI PHE RIS CER TAI NLY NOT SEC URE}$$

then

$$c = E_e(m) = \text{WOS VJS SOO UPC FLB WHS QSI QVD VLM XYO.} \qquad \square$$

Polyalphabetic ciphers have the advantage over simple substitution ciphers that symbol frequencies are not preserved. In the example above, the letter E is encrypted to both O and L. However, polyalphabetic ciphers are not significantly more difficult to cryptanalyze, the approach being similar to the simple substitution cipher. In fact, once the block length t is determined, the ciphertext letters can be divided into t groups (where group i, $1 \leq i \leq t$, consists of those ciphertext letters derived using permutation p_i), and a frequency analysis can be done on each group.

Transposition ciphers

Another class of symmetric-key ciphers is the simple transposition cipher, which simply permutes the symbols in a block.

1.32 Definition Consider a symmetric-key block encryption scheme with block length t. Let $\mathcal{K}$ be the set of all permutations on the set $\{1, 2, \ldots, t\}$. For each $e \in \mathcal{K}$ define the encryption function

$$E_e(m) = (m_{e(1)} m_{e(2)} \cdots m_{e(t)})$$

where $m = (m_1 m_2 \cdots m_t) \in \mathcal{M}$, the message space. The set of all such transformations is called a *simple transposition cipher.* The decryption key corresponding to e is the inverse permutation $d = e^{-1}$. To decrypt $c = (c_1 c_2 \cdots c_t)$, compute $D_d(c) = (c_{d(1)} c_{d(2)} \cdots c_{d(t)})$.

A simple transposition cipher preserves the number of symbols of a given type within a block, and thus is easily cryptanalyzed.

1.5.3 Composition of ciphers

In order to describe product ciphers, the concept of composition of functions is introduced. Compositions are a convenient way of constructing more complicated functions from simpler ones.

Composition of functions

1.33 Definition Let $\mathcal{S}$, $\mathcal{T}$, and $\mathcal{U}$ be finite sets and let $f\colon \mathcal{S} \longrightarrow \mathcal{T}$ and $g\colon \mathcal{T} \longrightarrow \mathcal{U}$ be functions. The *composition* of g with f, denoted $g \circ f$ (or simply gf), is a function from $\mathcal{S}$ to $\mathcal{U}$ as illustrated in Figure 1.8 and defined by $(g \circ f)(x) = g(f(x))$ for all $x \in \mathcal{S}$.

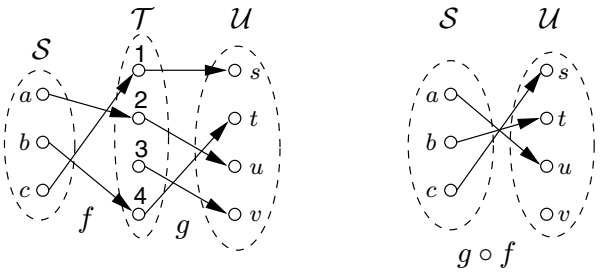


Figure 1.8: *The composition $g \circ f$ of functions g and f.*

Composition can be easily extended to more than two functions. For functions f_1, f_2, $\ldots$, f_t, one can define $f_t \circ \cdots \circ f_2 \circ f_1$, provided that the domain of f_t equals the codomain of f_{t-1} and so on.

Compositions and involutions

Involutions were introduced in §1.3.3 as a simple class of functions with an interesting property: $E_k(E_k(x)) = x$ for all x in the domain of E_k; that is, $E_k \circ E_k$ is the identity function.

1.34 Remark (*composition of involutions*) The composition of two involutions is not necessarily an involution, as illustrated in Figure 1.9. However, involutions may be composed to get somewhat more complicated functions whose inverses are easy to find. This is an important feature for decryption. For example if $E_{k_1}, E_{k_2}, \ldots, E_{k_t}$ are involutions then the inverse of $E_k = E_{k_1} E_{k_2} \cdots E_{k_t}$ is $E_k^{-1} = E_{k_t} E_{k_{t-1}} \cdots E_{k_1}$, the composition of the involutions in the reverse order.

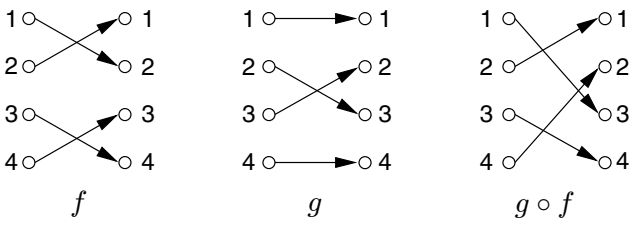


Figure 1.9: *The composition $g \circ f$ of involutions g and f is not an involution.*

Product ciphers

Simple substitution and transposition ciphers individually do not provide a very high level of security. However, by combining these transformations it is possible to obtain strong ciphers. As will be seen in Chapter 7 some of the most practical and effective symmetric-key systems are product ciphers. One example of a *product cipher* is a composition of $t \geq 2$ transformations $E_{k_1} E_{k_2} \cdots E_{k_t}$ where each E_{k_i}, $1 \leq i \leq t$, is either a substitution or a transposition cipher. For the purpose of this introduction, let the composition of a substitution and a transposition be called a *round*.

1.35 Example (*product cipher*) Let $\mathcal{M} = \mathcal{C} = \mathcal{K}$ be the set of all binary strings of length six. The number of elements in $\mathcal{M}$ is $2^6 = 64$. Let $m = (m_1 m_2 \cdots m_6)$ and define

$$\begin{aligned} E_k^{(1)}(m) &= m \oplus k, \text{ where } k \in \mathcal{K}, \\ E^{(2)}(m) &= (m_4 m_5 m_6 m_1 m_2 m_3). \end{aligned}$$

Here, $\oplus$ is the *exclusive-OR* (XOR) operation defined as follows: $0 \oplus 0 = 0$, $0 \oplus 1 = 1$, $1 \oplus 0 = 1$, $1 \oplus 1 = 0$. $E_k^{(1)}$ is a polyalphabetic substitution cipher and $E^{(2)}$ is a transposition cipher (not involving the key). The product $E_k^{(1)} E^{(2)}$ is a round. While here the transposition cipher is very simple and is not determined by the key, this need not be the case. □

1.36 Remark (*confusion and diffusion*) A substitution in a round is said to add *confusion* to the encryption process whereas a transposition is said to add *diffusion*. Confusion is intended to make the relationship between the key and ciphertext as complex as possible. Diffusion refers to rearranging or spreading out the bits in the message so that any redundancy in the plaintext is spread out over the ciphertext. A round then can be said to add both confusion and diffusion to the encryption. Most modern block cipher systems apply a number of rounds in succession to encrypt plaintext.

1.5.4 Stream ciphers

Stream ciphers form an important class of symmetric-key encryption schemes. They are, in one sense, very simple block ciphers having block length equal to one. What makes them useful is the fact that the encryption transformation can change for each symbol of plaintext being encrypted. In situations where transmission errors are highly probable, stream ciphers are advantageous because they have no error propagation. They can also be used when the data must be processed one symbol at a time (e.g., if the equipment has no memory or buffering of data is limited).

1.37 Definition Let $\mathcal{K}$ be the key space for a set of encryption transformations. A sequence of symbols $e_1 e_2 e_3 \cdots e_i \in \mathcal{K}$, is called a *keystream*.

1.38 Definition Let $\mathcal{A}$ be an alphabet of q symbols and let E_e be a simple substitution cipher with block length 1 where $e \in \mathcal{K}$. Let $m_1 m_2 m_3 \cdots$ be a plaintext string and let $e_1 e_2 e_3 \cdots$ be a keystream from $\mathcal{K}$. A *stream cipher* takes the plaintext string and produces a ciphertext string $c_1 c_2 c_3 \cdots$ where $c_i = E_{e_i}(m_i)$. If d_i denotes the inverse of e_i, then $D_{d_i}(c_i) = m_i$ decrypts the ciphertext string.

A stream cipher applies simple encryption transformations according to the keystream being used. The keystream could be generated at random, or by an algorithm which generates the keystream from an initial small keystream (called a *seed*), or from a seed and previous ciphertext symbols. Such an algorithm is called a *keystream generator*.

The Vernam cipher

A motivating factor for the Vernam cipher was its simplicity and ease of implementation.

1.39 Definition The *Vernam Cipher* is a stream cipher defined on the alphabet $\mathcal{A} = \{0, 1\}$. A binary message $m_1 m_2 \cdots m_t$ is operated on by a binary key string $k_1 k_2 \cdots k_t$ of the same length to produce a ciphertext string $c_1 c_2 \cdots c_t$ where

$$c_i = m_i \oplus k_i, \;\; 1 \leq i \leq t.$$

If the key string is randomly chosen and never used again, the Vernam cipher is called a *one-time system* or a *one-time pad*.

To see how the Vernam cipher corresponds to Definition 1.38, observe that there are precisely two substitution ciphers on the set $\mathcal{A}$. One is simply the identity map E_0 which sends 0 to 0 and 1 to 1; the other E_1 sends 0 to 1 and 1 to 0. When the keystream contains a 0, apply E_0 to the corresponding plaintext symbol; otherwise, apply E_1.

If the key string is reused there are ways to attack the system. For example, if $c_1 c_2 \cdots c_t$ and $c'_1 c'_2 \cdots c'_t$ are two ciphertext strings produced by the same keystream $k_1 k_2 \cdots k_t$ then

$$c_i = m_i \oplus k_i, \quad c'_i = m'_i \oplus k_i$$

and $c_i \oplus c'_i = m_i \oplus m'_i$. The redundancy in the latter may permit cryptanalysis.

The one-time pad can be shown to be theoretically unbreakable. That is, if a cryptanalyst has a ciphertext string $c_1 c_2 \cdots c_t$ encrypted using a random key string which has been used only once, the cryptanalyst can do no better than guess at the plaintext being any binary string of length t (i.e., t-bit binary strings are equally likely as plaintext). It has been proven that to realize an unbreakable system requires a random key of the same length as the message. This reduces the practicality of the system in all but a few specialized situations. Reportedly until very recently the communication line between Moscow and Washington was secured by a one-time pad. Transport of the key was done by trusted courier.

1.5.5 The key space

The size of the key space is the number of encryption/decryption key pairs that are available in the cipher system. A key is typically a compact way to specify the encryption transformation (from the set of all encryption transformations) to be used. For example, a transposition cipher of block length t has $t!$ encryption functions from which to select. Each can be simply described by a permutation which is called the key.

It is a great temptation to relate the security of the encryption scheme to the size of the key space. The following statement is important to remember.

1.40 Fact A necessary, but usually not sufficient, condition for an encryption scheme to be secure is that the key space be large enough to preclude exhaustive search.

For instance, the simple substitution cipher in Example 1.25 has a key space of size $26! \approx 4 \times 10^{26}$. The polyalphabetic substitution cipher of Example 1.31 has a key space of size $(26!)^3 \approx 7 \times 10^{79}$. Exhaustive search of either key space is completely infeasible, yet both ciphers are relatively weak and provide little security.

1.6 Digital signatures

A cryptographic primitive which is fundamental in authentication, authorization, and non-repudiation is the *digital signature*. The purpose of a digital signature is to provide a means for an entity to bind its identity to a piece of information. The process of *signing* entails transforming the message and some secret information held by the entity into a tag called a *signature*. A generic description follows.

Nomenclature and set-up

- $\mathcal{M}$ is the set of messages which can be signed.
- $\mathcal{S}$ is a set of elements called *signatures*, possibly binary strings of a fixed length.
- S_A is a transformation from the message set $\mathcal{M}$ to the signature set $\mathcal{S}$, and is called a *signing transformation* for entity A.[3] The transformation S_A is kept secret by A, and will be used to create signatures for messages from $\mathcal{M}$.
- V_A is a transformation from the set $\mathcal{M} \times \mathcal{S}$ to the set $\{true, false\}$.[4] V_A is called a *verification transformation* for A's signatures, is publicly known, and is used by other entities to verify signatures created by A.

1.41 Definition The transformations S_A and V_A provide a *digital signature scheme* for A. Occasionally the term *digital signature mechanism* is used.

1.42 Example (*digital signature scheme*) $\mathcal{M} = \{m_1, m_2, m_3\}$ and $\mathcal{S} = \{s_1, s_2, s_3\}$. The left side of Figure 1.10 displays a signing function S_A from the set $\mathcal{M}$ and, the right side, the corresponding verification function V_A. □

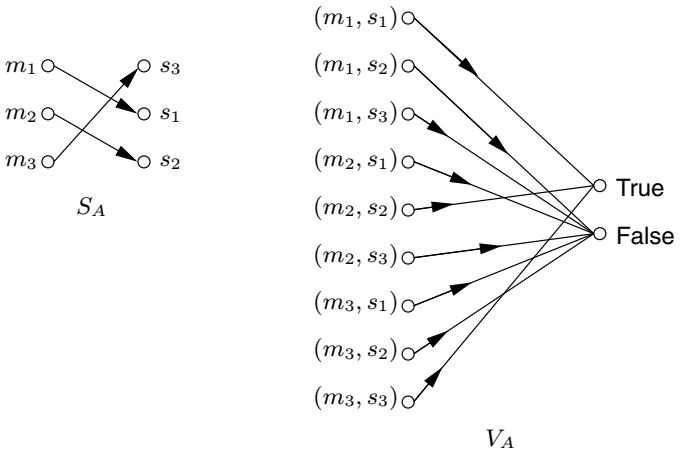


Figure 1.10: *A signing and verification function for a digital signature scheme.*

[3] The names of Alice and Bob are usually abbreviated to A and B, respectively.
[4] $\mathcal{M} \times \mathcal{S}$ consists of all pairs (m, s) where $m \in \mathcal{M}$, $s \in \mathcal{S}$, called the *Cartesian product* of $\mathcal{M}$ and $\mathcal{S}$.

Signing procedure

Entity A (the *signer*) creates a signature for a message $m \in \mathcal{M}$ by doing the following:

1. Compute $s = S_A(m)$.
2. Transmit the pair (m, s). s is called the *signature* for message m.

Verification procedure

To verify that a signature s on a message m was created by A, an entity B (the *verifier*) performs the following steps:

1. Obtain the verification function V_A of A.
2. Compute $u = V_A(m, s)$.
3. Accept the signature as having been created by A if $u = \mathit{true}$, and reject the signature if $u = \mathit{false}$.

1.43 Remark (*concise representation*) The transformations S_A and V_A are typically characterized more compactly by a key; that is, there is a class of signing and verification algorithms publicly known, and each algorithm is identified by a key. Thus the signing algorithm S_A of A is determined by a key k_A and A is only required to keep k_A secret. Similarly, the verification algorithm V_A of A is determined by a key l_A which is made public.

1.44 Remark (*handwritten signatures*) Handwritten signatures could be interpreted as a special class of digital signatures. To see this, take the set of signatures $\mathcal{S}$ to contain only one element which is the handwritten signature of A, denoted by s_A. The verification function simply checks if the signature on a message purportedly signed by A is s_A.

An undesirable feature in Remark 1.44 is that the signature is not message-dependent. Hence, further constraints are imposed on digital signature mechanisms as next discussed.

Properties required for signing and verification functions

There are several properties which the signing and verification transformations must satisfy.

(a) s is a valid signature of A on message m if and only if $V_A(m, s) = \mathit{true}$.
(b) It is computationally infeasible for any entity other than A to find, for any $m \in \mathcal{M}$, an $s \in \mathcal{S}$ such that $V_A(m, s) = \mathit{true}$.

Figure 1.10 graphically displays property (a). There is an arrowed line in the diagram for V_A from (m_i, s_j) to *true* provided there is an arrowed line from m_i to s_j in the diagram for S_A. Property (b) provides the security for the method – the signature uniquely binds A to the message which is signed.

No one has yet formally proved that digital signature schemes satisfying (b) exist (although existence is widely believed to be true); however, there are some very good candidates. §1.8.3 introduces a particular class of digital signatures which arise from public-key encryption techniques. Chapter 11 describes a number of digital signature mechanisms which are believed to satisfy the two properties cited above. Although the description of a digital signature given in this section is quite general, it can be broadened further, as presented in §11.2.

1.7 Authentication and identification

Authentication is a term which is used (and often abused) in a very broad sense. By itself it has little meaning other than to convey the idea that some means has been provided to guarantee that entities are who they claim to be, or that information has not been manipulated by unauthorized parties. Authentication is specific to the security objective which one is trying to achieve. Examples of specific objectives include access control, entity authentication, message authentication, data integrity, non-repudiation, and key authentication. These instances of authentication are dealt with at length in Chapters 9 through 13. For the purposes of this chapter, it suffices to give a brief introduction to authentication by describing several of the most obvious applications.

Authentication is one of the most important of all information security objectives. Until the mid 1970s it was generally believed that secrecy and authentication were intrinsically connected. With the discovery of hash functions (§1.9) and digital signatures (§1.6), it was realized that secrecy and authentication were truly separate and independent information security objectives. It may at first not seem important to separate the two but there are situations where it is not only useful but essential. For example, if a two-party communication between Alice and Bob is to take place where Alice is in one country and Bob in another, the host countries might not permit secrecy on the channel; one or both countries might want the ability to monitor all communications. Alice and Bob, however, would like to be assured of the identity of each other, and of the integrity and origin of the information they send and receive.

The preceding scenario illustrates several independent aspects of authentication. If Alice and Bob desire assurance of each other's identity, there are two possibilities to consider.

1. Alice and Bob could be communicating with no appreciable time delay. That is, they are both active in the communication in "real time".
2. Alice or Bob could be exchanging messages with some delay. That is, messages might be routed through various networks, stored, and forwarded at some later time.

In the first instance Alice and Bob would want to verify identities in real time. This might be accomplished by Alice sending Bob some challenge, to which Bob is the only entity which can respond correctly. Bob could perform a similar action to identify Alice. This type of authentication is commonly referred to as *entity authentication* or more simply *identification*.

For the second possibility, it is not convenient to challenge and await response, and moreover the communication path may be only in one direction. Different techniques are now required to authenticate the originator of the message. This form of authentication is called *data origin authentication*.

1.7.1 Identification

1.45 Definition An *identification* or *entity authentication* technique assures one party (through acquisition of corroborative evidence) of both the identity of a second party involved, and that the second was active at the time the evidence was created or acquired.

Typically the only data transmitted is that necessary to identify the communicating parties. The entities are both active in the communication, giving a timeliness guarantee.

1.46 Example (*identification*) A calls B on the telephone. If A and B know each other then entity authentication is provided through voice recognition. Although not foolproof, this works effectively in practice. □

1.47 Example (*identification*) Person A provides to a banking machine a personal identification number (PIN) along with a magnetic stripe card containing information about A. The banking machine uses the information on the card and the PIN to verify the identity of the card holder. If verification succeeds, A is given access to various services offered by the machine. □

Example 1.46 is an instance of *mutual authentication* whereas Example 1.47 only provides *unilateral authentication*. Numerous mechanisms and protocols devised to provide mutual or unilateral authentication are discussed in Chapter 10.

1.7.2 Data origin authentication

1.48 Definition *Data origin authentication* or *message authentication* techniques provide to one party which receives a message assurance (through corroborative evidence) of the identity of the party which originated the message.

Often a message is provided to B along with additional information so that B can determine the identity of the entity who originated the message. This form of authentication typically provides no guarantee of timeliness, but is useful in situations where one of the parties is not active in the communication.

1.49 Example (*need for data origin authentication*) A sends to B an electronic mail message (e-mail). The message may travel through various network communications systems and be stored for B to retrieve at some later time. A and B are usually not in direct communication. B would like some means to verify that the message received and purportedly created by A did indeed originate from A. □

Data origin authentication implicitly provides data integrity since, if the message was modified during transmission, A would no longer be the originator.

1.8 Public-key cryptography

The concept of public-key encryption is simple and elegant, but has far-reaching consequences.

1.8.1 Public-key encryption

Let $\{E_e : e \in \mathcal{K}\}$ be a set of encryption transformations, and let $\{D_d : d \in \mathcal{K}\}$ be the set of corresponding decryption transformations, where $\mathcal{K}$ is the key space. Consider any pair of associated encryption/decryption transformations (E_e, D_d) and suppose that each pair has the property that knowing E_e it is computationally infeasible, given a random ciphertext $c \in \mathcal{C}$, to find the message $m \in \mathcal{M}$ such that $E_e(m) = c$. This property implies that given e it is infeasible to determine the corresponding decryption key d. (Of course e and d are

simply means to describe the encryption and decryption functions, respectively.) E_e is being viewed here as a trapdoor one-way function (Definition 1.16) with d being the trapdoor information necessary to compute the inverse function and hence allow decryption. This is unlike symmetric-key ciphers where e and d are essentially the same.

Under these assumptions, consider the two-party communication between Alice and Bob illustrated in Figure 1.11. Bob selects the key pair (e, d). Bob sends the encryption key e (called the *public key*) to Alice over any channel but keeps the decryption key d (called the *private key*) secure and secret. Alice may subsequently send a message m to Bob by applying the encryption transformation determined by Bob's public key to get $c = E_e(m)$. Bob decrypts the ciphertext c by applying the inverse transformation D_d uniquely determined by d.

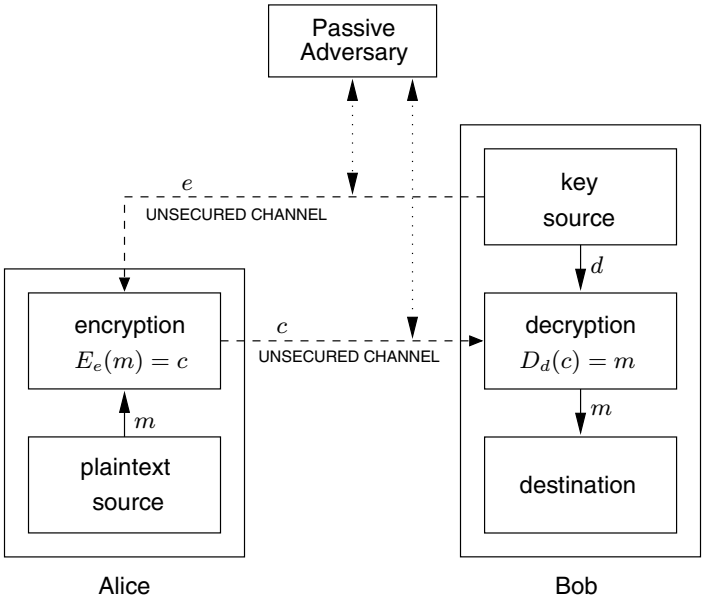


Figure 1.11: *Encryption using public-key techniques.*

Notice how Figure 1.11 differs from Figure 1.7 for a symmetric-key cipher. Here the encryption key is transmitted to Alice over an unsecured channel. This unsecured channel may be the same channel on which the ciphertext is being transmitted (but see §1.8.2).

Since the encryption key e need not be kept secret, it may be made public. Any entity can subsequently send encrypted messages to Bob which only Bob can decrypt. Figure 1.12 illustrates this idea, where A_1, A_2, and A_3 are distinct entities. Note that if A_1 destroys message m_1 after encrypting it to c_1, then even A_1 cannot recover m_1 from c_1.

As a physical analogue, consider a metal box with the lid secured by a combination lock. The combination is known only to Bob. If the lock is left open and made publicly available then anyone can place a message inside and lock the lid. Only Bob can retrieve the message. Even the entity which placed the message into the box is unable to retrieve it.

Public-key encryption, as described here, assumes that knowledge of the public key e does not allow computation of the private key d. In other words, this assumes the existence of trapdoor one-way functions (§1.3.1(iii)).

1.50 Definition Consider an encryption scheme consisting of the sets of encryption and decryp-

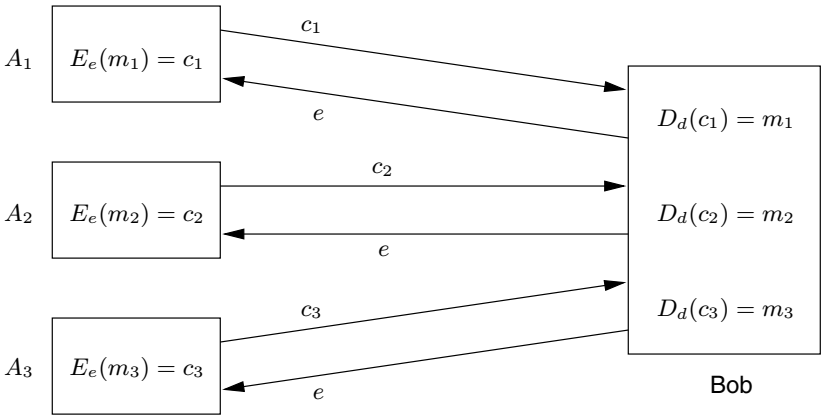


Figure 1.12: *Schematic use of public-key encryption.*

tion transformations $\{E_e : e \in \mathcal{K}\}$ and $\{D_d : d \in \mathcal{K}\}$, respectively. The encryption method is said to be a *public-key encryption scheme* if for each associated encryption/decryption pair (e, d), one key e (the *public key*) is made publicly available, while the other d (the *private key*) is kept secret. For the scheme to be *secure*, it must be computationally infeasible to compute d from e.

1.51 Remark (*private key vs. secret key*) To avoid ambiguity, a common convention is to use the term *private key* in association with public-key cryptosystems, and *secret key* in association with symmetric-key cryptosystems. This may be motivated by the following line of thought: it takes two or more parties to *share* a secret, but a key is truly *private* only when one party alone knows it.

There are many schemes known which are widely believed to be secure public-key encryption methods, but none have been mathematically proven to be secure independent of qualifying assumptions. This is not unlike the symmetric-key case where the only system which has been proven secure is the one-time pad (§1.5.4).

1.8.2 The necessity of authentication in public-key systems

It would appear that public-key cryptography is an ideal system, not requiring a secure channel to pass the encryption key. This would imply that two entities could communicate over an unsecured channel without ever having met to exchange keys. Unfortunately, this is not the case. Figure 1.13 illustrates how an active adversary can defeat the system (decrypt messages intended for a second entity) without breaking the encryption system. This is a type of *impersonation* and is an example of *protocol failure* (see §1.10). In this scenario the adversary impersonates entity B by sending entity A a public key e' which A assumes (incorrectly) to be the public key of B. The adversary intercepts encrypted messages from A to B, decrypts with its own private key d', re-encrypts the message under B's public key e, and sends it on to B. This highlights the necessity to *authenticate* public keys to achieve data origin authentication of the public keys themselves. A must be convinced that she is

encrypting under the legitimate public key of B. Fortunately, public-key techniques also allow an elegant solution to this problem (see §1.11).

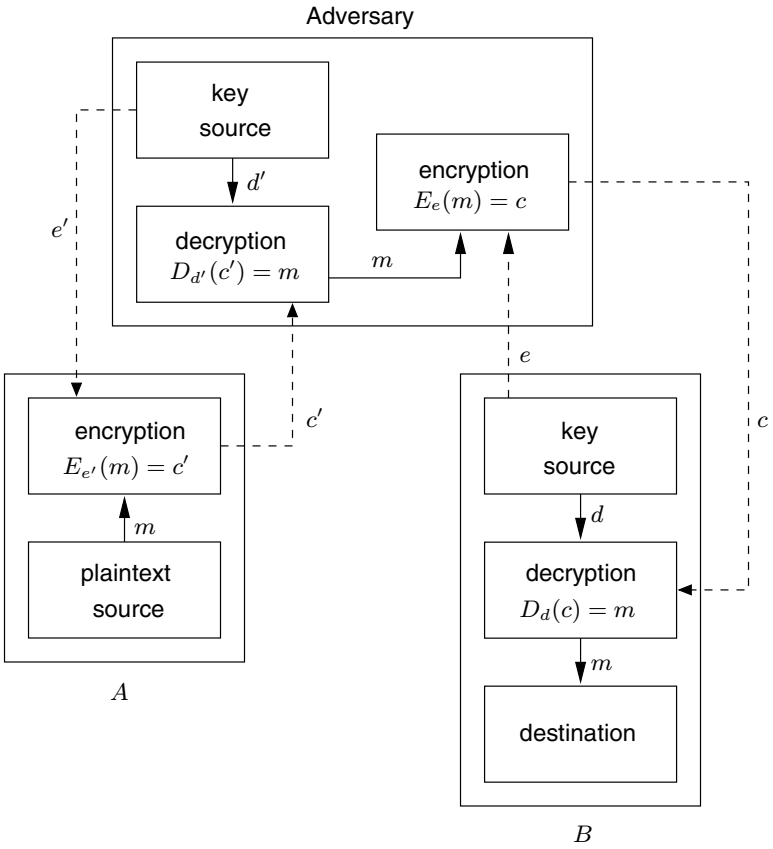


Figure 1.13: *An impersonation attack on a two-party communication.*

1.8.3 Digital signatures from reversible public-key encryption

This section considers a class of digital signature schemes which is based on public-key encryption systems of a particular type.

Suppose E_e is a public-key encryption transformation with message space $\mathcal{M}$ and ciphertext space $\mathcal{C}$. Suppose further that $\mathcal{M} = \mathcal{C}$. If D_d is the decryption transformation corresponding to E_e then since E_e and D_d are both permutations, one has

$$D_d(E_e(m)) = E_e(D_d(m)) = m, \text{ for all } m \in \mathcal{M}.$$

A public-key encryption scheme of this type is called *reversible*.[5] Note that it is essential that $\mathcal{M} = \mathcal{C}$ for this to be a valid equality for all $m \in \mathcal{M}$; otherwise, $D_d(m)$ will be meaningless for $m \notin \mathcal{C}$.

[5] There is a broader class of digital signatures which can be informally described as arising from *irreversible* cryptographic algorithms. These are described in §11.2.

Construction for a digital signature scheme

1. Let $\mathcal{M}$ be the message space for the signature scheme.
2. Let $\mathcal{C} = \mathcal{M}$ be the signature space $\mathcal{S}$.
3. Let (e, d) be a key pair for the public-key encryption scheme.
4. Define the signing function S_A to be D_d. That is, the signature for a message $m \in \mathcal{M}$ is $s = D_d(m)$.
5. Define the verification function V_A by

$$V_A(m, s) = \begin{cases} \textit{true}, & \text{if } E_e(s) = m, \\ \textit{false}, & \text{otherwise.} \end{cases}$$

The signature scheme can be simplified further if A only signs messages having a special structure, and this structure is publicly known. Let $\mathcal{M}'$ be a subset of $\mathcal{M}$ where elements of $\mathcal{M}'$ have a well-defined special structure, such that $\mathcal{M}'$ contains only a negligible fraction of messages from the set. For example, suppose that $\mathcal{M}$ consists of all binary strings of length $2t$ for some positive integer t. Let $\mathcal{M}'$ be the subset of $\mathcal{M}$ consisting of all strings where the first t bits are replicated in the last t positions (e.g., 101101 would be in $\mathcal{M}'$ for $t = 3$). If A only signs messages within the subset $\mathcal{M}'$, these are easily recognized by a verifier.

Redefine the verification function V_A as

$$V_A(s) = \begin{cases} \textit{true}, & \text{if } E_e(s) \in \mathcal{M}', \\ \textit{false}, & \text{otherwise.} \end{cases}$$

Under this new scenario A only needs to transmit the signature s since the message $m = E_e(s)$ can be recovered by applying the verification function. Such a scheme is called a *digital signature scheme with message recovery*. Figure 1.14 illustrates how this signature function is used. The feature of selecting messages of special structure is referred to as selecting messages with *redundancy*.

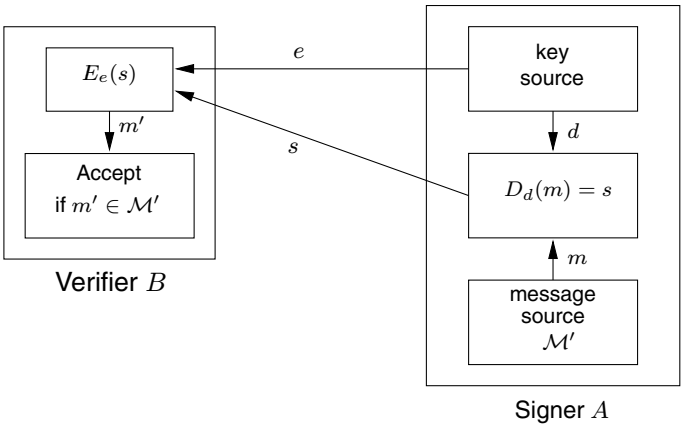


Figure 1.14: *A digital signature scheme with message recovery.*

The modification presented above is more than a simplification; it is absolutely crucial if one hopes to meet the requirement of property (b) of signing and verification functions (see page 23). To see why this is the case, note that any entity B can select a random element $s \in \mathcal{S}$ as a signature and apply E_e to get $u = E_e(s)$, since $\mathcal{S} = \mathcal{M}$ and E_e is public

knowledge. B may then take the message $m = u$ and the signature on m to be s and transmits (m, s). It is easy to check that s will verify as a signature created by A for m but in which A has had no part. In this case B has *forged* a signature of A. This is an example of what is called *existential forgery*. (B has produced A's signature on some message likely not of B's choosing.)

If $\mathcal{M}'$ contains only a negligible fraction of messages from $\mathcal{M}$, then the probability of some entity forging a signature of A in this manner is negligibly small.

1.52 Remark (*digital signatures vs. confidentiality*) Although digital signature schemes based on reversible public-key encryption are attractive, they require an encryption method as a primitive. There are situations where a digital signature mechanism is required but encryption is forbidden. In such cases these digital signature schemes are inappropriate.

Digital signatures in practice

For digital signatures to be useful in practice, concrete realizations of the preceding concepts should have certain additional properties. A digital signature must

1. be easy to compute by the signer (the signing function should be easy to apply);
2. be easy to verify by anyone (the verification function should be easy to apply); and
3. have an appropriate lifespan, i.e., be computationally secure from forgery until the signature is no longer necessary for its original purpose.

Resolution of disputes

The purpose of a digital signature (or any signature method) is to permit the resolution of disputes. For example, an entity A could at some point deny having signed a message or some other entity B could falsely claim that a signature on a message was produced by A. In order to overcome such problems a *trusted third party* (TTP) or *judge* is required. The TTP must be some entity which all parties involved agree upon in advance.

If A denies that a message m held by B was signed by A, then B should be able to present the signature s_A for m to the TTP along with m. The TTP rules in favor of B if $V_A(m, s_A) = \textit{true}$ and in favor of A otherwise. B will accept the decision if B is confident that the TTP has the same verifying transformation V_A as A does. A will accept the decision if A is confident that the TTP used V_A and that S_A has not been compromised. Therefore, fair resolution of disputes requires that the following criteria are met.

Requirements for resolution of disputed signatures

1. S_A and V_A have properties (a) and (b) of page 23.
2. The TTP has an authentic copy of V_A.
3. The signing transformation S_A has been kept secret and remains secure.

These properties are necessary but in practice it might not be possible to guarantee them. For example, the assumption that S_A and V_A have the desired characteristics given in property 1 might turn out to be false for a particular signature scheme. Another possibility is that A claims falsely that S_A was compromised. To overcome these problems requires an agreed method to validate the time period for which A will accept responsibility for the verification transformation. An analogue of this situation can be made with credit card revocation. The holder of a card is responsible until the holder notifies the card issuing company that the card has been lost or stolen. §13.8.2 gives a more indepth discussion of these problems and possible solutions.

1.8.4 Symmetric-key vs. public-key cryptography

Symmetric-key and public-key encryption schemes have various advantages and disadvantages, some of which are common to both. This section highlights a number of these and summarizes features pointed out in previous sections.

(i) Advantages of symmetric-key cryptography

1. Symmetric-key ciphers can be designed to have high rates of data throughput. Some hardware implementations achieve encrypt rates of hundreds of megabytes per second, while software implementations may attain throughput rates in the megabytes per second range.
2. Keys for symmetric-key ciphers are relatively short.
3. Symmetric-key ciphers can be employed as primitives to construct various cryptographic mechanisms including pseudorandom number generators (see Chapter 5), hash functions (see Chapter 9), and computationally efficient digital signature schemes (see Chapter 11), to name just a few.
4. Symmetric-key ciphers can be composed to produce stronger ciphers. Simple transformations which are easy to analyze, but on their own weak, can be used to construct strong product ciphers.
5. Symmetric-key encryption is perceived to have an extensive history, although it must be acknowledged that, notwithstanding the invention of rotor machines earlier, much of the knowledge in this area has been acquired subsequent to the invention of the digital computer, and, in particular, the design of the Data Encryption Standard (see Chapter 7) in the early 1970s.

(ii) Disadvantages of symmetric-key cryptography

1. In a two-party communication, the key must remain secret at both ends.
2. In a large network, there are many key pairs to be managed. Consequently, effective key management requires the use of an unconditionally trusted TTP (Definition 1.65).
3. In a two-party communication between entities A and B, sound cryptographic practice dictates that the key be changed frequently, and perhaps for each communication session.
4. Digital signature mechanisms arising from symmetric-key encryption typically require either large keys for the public verification function or the use of a TTP (see Chapter 11).

(iii) Advantages of public-key cryptography

1. Only the private key must be kept secret (authenticity of public keys must, however, be guaranteed).
2. The administration of keys on a network requires the presence of only a functionally trusted TTP (Definition 1.66) as opposed to an unconditionally trusted TTP. Depending on the mode of usage, the TTP might only be required in an "off-line" manner, as opposed to in real time.
3. Depending on the mode of usage, a private key/public key pair may remain unchanged for considerable periods of time, e.g., many sessions (even several years).
4. Many public-key schemes yield relatively efficient digital signature mechanisms. The key used to describe the public verification function is typically much smaller than for the symmetric-key counterpart.

5. In a large network, the number of keys necessary may be considerably smaller than in the symmetric-key scenario.

(iv) Disadvantages of public-key encryption

1. Throughput rates for the most popular public-key encryption methods are several orders of magnitude slower than the best known symmetric-key schemes.
2. Key sizes are typically much larger than those required for symmetric-key encryption (see Remark 1.53), and the size of public-key signatures is larger than that of tags providing data origin authentication from symmetric-key techniques.
3. No public-key scheme has been proven to be secure (the same can be said for block ciphers). The most effective public-key encryption schemes found to date have their security based on the presumed difficulty of a small set of number-theoretic problems.
4. Public-key cryptography does not have as extensive a history as symmetric-key encryption, being discovered only in the mid 1970s.[6]

Summary of comparison

Symmetric-key and public-key encryption have a number of complementary advantages. Current cryptographic systems exploit the strengths of each. An example will serve to illustrate.

Public-key encryption techniques may be used to establish a key for a symmetric-key system being used by communicating entities A and B. In this scenario A and B can take advantage of the long term nature of the public/private keys of the public-key scheme and the performance efficiencies of the symmetric-key scheme. Since data encryption is frequently the most time consuming part of the encryption process, the public-key scheme for key establishment is a small fraction of the total encryption process between A and B.

To date, the computational performance of public-key encryption is inferior to that of symmetric-key encryption. There is, however, no proof that this must be the case. The important points in practice are:

1. public-key cryptography facilitates efficient signatures (particularly non-repudiation) and key mangement; and
2. symmetric-key cryptography is efficient for encryption and some data integrity applications.

1.53 Remark (*key sizes: symmetric key vs. private key*) Private keys in public-key systems must be larger (e.g., 1024 bits for RSA) than secret keys in symmetric-key systems (e.g., 64 or 128 bits) because whereas (for secure algorithms) the most efficient attack on symmetric-key systems is an exhaustive key search, all known public-key systems are subject to "shortcut" attacks (e.g., factoring) more efficient than exhaustive search. Consequently, for equivalent security, symmetric keys have bitlengths considerably smaller than that of private keys in public-key systems, e.g., by a factor of 10 or more.

[6] It is, of course, arguable that some public-key schemes which are based on hard mathematical problems have a long history since these problems have been studied for many years. Although this may be true, one must be wary that the mathematics was not studied with this application in mind.

1.9 Hash functions

One of the fundamental primitives in modern cryptography is the cryptographic hash function, often informally called a one-way hash function. A simplified definition for the present discussion follows.

1.54 Definition A *hash function* is a computationally efficient function mapping binary strings of arbitrary length to binary strings of some fixed length, called *hash-values*.

For a hash function which outputs n-bit hash-values (e.g., $n = 128$ or 160) and has desirable properties, the probability that a randomly chosen string gets mapped to a particular n-bit hash-value (image) is 2^{-n}. The basic idea is that a hash-value serves as a compact representative of an input string. To be of cryptographic use, a hash function h is typically chosen such that it is computationally infeasible to find two distinct inputs which hash to a common value (i.e., two *colliding* inputs x and y such that $h(x) = h(y)$), and that given a specific hash-value y, it is computationally infeasible to find an input (pre-image) x such that $h(x) = y$.

The most common cryptographic uses of hash functions are with digital signatures and for data integrity. With digital signatures, a long message is usually hashed (using a publicly available hash function) and only the hash-value is signed. The party receiving the message then hashes the received message, and verifies that the received signature is correct for this hash-value. This saves both time and space compared to signing the message directly, which would typically involve splitting the message into appropriate-sized blocks and signing each block individually. Note here that the inability to find two messages with the same hash-value is a security requirement, since otherwise, the signature on one message hash-value would be the same as that on another, allowing a signer to sign one message and at a later point in time claim to have signed another.

Hash functions may be used for data integrity as follows. The hash-value corresponding to a particular input is computed at some point in time. The integrity of this hash-value is protected in some manner. At a subsequent point in time, to verify that the input data has not been altered, the hash-value is recomputed using the input at hand, and compared for equality with the original hash-value. Specific applications include virus protection and software distribution.

A third application of hash functions is their use in protocols involving a priori commitments, including some digital signature schemes and identification protocols (e.g., see Chapter 10).

Hash functions as discussed above are typically publicly known and involve no secret keys. When used to detect whether the message input has been altered, they are called *modification detection codes* (MDCs). Related to these are hash functions which involve a secret key, and provide data origin authentication (§9.76) as well as data integrity; these are called *message authentication codes* (MACs).

1.10 Protocols and mechanisms

1.55 Definition A *cryptographic protocol* (*protocol*) is a distributed algorithm defined by a sequence of steps precisely specifying the actions required of two or more entities to achieve a specific security objective.

1.56 Remark (*protocol vs. mechanism*) As opposed to a protocol, a *mechanism* is a more general term encompassing protocols, algorithms (specifying the steps followed by a single entity), and non-cryptographic techniques (e.g., hardware protection and procedural controls) to achieve specific security objectives.

Protocols play a major role in cryptography and are essential in meeting cryptographic goals as discussed in §1.2. Encryption schemes, digital signatures, hash functions, and random number generation are among the primitives which may be utilized to build a protocol.

1.57 Example (*a simple key agreement protocol*) Alice and Bob have chosen a symmetric-key encryption scheme to use in communicating over an unsecured channel. To encrypt information they require a key. The communication protocol is the following:

1. Bob constructs a public-key encryption scheme and sends his public key to Alice over the channel.
2. Alice generates a key for the symmetric-key encryption scheme.
3. Alice encrypts the key using Bob's public key and sends the encrypted key to Bob.
4. Bob decrypts using his private key and recovers the symmetric (secret) key.
5. Alice and Bob begin communicating with privacy by using the symmetric-key system and the common secret key.

This protocol uses basic functions to attempt to realize private communications on an unsecured channel. The basic primitives are the symmetric-key and the public-key encryption schemes. The protocol has shortcomings including the impersonation attack of §1.8.2, but it does convey the idea of a protocol. □

Often the role of public-key encryption in privacy communications is exactly the one suggested by this protocol – public-key encryption is used as a means to exchange keys for subsequent use in symmetric-key encryption, motivated by performance differences between symmetric-key and public-key encryption.

Protocol and mechanism failure

1.58 Definition A *protocol failure* or *mechanism failure* occurs when a mechanism fails to meet the goals for which it was intended, in a manner whereby an adversary gains advantage not by breaking an underlying primitive such as an encryption algorithm directly, but by manipulating the protocol or mechanism itself.

1.59 Example (*mechanism failure*) Alice and Bob are communicating using a stream cipher. Messages which they encrypt are known to have a special form: the first twenty bits carry information which represents a monetary amount. An active adversary can simply XOR an appropriate bitstring into the first twenty bits of ciphertext and change the amount. While the adversary has not been able to read the underlying message, she has been able to alter the transmission. The encryption has not been compromised but the protocol has failed to perform adequately; the inherent assumption that encryption provides data integrity is incorrect. □

1.60 Example (*forward search attack*) Suppose that in an electronic bank transaction the 32-bit field which records the value of the transaction is to be encrypted using a public-key scheme. This simple protocol is intended to provide privacy of the value field – but does it? An adversary could easily take all 2^{32} possible entries that could be plaintext in this field and encrypt them using the public encryption function. (Remember that by the very nature of public-key encryption this function must be available to the adversary.) By comparing

each of the 2^{32} ciphertexts with the one which is actually encrypted in the transaction, the adversary can determine the plaintext. Here the public-key encryption function is not compromised, but rather the way it is used. A closely related attack which applies directly to authentication for access control purposes is the dictionary attack (see §10.2.2). □

1.61 Remark (*causes of protocol failure*) Protocols and mechanisms may fail for a number of reasons, including:

1. weaknesses in a particular cryptographic primitive which may be amplified by the protocol or mechanism;
2. claimed or assumed security guarantees which are overstated or not clearly understood; and
3. the oversight of some principle applicable to a broad class of primitives such as encryption.

Example 1.59 illustrates item 2 if the stream cipher is the one-time pad, and also item 1. Example 1.60 illustrates item 3. See also §1.8.2.

1.62 Remark (*protocol design*) When designing cryptographic protocols and mechanisms, the following two steps are essential:

1. identify *all* assumptions in the protocol or mechanism design; and
2. for each assumption, determine the effect on the security objective if that assumption is violated.

1.11 Key establishment, management, and certification

This section gives a brief introduction to methodology for ensuring the secure distribution of keys for cryptographic purposes.

1.63 Definition *Key establishment* is any process whereby a shared secret key becomes available to two or more parties, for subsequent cryptographic use.

1.64 Definition *Key management* is the set of processes and mechanisms which support key establishment and the maintenance of ongoing keying relationships between parties, including replacing older keys with new keys as necessary.

Key establishment can be broadly subdivided into *key agreement* and *key transport*. Many and various protocols have been proposed to provide key establishment. Chapter 12 describes a number of these in detail. For the purpose of this chapter only a brief overview of issues related to key management will be given. Simple architectures based on symmetric-key and public-key cryptography along with the concept of certification will be addressed.

As noted in §1.5, a major issue when using symmetric-key techniques is the establishment of pairwise secret keys. This becomes more evident when considering a network of entities, any two of which may wish to communicate. Figure 1.15 illustrates a network consisting of 6 entities. The arrowed edges indicate the 15 possible two-party communications which could take place. Since each pair of entities wish to communicate, this small network requires the secure exchange of $\binom{6}{2} = 15$ key pairs. In a network with n entities, the number of secure key exchanges required is $\binom{n}{2} = \frac{n(n-1)}{2}$.

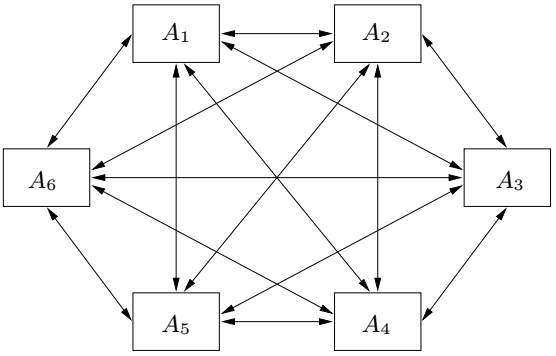


Figure 1.15: *Keying relationships in a simple 6-party network.*

The network diagram depicted in Figure 1.15 is simply the amalgamation of 15 two-party communications as depicted in Figure 1.7. In practice, networks are very large and the key management problem is a crucial issue. There are a number of ways to handle this problem. Two simplistic methods are discussed; one based on symmetric-key and the other on public-key techniques.

1.11.1 Key management through symmetric-key techniques

One solution which employs symmetric-key techniques involves an entity in the network which is trusted by all other entities. As in §1.8.3, this entity is referred to as a *trusted third party* (TTP). Each entity A_i shares a distinct symmetric key k_i with the TTP. These keys are assumed to have been distributed over a secured channel. If two entities subsequently wish to communicate, the TTP generates a key k (sometimes called a *session key*) and sends it encrypted under each of the fixed keys as depicted in Figure 1.16 for entities A_1 and A_5.

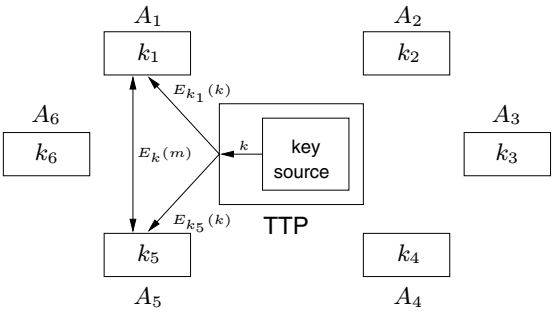


Figure 1.16: *Key management using a trusted third party (TTP).*

Advantages of this approach include:

1. It is easy to add and remove entities from the network.
2. Each entity needs to store only one long-term secret key.

Disadvantages include:

1. All communications require initial interaction with the TTP.
2. The TTP must store n long-term secret keys.

3. The TTP has the ability to read all messages.
4. If the TTP is compromised, all communications are insecure.

1.11.2 Key management through public-key techniques

There are a number of ways to address the key management problem through public-key techniques. Chapter 13 describes many of these in detail. For the purpose of this chapter a very simple model is considered.

Each entity in the network has a public/private encryption key pair. The public key along with the identity of the entity is stored in a central repository called a *public file*. If an entity A_1 wishes to send encrypted messages to entity A_6, A_1 retrieves the public key e_6 of A_6 from the public file, encrypts the message using this key, and sends the ciphertext to A_6. Figure 1.17 depicts such a network.

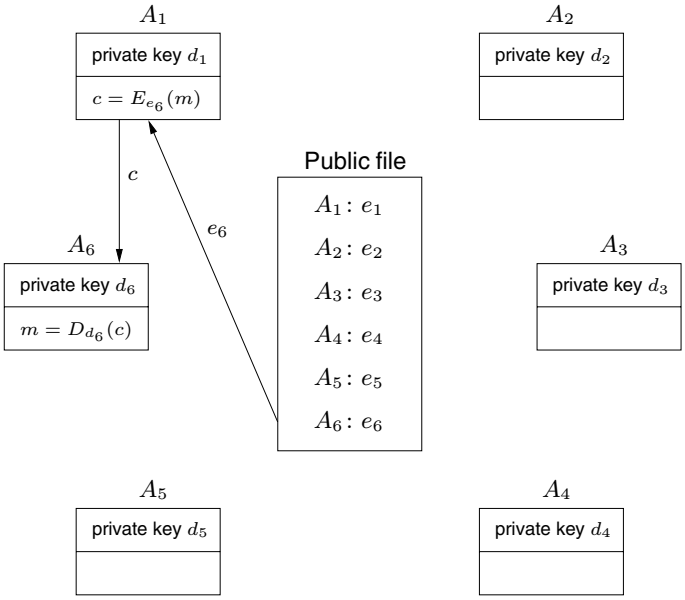


Figure 1.17: *Key management using public-key techniques.*

Advantages of this approach include:

1. No trusted third party is required.
2. The public file could reside with each entity.
3. Only n public keys need to be stored to allow secure communications between any pair of entities, assuming the only attack is that by a passive adversary.

The key management problem becomes more difficult when one must take into account an adversary who is *active* (i.e. an adversary who can alter the public file containing public keys). Figure 1.18 illustrates how an active adversary could compromise the key management scheme given above. (This is directly analogous to the attack in §1.8.2.) In the figure, the adversary alters the public file by replacing the public key e_6 of entity A_6 by the adversary's public key e^*. Any message encrypted for A_6 using the public key from the public file can be decrypted by only the adversary. Having decrypted and read the message, the

adversary can now encrypt it using the public key of A_6 and forward the ciphertext to A_6. A_1 however believes that only A_6 can decrypt the ciphertext c.

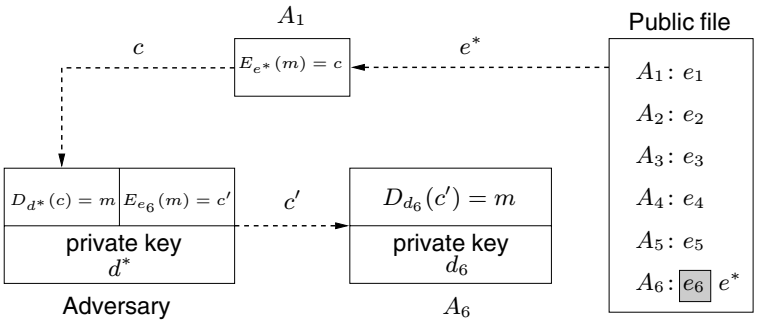


Figure 1.18: *An impersonation of A_6 by an active adversary with public key e^*.*

To prevent this type of attack, the entities may use a TTP to *certify* the public key of each entity. The TTP has a private signing algorithm S_T and a verification algorithm V_T (see §1.6) assumed to be known by all entities. The TTP carefully verifies the identity of each entity, and signs a message consisting of an identifier and the entity's authentic public key. This is a simple example of a *certificate*, binding the identity of an entity to its public key (see §1.11.3). Figure 1.19 illustrates the network under these conditions. A_1 uses the public key of A_6 only if the certificate signature verifies successfully.

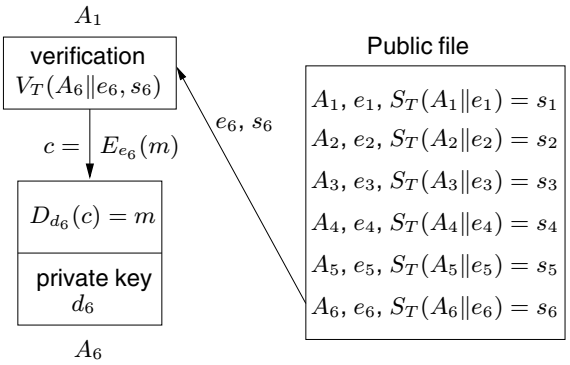


Figure 1.19: *Authentication of public keys by a TTP. $\|$ denotes concatenation.*

Advantages of using a TTP to maintain the integrity of the public file include:

1. It prevents an active adversary from impersonation on the network.
2. The TTP cannot monitor communications. Entities need trust the TTP only to bind identities to public keys properly.
3. Per-communication interaction with the public file can be eliminated if entities store certificates locally.

Even with a TTP, some concerns still remain:

1. If the signing key of the TTP is compromised, all communications become insecure.
2. All trust is placed with one entity.

1.11.3 Trusted third parties and public-key certificates

A trusted third party has been used in §1.8.3 and again here in §1.11. The trust placed on this entity varies with the way it is used, and hence motivates the following classification.

1.65 Definition A TTP is said to be *unconditionally trusted* if it is trusted on all matters. For example, it may have access to the secret and private keys of users, as well as be charged with the association of public keys to identifiers.

1.66 Definition A TTP is said to be *functionally trusted* if the entity is assumed to be honest and fair but it does not have access to the secret or private keys of users.

§1.11.1 provides a scenario which employs an unconditionally trusted TTP. §1.11.2 uses a functionally trusted TTP to maintain the integrity of the public file. A functionally trusted TTP could be used to register or certify users and contents of documents or, as in §1.8.3, as a judge.

Public-key certificates

The distribution of public keys is generally easier than that of symmetric keys, since secrecy is not required. However, the integrity (authenticity) of public keys is critical (recall §1.8.2).

A *public-key certificate* consists of a *data part* and a *signature part*. The data part consists of the name of an entity, the public key corresponding to that entity, possibly additional relevant information (e.g., the entity's street or network address, a validity period for the public key, and various other attributes). The signature part consists of the signature of a TTP over the data part.

In order for an entity B to verify the authenticity of the public key of an entity A, B must have an authentic copy of the public signature verification function of the TTP. For simplicity, assume that the authenticity of this verification function is provided to B by non-cryptographic means, for example by B obtaining it from the TTP in person. B can then carry out the following steps:

1. Acquire the public-key certificate of A over some unsecured channel, either from a central database of certificates, from A directly, or otherwise.
2. Use the TTP's verification function to verify the TTP's signature on A's certificate.
3. If this signature verifies correctly, accept the public key in the certificate as A's authentic public key; otherwise, assume the public key is invalid.

Before creating a public-key certificate for A, the TTP must take appropriate measures to verify the identity of A and the fact that the public key to be certificated actually belongs to A. One method is to require that A appear before the TTP with a conventional passport as proof of identity, and obtain A's public key from A in person along with evidence that A knows the corresponding private key. Once the TTP creates a certificate for a party, the trust that all other entities have in the authenticity of the TTP's public key can be used transitively to gain trust in the authenticity of that party's public key, through acquisition and verification of the certificate.

1.12 Pseudorandom numbers and sequences

Random number generation is an important primitive in many cryptographic mechanisms. For example, keys for encryption transformations need to be generated in a manner which is

unpredictable to an adversary. Generating a random key typically involves the selection of random numbers or bit sequences. Random number generation presents challenging issues. A brief introduction is given here with details left to Chapter 5.

Often in cryptographic applications, one of the following steps must be performed:

(i) From a finite set of n elements (e.g., $\{1, 2, \ldots, n\}$), select an element at random.

(ii) From the set of all sequences (strings) of length m over some finite alphabet $\mathcal{A}$ of n symbols, select a sequence at random.

(iii) Generate a random sequence (string) of symbols of length m over a set of n symbols.

It is not clear what exactly it means to *select at random* or *generate at random*. Calling a number random without a context makes little sense. Is the number 23 a random number? No, but if 49 identical balls labeled with a number from 1 to 49 are in a container, and this container mixes the balls uniformly, drops one ball out, and this ball happens to be labeled with the number 23, then one would say that 23 was generated randomly from a uniform distribution. The *probability* that 23 drops out is 1 in 49 or $\frac{1}{49}$.

If the number on the ball which was dropped from the container is recorded and the ball is placed back in the container and the process repeated 6 times, then a random sequence of length 6 defined on the alphabet $\mathcal{A} = \{1, 2, \ldots, 49\}$ will have been generated. What is the chance that the sequence $17, 45, 1, 7, 23, 35$ occurs? Since each element in the sequence has probability $\frac{1}{49}$ of occuring, the probability of the sequence $17, 45, 1, 7, 23, 35$ occurring is

$$\frac{1}{49} \times \frac{1}{49} \times \frac{1}{49} \times \frac{1}{49} \times \frac{1}{49} \times \frac{1}{49} = \frac{1}{13841287201}.$$

There are precisely 13841287201 sequences of length 6 over the alphabet $\mathcal{A}$. If each of these sequences is written on one of 13841287201 balls and they are placed in the container (first removing the original 49 balls) then the chance that the sequence given above drops out is the same as if it were generated one ball at a time. Hence, (ii) and (iii) above are essentially the same statements.

Finding good methods to generate random sequences is difficult.

1.67 Example (*random sequence generator*) To generate a random sequence of 0's and 1's, a coin could be tossed with a head landing up recorded as a 1 and a tail as a 0. It is assumed that the coin is *unbiased*, which means that the probability of a 1 on a given toss is exactly $\frac{1}{2}$. This will depend on how well the coin is made and how the toss is performed. This method would be of little value in a system where random sequences must be generated quickly and often. It has no practical value other than to serve as an example of the idea of random number generation. □

1.68 Example (*random sequence generator*) A *noise diode* may be used to produce random binary sequences. This is reasonable if one has some way to be convinced that the probability that a 1 will be produced on any given trial is $\frac{1}{2}$. Should this assumption be false, the sequence generated would not have been selected from a uniform distribution and so not all sequences of a given length would be equally likely. The only way to get some feeling for the reliability of this type of random source is to carry out statistical tests on its output. These are considered in Chapter 5. If the diode is a source of a uniform distribution on the set of all binary sequences of a given length, it provides an effective way to generate random sequences. □

Since most *true sources* of random sequences (if there is such a thing) come from *physical means*, they tend to be either costly or slow in their generation. To overcome these

problems, methods have been devised to construct *pseudorandom sequences* in a deterministic manner from a shorter random sequence called a *seed*. The pseudorandom sequences appear to be generated by a truly random source to anyone not knowing the method of generation. Often the generation algorithm is known to all, but the seed is unknown except by the entity generating the sequence. A plethora of algorithms has been developed to generate pseudorandom bit sequences of various types. Many of these are completely unsuitable for cryptographic purposes and one must be cautious of claims by creators of such algorithms as to the random nature of the output.

1.13 Classes of attacks and security models

Over the years, many different types of attacks on cryptographic primitives and protocols have been identified. The discussion here limits consideration to attacks on encryption and protocols. Attacks on other cryptographic primitives will be given in appropriate chapters.

In §1.11 the roles of an active and a passive adversary were discussed. The attacks these adversaries can mount may be classified as follows:.

1. A *passive attack* is one where the adversary only monitors the communication channel. A passive attacker only threatens confidentiality of data.
2. An *active attack* is one where the adversary attempts to delete, add, or in some other way alter the transmission on the channel. An active attacker threatens data integrity and authentication as well as confidentiality.

A passive attack can be further subdivided into more specialized attacks for deducing plaintext from ciphertext, as outlined in §1.13.1.

1.13.1 Attacks on encryption schemes

The objective of the following attacks is to systematically recover plaintext from ciphertext, or even more drastically, to deduce the decryption key.

1. A *ciphertext-only attack* is one where the adversary (or cryptanalyst) tries to deduce the decryption key or plaintext by only observing ciphertext. Any encryption scheme vulnerable to this type of attack is considered to be completely insecure.
2. A *known-plaintext attack* is one where the adversary has a quantity of plaintext and corresponding ciphertext. This type of attack is typically only marginally more difficult to mount.
3. A *chosen-plaintext attack* is one where the adversary chooses plaintext and is then given corresponding ciphertext. Subsequently, the adversary uses any information deduced in order to recover plaintext corresponding to previously unseen ciphertext.
4. An *adaptive chosen-plaintext attack* is a chosen-plaintext attack wherein the choice of plaintext may depend on the ciphertext received from previous requests.
5. A *chosen-ciphertext attack* is one where the adversary selects the ciphertext and is then given the corresponding plaintext. One way to mount such an attack is for the adversary to gain access to the equipment used for decryption (but not the decryption key, which may be securely embedded in the equipment). The objective is then to be able, without access to such equipment, to deduce the plaintext from (different) ciphertext.

6. An *adaptive chosen-ciphertext attack* is a chosen-ciphertext attack where the choice of ciphertext may depend on the plaintext received from previous requests.

Most of these attacks also apply to digital signature schemes and message authentication codes. In this case, the objective of the attacker is to forge messages or MACs, as discussed in Chapters 11 and 9, respectively.

1.13.2 Attacks on protocols

The following is a partial list of attacks which might be mounted on various protocols. Until a protocol is proven to provide the service intended, the list of possible attacks can never be said to be complete.

1. *known-key attack.* In this attack an adversary obtains some keys used previously and then uses this information to determine new keys.
2. *replay.* In this attack an adversary records a communication session and replays the entire session, or a portion thereof, at some later point in time.
3. *impersonation.* Here an adversary assumes the identity of one of the legitimate parties in a network.
4. *dictionary.* This is usually an attack against passwords. Typically, a password is stored in a computer file as the image of an unkeyed hash function. When a user logs on and enters a password, it is hashed and the image is compared to the stored value. An adversary can take a list of probable passwords, hash all entries in this list, and then compare this to the list of true encrypted passwords with the hope of finding matches.
5. *forward search.* This attack is similar in spirit to the dictionary attack and is used to decrypt messages. An example of this method was cited in Example 1.60.
6. *interleaving attack.* This type of attack usually involves some form of impersonation in an authentication protocol (see §12.9.1).

1.13.3 Models for evaluating security

The security of cryptographic primitives and protocols can be evaluated under several different models. The most practical security metrics are computational, provable, and ad hoc methodology, although the latter is often dangerous. The confidence level in the amount of security provided by a primitive or protocol based on computational or ad hoc security increases with time and investigation of the scheme. However, time is not enough if few people have given the method careful analysis.

(i) Unconditional security

The most stringent measure is an information-theoretic measure – whether or not a system has *unconditional security*. An adversary is assumed to have unlimited computational resources, and the question is whether or not there is enough information available to defeat the system. Unconditional security for encryption systems is called *perfect secrecy*. For perfect secrecy, the uncertainty in the plaintext, after observing the ciphertext, must be equal to the a priori uncertainty about the plaintext – observation of the ciphertext provides no information whatsoever to an adversary.

A necessary condition for a symmetric-key encryption scheme to be unconditionally secure is that the key be at least as long as the message. The one-time pad (§1.5.4) is an example of an unconditionally secure encryption algorithm. In general, encryption schemes

do not offer perfect secrecy, and each ciphertext character observed decreases the theoretical uncertainty in the plaintext and the encryption key. Public-key encryption schemes cannot be unconditionally secure since, given a ciphertext c, the plaintext can in principle be recovered by encrypting all possible plaintexts until c is obtained.

(ii) Complexity-theoretic security

An appropriate model of computation is defined and adversaries are modeled as having polynomial computational power. (They mount attacks involving time and space polynomial in the size of appropriate security parameters.) A proof of security relative to the model is then constructed. An objective is to design a cryptographic method based on the weakest assumptions possible anticipating a powerful adversary. Asymptotic analysis and usually also worst-case analysis is used and so care must be exercised to determine when proofs have practical significance. In contrast, polynomial attacks which are feasible under the model might, in practice, still be computationally infeasible.

Security analysis of this type, although not of practical value in all cases, may nonetheless pave the way to a better overall understanding of security. Complexity-theoretic analysis is invaluable for formulating fundamental principles and confirming intuition. This is like many other sciences, whose practical techniques are discovered early in the development, well before a theoretical basis and understanding is attained.

(iii) Provable security

A cryptographic method is said to be *provably secure* if the difficulty of defeating it can be shown to be essentially as difficult as solving a well-known and *supposedly* difficult (typically number-theoretic) problem, such as integer factorization or the computation of discrete logarithms. Thus, "provable" here means provable subject to assumptions.

This approach is considered by some to be as good a practical analysis technique as exists. Provable security may be considered part of a special sub-class of the larger class of computational security considered next.

(iv) Computational security

This measures the amount of computational effort required, by the best currently-known methods, to defeat a system; it must be assumed here that the system has been well-studied to determine which attacks are relevant. A proposed technique is said to be *computationally secure* if the perceived level of computation required to defeat it (using the best attack known) exceeds, by a comfortable margin, the computational resources of the hypothesized adversary.

Often methods in this class are related to hard problems but, unlike for provable security, no proof of equivalence is known. Most of the best known public-key and symmetric-key schemes in current use are in this class. This class is sometimes also called *practical security*.

(v) Ad hoc security

This approach consists of any variety of convincing arguments that every successful attack requires a resource level (e.g., time and space) greater than the fixed resources of a perceived adversary. Cryptographic primitives and protocols which survive such analysis are said to have *heuristic security*, with security here typically in the computational sense.

Primitives and protocols are usually designed to counter standard attacks such as those given in §1.13. While perhaps the most commonly used approach (especially for protocols), it is, in some ways, the least satisfying. Claims of security generally remain questionable and unforeseen attacks remain a threat.

1.13.4 Perspective for computational security

To evaluate the security of cryptographic schemes, certain quantities are often considered.

1.69 Definition The *work factor* W_d is the minimum amount of work (measured in appropriate units such as elementary operations or clock cycles) required to compute the private key d given the public key e, or, in the case of symmetric-key schemes, to determine the secret key k. More specifically, one may consider the work required under a ciphertext-only attack given n ciphertexts, denoted $W_d(n)$.

If W_d is t years, then for sufficiently large t the cryptographic scheme is, for all practical purposes, a secure system. To date no public-key system has been found where one can prove a sufficiently large lower bound on the work factor W_d. The best that is possible to date is to rely on the following as a basis for security.

1.70 Definition The *historical work factor* $\overline{W_d}$ is the minimum amount of work required to compute the private key d from the public key e using the best known algorithms at a given point in time.

The historical work factor $\overline{W_d}$ varies with time as algorithms and technology improve. It corresponds to computational security, whereas W_d corresponds to the true security level, although this typically cannot be determined.

How large is large?

§1.4 described how the designer of an encryption system tries to create a scheme for which the best approach to breaking it is through exhaustive search of the key space. The key space must then be large enough to make an exhaustive search completely infeasible. An important question then is "How large is large?". In order to gain some perspective on the magnitude of numbers, Table 1.2 lists various items along with an associated magnitude.

Reference	Magnitude
Seconds in a year	$\approx 3 \times 10^7$
Age of our solar system (years)	$\approx 6 \times 10^9$
Seconds since creation of solar system	$\approx 2 \times 10^{17}$
Clock cycles per year, 50 MHz computer	$\approx 1.6 \times 10^{15}$
Binary strings of length 64	$2^{64} \approx 1.8 \times 10^{19}$
Binary strings of length 128	$2^{128} \approx 3.4 \times 10^{38}$
Binary strings of length 256	$2^{256} \approx 1.2 \times 10^{77}$
Number of 75-digit prime numbers	$\approx 5.2 \times 10^{72}$
Electrons in the universe	$\approx 8.37 \times 10^{77}$

Table 1.2: *Reference numbers comparing relative magnitudes.*

Some powers of 10 are referred to by prefixes. For example, high-speed modern computers are now being rated in terms of *teraflops* where a teraflop is 10^{12} floating point operations per second. Table 1.3 provides a list of commonly used prefixes.

Prefix	Symbol	Magnitude
exa	E	10^{18}
peta	P	10^{15}
tera	T	10^{12}
giga	G	10^{9}
mega	M	10^{6}
kilo	k	10^{3}
hecto	h	10^{2}
deca	da	10

Prefix	Symbol	Magnitude
deci	d	10^{-1}
centi	c	10^{-2}
milli	m	10^{-3}
micro	μ	10^{-6}
nano	n	10^{-9}
pico	p	10^{-12}
femto	f	10^{-15}
atto	a	10^{-18}

Table 1.3: *Prefixes used for various powers of 10.*

1.14 Notes and further references

§1.1

Kahn [648] gives a thorough, comprehensive, and non-technical history of cryptography, published in 1967. Feistel [387] provides an early exposition of block cipher ideas. The original specification of DES is the 1977 U.S. Federal Information Processing Standards Publication 46 [396]. Public-key cryptography was introduced by Diffie and Hellman [345]. The first concrete realization of a public-key encryption scheme was the knapsack scheme by Merkle and Hellman [857]. The RSA public-key encryption and signature scheme is due to Rivest, Shamir, and Adleman [1060], while the ElGamal public-key encryption and signature schemes are due to ElGamal [368]. The two digital signature standards, ISO/IEC 9796 [596] and the Digital Signature Standard [406], are discussed extensively in Chapter 11.

Cryptography has used specialized areas of mathematics such as number theory to realize very practical mechanisms such as public-key encryption and digital signatures. Such usage was not conceived as possible a mere twenty years ago. The famous mathematician, Hardy [539], went as far as to boast about its lack of utility:

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

§1.2

This section was inspired by the foreword to the book *Contemporary Cryptology, The Science of Information Integrity*, edited by Simmons [1143]. The handwritten signature came into the British legal system in the seventeenth century as a means to provide various functions associated with information security. See Chapter 9 of Meyer and Matyas [859] for details.

This book only considers cryptography as it applies to information in digital form. Chapter 9 of Beker and Piper [84] provides an introduction to the encryption of analogue signals, in particular, speech. Although in many cases physical means are employed to facilitate privacy, cryptography plays the major role. Physical means of providing privacy include fiber optic communication links, spread spectrum technology, TEMPEST techniques, and

tamper-resistant hardware. *Steganography* is that branch of information privacy which attempts to obscure the existence of data through such devices as invisible inks, secret compartments, the use of subliminal channels, and the like. Kahn [648] provides an historical account of various steganographic techniques.

Excellent introductions to cryptography can be found in the articles by Diffie and Hellman [347], Massey [786], and Rivest [1054]. A concise and elegant way to describe cryptography was given by Rivest [1054]: *Cryptography is about communication in the presence of adversaries*. The taxonomy of cryptographic primitives (Figure 1.1) was derived from the classification given by Bosselaers, Govaerts, and Vandewalle [175].

§1.3

The theory of functions is fundamental in modern mathematics. The term *range* is often used in place of image of a function. The latter, being more descriptive, is preferred. An alternate term for one-to-one is *injective*; an alternate term for onto is *surjective*.

One-way functions were introduced by Diffie and Hellman [345]. A more extensive history is given on page 377. Trapdoor one-way functions were first postulated by Diffie and Hellman [345] and independently by Merkle [850] as a means to obtain public-key encryption schemes; several candidates are given in Chapter 8.

§1.4

The basic concepts of cryptography are treated quite differently by various authors, some being more technical than others. Brassard [192] provides a concise, lucid, and technically accurate account. Schneier [1094] gives a less technical but very accessible introduction. Salomaa [1089], Stinson [1178], and Rivest [1054] present more mathematical approaches. Davies and Price [308] provide a very readable presentation suitable for the practitioner.

The comparison of an encryption scheme to a resettable combination lock is from Diffie and Hellman [347]. Kerckhoffs' desiderata [668] were originally stated in French. The translation stated here is given in Kahn [648]. Shannon [1121] also gives desiderata for encryption schemes.

§1.5

Symmetric-key encryption has a very long history, as recorded by Kahn [648]. Most systems invented prior to the 1970s are now of historical interest only. Chapter 2 of Denning [326] is also a good source for many of the more well known schemes such as the Caesar cipher, Vigenère and Beaufort ciphers, rotor machines (Enigma and Hagelin), running key ciphers, and so on; see also Davies and Price [308] and Konheim [705]. Beker and Piper [84] give an indepth treatment, including cryptanalysis of several of the classical systems used in World War II. Shannon's paper [1121] is considered the seminal work on secure communications. It is also an excellent source for descriptions of various well-known historical symmetric-key ciphers.

Simple substitution and transposition ciphers are the focus of §1.5. Hill ciphers [557], a class of substitution ciphers which substitute blocks using matrix methods, are covered in Example 7.52. The idea of confusion and diffusion (Remark 1.36) was introduced by Shannon [1121].

Kahn [648] gives 1917 as the date when Vernam discovered the cipher which bears Vernam's name, however, Vernam did not publish the result until 1926 [1222]; see page 274 for further discussion. Massey [786] states that reliable sources have suggested that the Moscow-Washington hot-line (channel for very high level communications) is no longer secured with a one-time pad, which has been replaced by a symmetric-key cipher requiring a much shorter key. This change would indicate that confidence and understanding in the

ability to construct very strong symmetric-key encryption schemes exists. The one-time pad seems to have been used extensively by Russian agents operating in foreign countries. The highest ranking Russian agent ever captured in the United States was Rudolph Abel. When apprehended in 1957 he had in his possession a booklet the size of a postage stamp ($1\frac{7}{8} \times \frac{7}{8} \times \frac{7}{8}$ inches) containing a one-time key; see Kahn [648, p.664].

§1.6

The concept of a digital signature was introduced by Diffie and Hellman [345] and independently by Merkle [850]. The first practical realization of a digital signature scheme appeared in the paper by Rivest, Shamir, and Adleman [1060]. Rabin [1022] (see also [1023]) also claims to have independently discovered RSA but did not publish the result.

Most introductory sources for digital signatures stress digital signatures with message recovery coming from a public-key encryption system. Mitchell, Piper, and Wild [882] give a good general treatment of the subject. Stinson [1178] provides a similar elementary but general introduction. Chapter 11 generalizes the definition of a digital signature by allowing randomization. The scheme described in §1.8 is referred to as *deterministic*. Many other types of digital signatures with specific properties have been created, such as blind signatures, undeniable signatures, and failstop signatures (see Chapter 11).

§1.7

Much effort has been devoted to developing a theory of authentication. At the forefront of this is Simmons [1144], whose contributions are nicely summarized by Massey [786]. For a more concrete example of the necessity for authentication without secrecy, see the article by Simmons [1146].

§1.8

1976 marked a major turning point in the history of cryptography. In several papers that year, Diffie and Hellman introduced the idea of public-key cryptography and gave concrete examples of how such a scheme might be realized. The first paper on public-key cryptography was "Multiuser cryptographic techniques" by Diffie and Hellman [344], presented at the National Computer Conference in June of 1976. Although the authors were not satisfied with the examples they cited, the concept was made clear. In their landmark paper, Diffie and Hellman [345] provided a more comprehensive account of public-key cryptography and described the first viable method to realize this elegant concept. Another good source for the early history and development of the subject is Diffie [343]. Nechvatal [922] also provides a broad survey of public-key cryptography.

Merkle [849, 850] independently discovered public-key cryptography, illustrating how this concept could be realized by giving an elegant and ingenious example now commonly referred to as the *Merkle puzzle scheme*. Simmons [1144, p.412] notes the first reported application of public-key cryptography was fielded by Sandia National Laboratories (U.S.) in 1978.

§1.9

Much of the early work on cryptographic hash functions was done by Merkle [850]. The most comprehensive current treatment of the subject is by Preneel [1004].

§1.10

A large number of successful cryptanalytic attacks on systems claiming security are due to protocol failure. An overview of this area is given by Moore [899], including classifications of protocol failures and design principles.

§1.11

One approach to distributing public-keys is the so-called *Merkle channel* (see Simmons [1144, p.387]). Merkle proposed that public keys be distributed over so many independent public channels (newspaper, radio, television, etc.) that it would be improbable for an adversary to compromise all of them.

In 1979 Kohnfelder [702] suggested the idea of using *public-key certificates* to facilitate the distribution of public keys over unsecured channels, such that their authenticity can be verified. Essentially the same idea, but by on-line requests, was proposed by Needham and Schroeder (ses Wilkes [1244]).

A provably secure key agreement protocol has been proposed whose security is based on the Heisenberg uncertainty principle of quantum physics. The security of so-called *quantum cryptography* does not rely upon any complexity-theoretic assumptions. For further details on quantum cryptography, consult Chapter 6 of Brassard [192], and Bennett, Brassard, and Ekert [115].

§1.12

For an introduction and detailed treatment of many pseudorandom sequence generators, see Knuth [692]. Knuth cites an example of a complex scheme to generate random numbers which on closer analysis is shown to produce numbers which are far from random, and concludes: *...random numbers should not be generated with a method chosen at random.*

§1.13

The seminal work of Shannon [1121] on secure communications, published in 1949, remains as one of the best introductions to both practice and theory, clearly presenting many of the fundamental ideas including redundancy, entropy, and unicity distance. Various models under which security may be examined are considered by Rueppel [1081], Simmons [1144], and Preneel [1003], among others; see also Goldwasser [476].

References

M. Abadi and R. Needham , “Prudent engineering practice for cryptographic protocols”, DEC SRC report #125, Digital Equipment Corporation, Palo Alto, CA, 1994.

M. Abadi and M.R. Tuttle , “A semantics for a logic of authentication”, Proceedings of the Tenth Annual ACM Symposium on Principles of Distributed Computing, 201–216, 1991.

C. Adams , “Symmetric cryptographic system for data encryption”, U.S.Patent # 5,511,123,23 Apr 1996.

C. Adams , “IDUP and SPKM: Developing public-key-based APIs and mechanisms for communication security services”, Proceedings of the Internet Society Symposium on Network and Distributed System Security, 128–135, IEEE Computer Society Press, 1996.

C. Adams and H. Meijer , “Security-related comments regarding McEliece’spublic-key cryptosystem”, Advances in Cryptology–CRYPTO ’87 (LNCS 293), 224–228, 1988.

C. Adams and H. Meijer , “Security-related comments regarding McEliece’s public-key cryptosystem”, IEEE Transactions on Information Theory, 35 (1989), 454–455. An earlier version appeared in [5].

C. Adams and S.E. Tavares , “Designing S-boxes for ciphers resistant to differential cryptanalysis”, W. Wolfowicz , editor, Proceedings of the 3rd Symposium on State and Progress of Research in Cryptography, *Rome, Italy* , 181–190, 1993.

L.M. Adleman , “A subexponential algorithm for the discrete logarithm problem with applications to cryptography”, Proceedings of the IEEE 20th Annual Symposium on Foundations of Computer Science, 55–60, 1979.

L.M. Adleman , “The function field sieve”, Algorithmic Number Theory (LNCS 877), 108–121, 1994.

L.M. Adleman , “Molecular computation of solutions to combinatorial problems”, Science, 266 (1994), 1021–1024.

L.M. Adleman and J. Demarrais , “A subexponential algorithm for discrete logarithms over all finite fields”, Mathematics of Computation, 61 (1993), 1–15.

L.M. Adleman , J. Demarrais , and M.-D. Huang , “A subexponential algorithm for discrete logarithms over the rational subgroup of the Jacobians of large genus hyperelliptic curves over finite fields”, Algorithmic Number Theory (LNCS 877), 28–40, 1994.

L.M. Adleman and M.-D. A. Huang , Primality Testing and Abelian Varieties Over Finite Fields, Springer-Verlag, Berlin, 1992.

L.M. Adleman and H.W. Lenstra Jr. , “Finding irreducible polynomials over finite fields”, Proceedings of the 18th Annual ACM Symposium on Theory of Computing, 350–355, 1986.

L.M. Adleman and K.S. Mccurley , “Open problems in number theoretic complexity, II”, Algorithmic Number Theory (LNCS 877), 291–322, 1994.

L.M. Adleman , C. Pomerance , and R.S. Rumely , “On distinguishing prime numbers from composite numbers”, Annals of Mathematics, 117 (1983), 173–206.

G.B. Agnew , “Random sources for cryptographic systems”, Advances in Cryptology–EUROCRYPT ’87 (LNCS 304), 77–81, 1988.

G.B. Agnew , R.C. Mullin , I.M. Onyszchuk , and S.A. Vanstone , “An implementation for a fast public-key cryptosystem”, Journal of Cryptology, 3 (1991), 63–79.

G.B. Agnew , R.C. Mullin , and S.A. Vanstone , “Improved digital signature scheme based on discrete exponentiation”, Electronics Letters, 26 (July 5, 1990), 1024–1025.

S.G. Akl , “On the security of compressed encodings”, Advances in Cryptology–Proceedings of Crypto 83, 209–230, 1984.

N. Alexandris , M. Burmester , V. Chrissikopoulos , and Y. Desmedt , “A secure key distribution system”, W. Wolfowicz , editor, Proceedings of the 3rd Symposium on State and Progress of Research in Cryptography, *Rome, Italy* , 30–34, Feb. 1993.

W. Alexi , B. Chor , O. Goldreich , and C.P. Schnorr , “RSA/Rabin bits are 1 2 + 1 /poly(log n) secure”, Proceedings of the IEEE 25th Annual Symposium on Foundations of Computer Science, 449–457, 1984.

W. Alexi , B. Chor , O. Goldreich , and C.P. Schnorr , “RSA and Rabin functions: Certain parts are as hard as the whole”, SIAM Journal on Computing, 17 (1988), 194–209. An earlier version appeared in [22].

W.R. Alford , A. Granville , and C. Pomerance , “There are infinitely many Carmichael numbers”, Annals of Mathematics, 140 (1994), 703–722.

H. Amirazizi and M. Hellman , “Time-memory-processor trade-offs”, IEEE Transactions on Information Theory, 34 (1988), 505–512.

R. Anderson , “Practical RSA trapdoor”, Electronics Letters, 29 (May 27, 1993), 995.

R. Anderson , “The classification of hash functions”, P.G. Farrell , editor, Codes and Cyphers: Cryptography and Coding IV, 83–93, Institute of Mathematics & Its Applications (IMA), 1995.

R. Anderson , “On Fibonacci keystream generators”, B. Preneel , editor, Fast Software Encryption, Second International Workshop (LNCS 1008), 346–352, Springer-Verlag, 1995.

R. Anderson , “Searching for the optimum correlation attack”, B. Preneel , editor, Fast Software Encryption, Second International Workshop (LNCS 1008), 137–143, Springer-Verlag, 1995.

R. Anderson and E. Biham , “Two practical and provably secure block ciphers: BEAR and LION”, D. Gollmann , editor, Fast Software Encryption, Third International Workshop (LNCS 1039), 113–120, Springer- Verlag, 1996.

R. Anderson and R. Needham , “Robustness principles for public key protocols”, Advances in Cryptology–CRYPTO ’95 (LNCS 963), 236–247, 1995.

N.C. Ankeny , “The least quadratic non residue”, Annals of Mathematics, 55 (1952), 65–72.

ANSI X3.92 , “American National Standard – Data Encryption Algorithm”, American National Standards Institute, 1981.

ANSI X3.106 , “American National Standard for Information Systems – Data Encryption Algorithm – Modes of Operation”, American National Standards Institute, 1983.

ANSI X9.8 , “American National Standard for Financial Services – Banking – Personal Identification Number management and security. Part 1: PIN protection principles and techniques; Part 2: Approved algorithms for PIN encipherment”, ASC X9 Secretariat – American Bankers Association, 1995.

ANSI X9.9 (REVISED) , “American National Standard – Financial institution message authentication (wholesale)”, ASCX9 Secretariat – American Bankers Association, 1986 (replaces X9.9–1982).

ANSI X9.17 , “American National Standard – Financial institution key management (wholesale)”, ASCX9 Secretariat – American Bankers Association, 1985.

ANSI X9.19 , “American National Standard – Financial institution retail message authentication”, ASC X9 Secretariat – American Bankers Association, 1986.

ANSI X9.23 , “American National Standard – Financial institution encryption of wholesale financial messages”, ASC X9 Secretariat – American Bankers Association, 1988.
ANSI X9.24 , “American National Standard for Financial Services – Financial services retail key management”, ASC X9 Secretariat – American Bankers Association, 1992.
ANSI X9.26 , “American National Standard – Financial institution sign-on authentication for wholesale financial transactions”, ASCX9 Secretariat – American Bankers Association, 1990.
ANSI X9.28 , “American National Standard for Financial Services – Financial institution multiple center key management (wholesale)”, ASCX9 Secretariat – American Bankers Association, 1991.
ANSI X9.30 (PART 1) , “American National Standard for Financial Services – Public key cryptography using irreversible algorithms for the financial services industry – Part 1: The digital signature algorithm (DSA)”, ASC X9 Secretariat – American Bankers Association, 1995.
ANSI X9.30 (PART 2) , “American National Standard for Financial Services – Public key cryptography using irreversible algorithms for the financial services industry – Part 2: The secure hash algorithm (SHA)”, ASC X9 Secretariat – American Bankers Association, 1993.
ANSI X9.31 (PART 1) , “American National Standard for Financial Services – Public key cryptography using RSA for the financial services industry – Part 1: The RSA signature algorithm”, draft, 1995.
ANSI X9.31 (PART 2) , “American National Standard for Financial Services – Public key cryptography using RSA for the financial services industry – Part 2: Hash algorithms for RSA”, draft, 1995.
ANSI X9.42 , “Public key cryptography for the financial services industry: Management of symmetric algorithm keys using Diffie-Hellman”, draft, 1995.
ANSI X9.44 , “Public key cryptography using reversible algorithms for the financial services industry: Transport of symmetric algorithm keys using RSA”, draft, 1994.
ANSI X9.45 , “Public key cryptography for the financial services industry – Enhanced management controls using digital signatures and attribute certificates”, draft, 1996.
ANSI X9.52 , “Triple data encryption algorithm modes of operation”, draft, 1996.
ANSI X9.55 , “Public key cryptography for the financial services industry – Extensions to public key certificates and certificate revocation lists”, draft, 1995.
ANSI X9.57 , “Public key cryptography for the financial services industry – Certificate management”, draft, 1995.
K. Aoki and K. Ohta , “Differential-linear cryptanalysis of FEAL-8”, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Science, E79-A (1996), 20–27.
B. Arazi , “Integrating a key distribution procedure into the digital signature standard”, Electronics Letters, 29 (May 27, 1993), 966–967.
B. Arazi , “On primality testing using purely divisionless operations”, The Computer Journal, 37 (1994), 219–222.
F. Arnault , “Rabin-Miller primality test: composite numbers which pass it”, Mathematics of Computation, 64 (1995), 355–361.
A.O.L. Atkin and R.G. Larson , “On a primality test of Solovay and Strassen”, SIAM Journal on Computing, 11 (1982), 789–791.
A.O.L. Atkin and F. Morain , “Elliptic curves and primality proving”, Mathematics of Computation, 61 (1993), 29–68.
D. Atkins , M. Graff , A.K. Lenstra , and P.C. Leyland , “The magic words are SQUEAMISH OSSIFRAGE”, Advances in Cryptology–ASIACRYPT ’94 (LNCS 917), 263–277, 1995.
L. Babai , “Trading group theory for randomness”, Proceedings of the 17th Annual ACM Symposium on Theory of Computing, 421–429, 1985.
L. Babai and S. Moran , “Arthur-Merlin games: a randomized proof system, and a hierarchy of complexity classes”, Journal of Computer and System Sciences, 36 (1988), 254–276.
E. Bach , “Discrete logarithms and factoring”, Report No. UCB/CSD 84/186, Computer Science Division (EECS), University of California, Berkeley, California, 1984.
E. Bach , Analytic Methods in the Analysis and Design of Number-Theoretic Algorithms, MIT Press, Cambridge, Massachusetts, 1985. An ACM Distinguished Dissertation.
E. Bach , “Explicit bounds for primality testing and related problems”, Mathematics of Computation, 55 (1990), 355–380.
E. Bach , “Number-theoretic algorithms”, Annual Review of Computer Science, 4 (1990), 119–172.
E. Bach , “Realistic analysis of some randomized algorithms”, Journal of Computer and System Sciences, 42 (1991), 30–53.
E. Bach , “Toward a theory of Pollard’s rho method”, Information and Computation,90 (1991), 139–155.
E. Bach and J. Shallit , “Factoring with cyclotomic polynomials”, Proceedings of the IEEE 26th Annual Symposium on Foundations of Computer Science, 443–450, 1985.
E. Bach and J. Shallit , “Factoring with cyclotomic polynomials”, Mathematics of Computation, 52 (1989), 201–219. An earlier version appeared in [68].
E. Bach and J. Shallit , Algorithmic Number Theory, Volume I: Efficient Algorithms, MIT Press, Cambridge, Massachusetts, 1996.
E. Bach and J. Sorenson , “Sieve algorithms for perfect power testing”, Algorithmica, 9 (1993), 313–328.
A. Bahreman , “PEMToolKit: Building a top-down certification hierarchy”, Proceedings of the Internet Society Symposium on Network and Distributed System Security, 161–171, IEEE Computer Society Press, 1995.
T. Baritaud , M. Campana , P. Chauvaud , and H. Gilbert , “On the security of the permuted kernel identification scheme”, Advances in Cryptology–CRYPTO ’92 (LNCS 740), 305–311, 1993.
W. Barker , Cryptanalysis of the Hagelin Cryptograph, Aegean Park Press, Laguna Hills, California, 1977.
P. Barrett , “Implementing the Rivest Shamir and Adleman public key encryption algorithm on a standard digital signal processor”, Advances in Cryptology–CRYPTO ’86 (LNCS 263), 311–323, 1987.
R.K. Bauer , T.A. Berson , and R.J. Feiertag , “A key distribution protocol using event markers”, ACM Transactions on Computer Systems, 1 (1983), 249–255.
U. Baum and S. Blackburn , “Clock-controlled pseudorandom generators on finite groups”, B. Preneel , editor, Fast Software Encryption, Second International Workshop (LNCS 1008), 6–21, Springer-Verlag, 1995.
F. Bauspiess and H.-J. Knobloch , “How to keep authenticity alive in a computer network”, Advances in Cryptology–EUROCRYPT ’89 (LNCS 434), 38–46, 1990.
D. Bayer , S. Haber , and W.S. Stornetta , “Improving the efficiency and reliability of digital time-stamping”, R. Capocelli , A. De Santis , and U. Vaccaro , editors, Sequences II: Methods in Communication, Security, and Computer Science, 329–334, Springer-Verlag, 1993.

P. Beauchemin and G. Brassard , “A generalization of Hellman’s extension to Shannon’s approach to cryptography”, Journal of Cryptology, 1 (1988), 129–131.
P. Beauchemin , G. Brassard , C. Crépeau , C. Goutier , and C. Pomerance , “The generation of random numbers that are probably prime”, Journal of Cryptology, 1 (1988), 53–64.
P. Béguin and J.-J. Quisquater , “Secure acceleration of DSS signatures using insecure server”, Advances in Cryptology–ASIACRYPT ’94 (LNCS 917), 249–259, 1995.
A. Beimel and B. Chor , “Interaction in key distribution schemes”, Advances in Cryptology–CRYPTO ’93 (LNCS 773), 444–455, 1994.
H. Beker and F. Piper , Cipher Systems: The Protection of Communications, John Wiley & Sons, New York, 1982.
H. Beker and M. Walker , “Key management for secure electronic funds transfer in a retail environment”, Advances in Cryptology–Proceedings of CRYPTO 84 (LNCS 196), 401–410, 1985.
M. Bellare , R. Canetti , and H. Krawczyk , “Keying hash functions for message authenticaion”, Advances in Cryptology–CRYPTO ’96 (LNCS 1109), 1–15, 1996.
M. Bellare and O. Goldreich , “On defining proofs of knowledge”, Advances in Cryptology–CRYPTO ’92 (LNCS 740), 390–420, 1993.
M. Bellare , O. Goldreich , and S. Goldwasser , “Incremental cryptography: The case of hashing and signing”, Advances in Cryptology–CRYPTO ’94 (LNCS 839), 216–233, 1994.
M. Bellare , O. Goldreich , and S. Goldwasser , “Incremental cryptography and application to virus protection”, Proceedings of the 27th Annual ACM Symposium on Theory of Computing, 45–56, 1995.
M. Bellare , R. Guérin , and P. Rogaway , “XOR MACs: New methods for message authentication using finite pseudorandom functions”, Advances in Cryptology–CRYPTO ’95 (LNCS 963), 15–28, 1995.
M. Bellare , J. Kilian , and P. Rogaway , “The security of cipher block chaining”, Advances in Cryptology–CRYPTO ’94 (LNCS 839), 341–358, 1994.
M. Bellare and S. Micali , “How to sign given any trapdoor function”, Advances in Cryptology–CRYPTO ’88 (LNCS 403), 200–215, 1990.
M. Bellare and P. Rogaway , “Random oracles are practical: a paradigm for designing efficient protocols”, 1st ACM Conference on Computer and Communications Security, 62–73, ACM Press, 1993.
M. Bellare and P. Rogaway , “Entity authentication and key distribution”, Advances in Cryptology–CRYPTO ’93 (LNCS 773), 232–249, 1994.
M. Bellare and P. Rogaway , “Optimal asymmetric encryption”, Advances in Cryptology–EUROCRYPT ’94 (LNCS 950), 92–111, 1995.
M. Bellare and P. Rogaway , “Provably secure session key distribution – the three party case”, Proceedings of the 27th Annual ACM Symposium on Theory of Computing, 57–66, 1995.
M.J. Beller , L.-F. Chang , and Y. YAcobi , “Privacy and authentication on a portable communications system”, IEEE Global Telecommunications Conference, 1922–1927, 1991.
M.J. Beller , L.-F. Chang , and Y. Yacobi , “Security for personal communications services: public-key vs. private key approaches”, The Third IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC’92), 26–31, 1992.
M.J. Beller , L.-F. Chang , and Y. Yacobi , “Privacy and authentication on a portable communications system”, IEEE Journal on Selected Areas in Communications, 11 (1993), 821–829.
M.J. Beller and Y. Yacobi , “Minimal asymmetric authentication and key agreement schemes”, October 1994 unpublished manuscript.
M.J. Beller and Y. Yacobi , “Fully-fledged two-way public key authentication and key agreement for low-cost terminals”, Electronics Letters, 29 (May 27, 1993), 999–1001.
S.M. Bellovin and M. Merritt , “Cryptographic protocol for secure communications”, U.S. Patent # 5,241,599, 31 Aug 1993.
S.M. Bellovin and M. Merritt , “Limitations of the Kerberos authentication system”, Computer Communication Review, 20 (1990), 119–132.
S.M. Bellovin and M. Merritt , “Encrypted key exchange: password-based protocols secure against dictionary attacks”, Proceedings of the 1992 IEEE Computer Society Symposium on Research in Security and Privacy, 72–84, 1992.
S.M. Bellovin and M. Merritt , “Augmented encrypted key exchange: a password-based protocol secure against dictionary attacks and password file compromise”, 1st ACM Conference on Computer and Communications Security, 244–250, ACM Press, 1993.
S.M. Bellovin and M. Merritt , “An attack on the Interlock Protocol when used for authentication”, IEEE Transactions on Information Theory, 40 (1994), 273–275.
I. Ben-Aroya and E. Biham , “Differential cyptanalysis of Lucifer”, Advances in Cryptology–CRYPTO ’93 (LNCS 773), 187–199, 1994.
I. Ben-Aroya and E. Biham , “Differential cryptanalysis of Lucifer”, Journal of Cryptology, 9 (1996), 21–34. An earlier version appeared in [107].
M. Ben-Or , “Probabilistic algorithms in finite fields”, Proceedings of the IEEE 22nd Annual Symposium on Foundations of Computer Science, 394–398, 1981.
J. Benaloh , “Secret sharing homomorphisms: Keeping shares of a secret secret”, Advances in Cryptology–CRYPTO ’86 (LNCS 263), 251–260, 1987.
J. Benaloh and M. De Mare , “One-way accumulators: A decentralized alternative to digital signatures”, Advances in Cryptology–EUROCRYPT ’93 (LNCS 765), 274–285, 1994.
J. Benaloh and J. Leichter , “Generalized secret sharing and monotone functions”, Advances in Cryptology–CRYPTO ’88 (LNCS 403), 27–35, 1990.
S. Bengio , G. Brassard , Y.G. Desmedt , C. Goutier , and J.-J. Quisquater , “Secure implementation of identification systems”, Journal of Cryptology, 4 (1991), 175–183.
C. Bennett , G. Brassard , S. Breidbart , and S. Wiesner , “Quantum cryptography, or unforgeable subway tokens”, Advances in Cryptology–Proceedings of Crypto 82, 267–275, 1983.
C. Bennett , G. Brassard , and A. Ekert , “Quantum cryptography”, Scientific American, special issue (1997), 164–171.
S. Berkovits , “How to broadcast a secret”, Advances in Cryptology–EUROCRYPT ’91 (LNCS 547), 535–541, 1991.
E.R. Berlekamp , “Factoring polynomials over finite fields”, Bell System Technical Journal, 46 (1967), 1853–1859.
E.R. Berlekamp , Algebric Coding Theory, McGraw Hill, New York, 1968.
E.R. Berlekamp , “Factoring polynomials over large finite fields”, Mathematics of Computation,24 (1970), 713–735.
E.R. Berlekamp , R.J. Mceliece , and H.C.A. Van Tilborg , “On the inherent intractability of certain coding problems”, IEEE Transactions on Information Theory,24 (1978), 384–386.

D.J. Bernstein , “Detecting perfect powers in essentially linear time”, preprint, 1995.
D.J. Bernstein and A.K. Lenstra , “A general number field sieve implementation”, A.K. Lenstra and H.W. Lenstra Jr. , editors, The Development of the Number Field Sieve, volume 1554 of *Lecture Notes in Mathematics*, 103–126, Springer-Verlag, 1993.
T. Beth , “Efficient zero-knowledge identification scheme for smart cards”, Advances in Cryptology–EUROCRYPT ’88 (LNCS 330), 77–84, 1988.
T. Beth and Z.-D. Dai , “On the complexity of pseudo-random sequences – or: If you can describe a sequence it can’t be random”, Advances in Cryptology–EUROCRYPT ’89 (LNCS 434), 533–543, 1990.
T. Beth , H.-J. Knobloch , M. Otten , G.J. Simmons , and P. Wichmann , “Towards acceptable key escrow systems”, 2nd ACM Conference on Computer and Communications Security, 51–58, ACM Press, 1994.
T. Beth and F.C. Piper , “The stop-and-go generator”, Advances in Cryptology–Proceedings of EUROCRYPT 84 (LNCS 209), 88–92, 1985.
J. Bierbrauer , T. Johansson , G. Kabatianskii , and B. Smeets , “On families of hash functions via geometric codes and concatenation”, Advances in Cryptology–CRYPTO ’93 (LNCS 773), 331–342, 1994.
E. Biham , “New types of cryptanalytic attacks using related keys”, Advances in Cryptology–EUROCRYPT ’93 (LNCS 765), 398–409, 1994.
E. Biham , “New types of cryptanalytic attacks using related keys”, Journal of Cryptology,7 (1994), 229–246. An earlier version appeared in [128].
E. Biham , “On modes of operation”, R. Anderson , editor, Fast Software Encryption, Cambridge Security Workshop (LNCS 809), 116–120, Springer-Verlag, 1994.
E. Biham , “Cryptanalysis of multiple modes of operation”, Advances in Cryptology–ASIACRYPT ’94 (LNCS 917), 278–292, 1995.
E. Biham , “On Matsui’s linear cryptanalysis”, Advances in Cryptology–EUROCRYPT ’94 (LNCS 950), 341–355, 1995.
E. Biham and A. Biryukov , “How to strengthen DES using existing hardware”, Advances in Cryptology–ASIACRYPT ’94 (LNCS 917), 398–412, 1995.
E. Biham and A. Shamir , “Differential cryptanalysis of DES-like cryptosystems”, Journal of Cryptology, 4 (1991), 3–72. An earlier version appeared in [135].
E. Biham and A. Shamir , “Differential cryptanalysis of DES-like cryptosystems”, Advances in Cryptology–CRYPTO ’90 (LNCS 537), 2–21, 1991.
E. Biham and A. Shamir , “Differential cryptanalysis of Feal and N-Hash”, Advances in Cryptology–EUROCRYPT ’91 (LNCS 547), 1–16, 1991.
E. Biham and A. Shamir , “Differential cryptanalysis of Snefru, Khafre, REDOC-II, LOKI, and Lucifer”, Advances in Cryptology–CRYPTO ’91 (LNCS 576), 156–171, 1992.
E. Biham and A. Shamir , Differential Cryptanalysis of the Data Encryption Standard, Springer-Verlag, New York, 1993.
E. Biham and A. Shamir , “Differential cryptanalysis of the full 16-round DES”, Advances in Cryptology–CRYPTO ’92 (LNCS 740), 487–496, 1993.
R. Bird , I. Gopal , A. Herzberg , P. Janson , S. Kutten , R. Molva , and M. Yung , “Systematic design of two-party authentication protocols”, Advances in Cryptology–CRYPTO ’91 (LNCS 576), 44–61, 1992.
R. Bird , I. Gopal , A. Herzberg , P. Janson , S. Kutten , R. Molva , and M. Yung , “Systematic design of a family of attack-resistant authentication protocols”, IEEE Journal on Selected Areas in Communications, 11 (1993), 679–693.
R. Bird , I. Gopal , A. Herzberg , P. Janson , S. Kutten , R. Molva , and M. Yung , “The KryptoKnight family of lightweight protocols for authentication and key distribution”, IEEE/ACM Transactions on Networking, 3 (1995), 31–41.
S. Blackburn , S. Murphy , and J. Stern , “The cryptanalysis of a public-key implementation of finite group mappings”, Journal of Cryptology, 8 (1995), 157–166.
R. E. Blahut , Principles and Practice of Information Theory, Addison-Wesley, Reading, Massachusetts, 1987.
I.F. Blake , R. Fuji-Hara , R.C. Mullin , and S.A. Vanstone , “Computing logarithms in finite fields of characteristic two”, SIAM Journal on Algebraic and Discrete Methods, 5 (1984), 276–285.
I.F. Blake , S. Gao , and R. Lambert , “Constructive problems for irreducible polynomials over finite fields”, T.A. Gulliver and N.P. Secord , editors, Information Theory and Applications (LNCS 793), 1–23, Springer-Verlag, 1994.
B. Blakley , G.R. Blakley , A.H. Chan , and J. L. Massey , “Threshold schemes with disenrollment”, Advances in Cryptology–CRYPTO ’92 (LNCS 740), 540–548, 1993.
G. Blakley , “Safeguarding cryptographic keys”, Proceedings of AFIPS National Computer Conference, 313–317, 1979.
G. Blakley , “A computer algorithm for calculating the product AB modulo M”, IEEE Transactions on Computers, 32 (1983), 497–500.
G. Blakley and I. Borosh , “Rivest-Shamir-Adleman public key cryptosystems do not always conceal messages”, Computers and Mathematics with Applications,5:3 (1979), 169–178.
G. Blakley and C. Meadows , “Security of ramp schemes”, Advances in Cryptology–Proceedings of CRYPTO 84 (LNCS 196), 242–268, 1985.
M. Blaze , “Protocol failure in the escrowed encryption standard”, 2nd ACM Conference on Computer and Communications Security, 59–67, ACM Press, 1994.
D. Bleichenbacher , “Generating ElGamal signatures without knowing the secret key”, Advances in Cryptology–EUROCRYPT ’96 (LNCS 1070), 10–18, 1996.
D. Bleichenbacher , W. Bosma , and A.K. Lenstra , “Some remarks on Lucas-based cryptosystems”, Advances in Cryptology–CRYPTO’95 (LNCS 963), 386–396, 1995.
D. Bleichenbacher and U. Maurer , “Directed acyclic graphs, one-way functions and digital signatures”, Advances in Cryptology–CRYPTO ’94 (LNCS 839), 75–82, 1994.
U. Blöcher and M. Dichtl , “Fish: A fast software stream cipher”, R. Anderson , editor, Fast Software Encryption, Cambridge Security Workshop (LNCS 809), 41–44, Springer-Verlag, 1994.
R. Blom , “Non-public key distribution”, Advances in Cryptology–Proceedings of Crypto 82, 231–236, 1983.
R. Blom , “An optimal class of symmetric key generation systems”, Advances in Cryptology–Proceedings of EUROCRYPT 84 (LNCS 209), 335–338, 1985.
L. Blum , M. Blum , and M. Shub , “Comparison of two pseudo-random number generators”, Advances in Cryptology–Proceedings of Crypto 82, 61–78, 1983.

L. Blum , M. Blum , and M. Shub , “A simple unpredictable pseudorandom number generator”, SIAM Journal on Computing, 15 (1986), 364–383. An earlier version appeared in [159].
M. Blum , “Independent unbiased coin flips from a correlated biased source: a finite state Markov chain”, Proceedings of the IEEE 25th Annual Symposium on Foundations of Computer Science, 425–433, 1984.
M. Blum , A. De Santis , S. Micali , and G. Persiano , “Noninteractive zero-knowledge”, SIAM Journal on Computing,20 (1991), 1084–1118.
M. Blum , P. Feldman , and S. Micali , “Non-interactive zero-knowledge and its applications”, Proceedings of the 20th Annual ACM Symposium on Theory of Computing, 103–112, 1988.
M. Blum and S. Goldwasser , “An efficient probabilistic public-key encryption scheme which hides all partial information”, Advances in Cryptology–Proceedings of CRYPTO 84 (LNCS 196), 289–299, 1985.
M. Blum and S. Micali , “How to generate cryptographically strong sequences of pseudo random bits”, Proceedings of the IEEE 23rd Annual Symposium on Foundations of Computer Science, 112–117, 1982.
M. Blum and S. Micali , “How to generate cryptographically strong sequences of pseudo-random bits”, SIAM Journal on Computing, 13 (1984), 850–864. An earlier version appeared in [165].
C. Blundo and A. Cresti , “Space requirements for broadcast encryption”, Advances in Cryptology–EUROCRYPT ’94 (LNCS 950), 287–298, 1995.
C. Blundo , A. Cresti , A. De Santis , and U. Vaccaro , “Fully dynamic secret sharing schemes”, Advances in Cryptology–CRYPTO ’93 (LNCS 773), 110–125, 1994.
C. Blundo , A. De Santis , A. Herzberg , S. Kutten , U. Vaccaro , and M. Yung , “Perfectly-secure key distribution for dynamic conferences”, Advances in Cryptology–CRYPTO ’92 (LNCS 740), 471–486, 1993.
R.V. Book and F. Otto , “The verifiability of two-party protocols”, Advances in Cryptology–EUROCRYPT ’85 (LNCS 219), 254–260, 1986.
A. Booth , “A signed binary multiplication technique”, The Quarterly Journal of Mechanics and Applied Mathematics, 4 (1951), 236–240.
J. Bos and D. Chaum , “Provably unforgeable signatures”, Advances in Cryptology–CRYPTO ’92 (LNCS 740), 1–14, 1993.
J. Bos and M. Coster , “Addition chain heuristics”, Advances in Cryptology–CRYPTO ’89 (LNCS 435), 400–407, 1990.
W. Bosma and M.-P. Van Der Hulst , “Faster primality testing”, Advances in Cryptology–EUROCRYPT ’89 (LNCS 434), 652–656, 1990.
A. Bosselaers , R. Govaerts , and J. Vandewalle , “Cryptography within phase I of the EEC-RACE programme”, B. Preneel , R. Govaerts , and J. Vandewalle , editors, Computer Security and Industrial Cryptography: State of the Art and Evolution (LNCS 741), 227–234, Springer-Verlag, 1993.
A. Bosselaers , R. Govaerts , and J. Vandewalle , “Comparison of three modular reduction functions”, Advances in Cryptology–CRYPTO ’93 (LNCS 773), 175–186, 1994.
A. Bosselaers , R. Govaerts , and J. Vandewalle , “Fast hashing on the Pentium”, Advances in Cryptology–CRYPTO ’96 (LNCS 1109), 298–312, 1996.
A. Bosselaers and B. Preneel , editors, Integrity Primitives for Secure Information Systems: Final Report of RACE Integrity Primitives Evaluation RIPE-RACE 1040, LNCS 1007, Springer-Verlag, New York, 1995.
J. Boyar , “Inferring sequences produced by a linear congruential generator missing low-order bits”, Journal of Cryptology, 1 (1989), 177–184.
J. Boyar , “Inferring sequences produced by pseudo-random number generators”, Journal of the Association for Computing Machinery, 36 (1989), 129–141.
J. Boyar , D. Chaum , I.B. Damgård , and T. Pedersen , “Convertible undeniable signatures”, Advances in Cryptology–CRYPTO ’90 (LNCS 537), 189–205, 1991.
C. Boyd , “Digital multisignatures”, H. Beker and F. Piper , editors, Cryptography and Coding, Institute of Mathematics & Its Applications (IMA), 241–246, Clarendon Press, 1989.
C. Boyd and W. Mao , “On a limitation of BAN logic”, Advances in Cryptology–EUROCRYPT ’93 (LNCS 765), 240–247, 1994.
B.O. Brachtl , D. Coppersmith , M.M. Hyden , S.M. Matyas Jr., C.H.W. Meyer , J. Oseas , S. Pilpel , and M. Schilling , “Data authentication using modification detection codes based on a public one-way encryption function”, U.S. Patent #4,908,861, 13 Mar 1990.
S. Brands , “Restrictive blinding of secret-key certificates”, Advances in Cryptology–EUROCRYPT ’95 (LNCS 921), 231–247, 1995.
J. Brandt and I. Damgård , “On generation of probable primes by incremental search”, Advances in Cryptology–CRYPTO ’92 (LNCS 740), 358–370, 1993.
J. Brandt , I. Damgård , and P. Landrock , “Speeding up prime number generation”, Advances in Cryptology–ASIACRYPT ’91 (LNCS 739), 440–449, 1993.
J. Brandt , I. Damgård , P. Landrock , and T. Pedersen , “Zero-knowledge authentication scheme with secret key exchange”, Advances in Cryptology–CRYPTO ’88 (LNCS 403), 583–588, 1990.
D.K. Branstad , “Encryption protection in computer data communications”, Proceedings of the 4th Data Communications Symposium (Quebec), 8.1–8.7, IEEE, 1975.
G. Brassard , “A note on the complexity of cryptography”, IEEE Transactions on Information Theory, 25 (1979), 232–233.
G. Brassard , “On computationally secure authentication tags requiring short secret shared keys”, Advances in Cryptology–Proceedings of Crypto 82, 79–86, 1983.
G. Brassard , Modern Cryptology: A Tutorial, LNCS 325, Springer-Verlag, New York, 1988.
G. Brassard , D. Chaum , and C. Crépeau , “Minimum disclosure proofs of knowledge”, Journal of Computer and System Sciences, 37 (1988), 156–189.
G. Brassard and C. Crépeau , “Zero-knowledge simulation of Boolean circuits”, Advances in Cryptology–CRYPTO ’86 (LNCS 263), 223–233, 1987.
G. Brassard and C. Crepeau , “Sorting out zero-knowledge”, Advances in Cryptology–EUROCRYPT ’89 (LNCS 434), 181–191, 1990.
R.P. Brent , “An improved Monte Carlo factorization algorithm”, BIT, 20 (1980), 176–184.
R.P. Brent and J.M. Pollard , “Factorization of the eighth Fermat number”, Mathematics of Computation, 36 (1981), 627–630.
D.M. Bressoud , Factorization and Primality Testing, Springer-Verlag, New York, 1989.
E.F. Brickell , “A fast modular multiplication algorithm with applications to two key cryptography”, Advances in Cryptology–Proceedings of Crypto 82, 51–60, 1983.

E.F. Brickell , “Breaking iterated knapsacks”, Advances in Cryptology–Proceedings of CRYPTO 84 (LNCS 196), 342–358, 1985.
E.F. Brickell , “The cryptanalysis of knapsack cryptosystems”, R.D. Ringeisen and F.S. Roberts , editors, Applications of Discrete Mathematics, 3–23, SIAM, 1988.
E.F. Brickell and J.M. Delaurentis , “An attack on a signature scheme proposed by Okamoto and Shiraishi”, Advances in Cryptology–CRYPTO ’85 (LNCS 218), 28–32, 1986.
E.F. Brickell , D.M. Gordon , and K.S. Mccurley , “Method for exponentiating in cryptographic systems”, U.S. Patent # 5,299,262, 29 Mar 1994.
E.F. Brickell , D.M. Gordon , K.S. Mccurley , and D.B. Wilson , “Fast exponentiation with precomputation”, Advances in Cryptology–EUROCRYPT ’92 (LNCS 658), 200–207, 1993.
E.F. Brickell , P.J. Lee , and Y. Yacobi , “Secure audio teleconference”, Advances in Cryptology–CRYPTO ’87 (LNCS 293), 418–426, 1988.
E.F. Brickell and K.S. Mccurley , “An interactive identification scheme based on discrete logarithms and factoring”, Advances in Cryptology–EUROCRYPT ’90 (LNCS 473), 63–71, 1991.
E.F. Brickell and K.S. Mccurley , “An interactive identification scheme based on discrete logarithms and factoring”, Journal of Cryptology, 5 (1992), 29–39. An earlier version appeared in [206].
E.F. Brickell and A.M. Odlyzko , “Cryptanalysis: A survey of recent results”, Proceedings of the IEEE, 76 (1988), 578–593.
E.F. Brickell and A.M. Odlyzko , “Cryptanalysis: A survey of recent results”, G.J. Simmons , editor, Contemporary Cryptology: The Science of Information Integrity, 501–540, IEEE Press, 1992. An earlier version appeared in [208].
J. Brillhart , D. Lehmer , and J. Selfridge , “New primality criteria and factorizations of 2m ± 1”, Mathematics of Computation, 29 (1975), 620–647.
J. Brillhart , D. Lehmer , J. Selfridge , B. Tuckerman , and S. Wagstaff Jr. , Factorizations of bn ± 1, b = 2, 3, 5, 6, 7, 10,11,12 up to High Powers, volume 22 of Contemporary Mathematics, American Mathematical Society, Providence, Rhode Island, 2nd edition, 1988.
J. Brillhart and J. Selfridge , “Some factorizations of 2n ± 1 and related results”, Mathematics of Computation, 21 (1967), 87–96.
D. Brillinger , Time Series: Data Analysis and Theory, Holden-Day, San Francisco, 1981.
L. Brown , M. Kwan , J. Pieprzyk , and J. Seberry , “Improving resistance to differential cryptanalysis and the redesign of LOKI”, Advances in Cryptology–ASIACRYPT ’91 (LNCS 739), 36–50, 1993.
L. Brown , J. Pieprzyk , and J. Seberry , “LOKI – a cryptographic primitive for authentication and secrecy applications”, Advances in Cryptology–AUSCRYPT ’90 (LNCS 453), 229–236, 1990.
J. Buchmann and S. Düllmann , “On the computation of discrete logarithms in class groups”, Advances in Cryptology–CRYPTO ’90 (LNCS 537), 134–139, 1991.
J. Buchmann , J. Loho , and J. Zayer , “An implementation of the general number field sieve”, Advances in Cryptology–CRYPTO ’93 (LNCS 773), 159–165, 1994.
J. Buchmann and H. C. Williams , “A key-exchange system based on imaginary quadratic fields”, Journal of Cryptology,1 (1988), 107–118.
J. P. Buhler , H. W. Lenstra Jr., and C. Pomerance , “Factoring integers with the number field sieve”, A.K. Lenstra and H.W. Lenstra Jr. , editors, The Development of the Number Field Sieve, volume 1554 of Lecture Notes in Mathematics, 50–94, Springer-Verlag, 1993.
M. Burmester , “On the risk of opening distributed keys”, Advances in Cryptology–CRYPTO ’94 (LNCS 839), 308–317, 1994.
M. Burmester and Y. Desmedt , “Remarks on soundness of proofs”, Electronics Letters, 25 (October 26, 1989), 1509–1511.
M. Burmester and Y. Desmedt “A secure and efficient conference key distribution system”, Advances in Cryptology–EUROCRYPT ’94 (LNCS 950), 275–286, 1995.
M. Burmester , Y. Desmedt , F. Piper , and M. Walker , “A general zero-knowledge scheme”, Advances in Cryptology–EUROCRYPT ’89 (LNCS 434), 122–133, 1990.
M. Burrows , M. Abadi , and R. Needham , “A logic of authentication”, Proceedings of the Royal Society of London Series A: Mathematical and Physical Sciences, 246 (1989), 233–271. Preliminary version appeared as 1989 version of [227].
M. Burrows , M. Abadi , and R. Needham , “A logic of authentication”, Proceedings of the 12th Annual ACM Symposium on Operating Systems Principles, 1–13, 1989.
M. Burrows , M. Abadi , and R. Needham , “A logic of authentication”, ACM Transactions on Computer Systems, 8 (1990), 18–36.
M. Burrows , M. Abadi , and R. Needham , “A logic of authentication”, DEC SRC report #39, Digital Equipment Corporation, Palo Alto, CA, Feb. 1989. Revised Feb. 1990.
J.L. Camenisch , J.-M. Piveteau , and M.A. Stadler , “Blind signatures based on the discrete logarithm problem”, Advances in Cryptology–EUROCRYPT ’94 (LNCS 950), 428–432, 1995.
K. W. Campbell and M.J. Wiener , “DES is not a group”, Advances in Cryptology–CRYPTO ’92 (LNCS 740), 512–520, 1993.
C.M. Campbell Jr. , “Design and specification of cryptographic capabilities”, D.K. Branstad , editor, Computer security and the Data Encryption Standard, 54–66, NBS Special Publication 500–27, U.S. Department of Commerce, National Bureau of Standards, Washington, D.C., 1977.
E.R. Canfield , P. Erdös , and C. Pomerance , “On a problem of Oppenheim concerning ’Factorisatio Numerorum’”, Journal of Number Theory, 17 (1983), 1–28.
D.G. Cantor and H. Zassenhaus , “A new algorithm for factoring polynomials over finite fields”, Mathematics of Computation,36 (1981), 587–592.
J.L. Carter and M.N. Wegman , “Universal classes of hash functions”, Proceedings of the 9th Annual ACM Symposium on Theory of Computing, 106–112, 1977.
J.L. Carter and M.N. Wegman , “Universal classes of hash functions”, Journal of Computer and System Sciences,18 (1979), 143–154. An earlier version appeared in [233].
F. Chabaud , “On the security of some cryptosystems based on error-correcting codes”, Advances in Cryptology–EUROCRYPT ’94 (LNCS 950), 131–139, 1995.
G. J. Chaitin , “On the length of programs for computing finite binary sequences”, Journal of the Association for Computing Machinery, 13 (1966), 547–569.
W.G. CHambers , “Clock-controlled shift registers in binary sequence generators”, IEE Proceedings E – Computers and Digital Techniques, 135 (1988), 17–24.
W.G. Chambers , “Two stream ciphers”, R. Anderson , editor, Fast Software Encryption, Cambridge Security Workshop (LNCS 809), 51–55, Springer-Verlag, 1994.

W.G. Chambers and D. Gollmann , “Lock-in effect in cascades of clock-controlled shift-registers”, Advances in Cryptology–EUROCRYPT ’88 (LNCS 330), 331–343, 1988.
B. Char , K. Geddes , G. Gonnet , B. Leong , M. Monagan , and S. Watt , Maple V Library Reference Manual, Springer-Verlag, New York, 1991.
C. Charnes , L. O’connor , J. Pieprzyk , R. Safavi-Naini , and Y. Zheng , “Comments on Soviet encryption algorithm”, Advances in Cryptology–EUROCRYPT ’94 (LNCS 950), 433–438, 1995.
D. Chaum , “Blind signatures for untraceable payments”, Advances in Cryptology–Proceedings of Crypto 82, 199–203, 1983.
D. Chaum , “Security without identification: transaction systems to make big brother obsolete”, Communications of the ACM, 28 (1985), 1030–1044.
D. Chaum , “Demonstrating that a public predicate can be satisfied without revealing any information about how”, Advances in Cryptology–CRYPTO ’86 (LNCS 263), 195–199, 1987.
D. Chaum , “Blinding for unanticipated signatures”, Advances in Cryptology–EUROCRYPT ’87 (LNCS 304), 227–233, 1988.
D. Chaum , “Zero-knowledge undeniable signatures”, Advances in Cryptology–EUROCRYPT ’90 (LNCS 473), 458–464, 1991.
D. Chaum , “Designated confirmer signatures”, Advances in Cryptology–EUROCRYPT ’94 (LNCS 950), 86–91, 1995.
D. Chaum , J.-H. Evertse , and J. Van De Graaf , “An improved protocol for demonstrating possession of discrete logarithms and some generalizations”, Advances in Cryptology–EUROCRYPT ’87 (LNCS 304), 127–141, 1988.
D. Chaum , J.-H. Evertse , J. Van De Graaf , and R. Peralta , “Demonstrating possession of a discrete logarithm without revealing it”, Advances in Cryptology–CRYPTO ’86 (LNCS 263), 200–212, 1987.
D. Chaum , A. Fiat , and M. Naor , “Untraceable electronic cash”, Advances in Cryptology–CRYPTO ’88 (LNCS 403), 319–327, 1990.
D. Chaum and T.P. Pedersen , “Wallet databases with observers”, Advances in Cryptology–CRYPTO ’92 (LNCS 740), 89–105, 1993.
D. Chaum and H. Van Antwerpen , “Undeniable signatures”, Advances in Cryptology–CRYPTO ’89 (LNCS 435), 212–216, 1990.
D. Chaum and E. Van Heijst , “Group signatures”, Advances in Cryptology–EUROCRYPT ’91 (LNCS 547), 257–265, 1991.
D. Chaum , E. Van Heijst , and B. Pfitzmann , “Cryptographically strong undeniable signatures, unconditionally secure for the signer”, Advances in Cryptology–CRYPTO ’91 (LNCS 576), 470–484, 1992.
L. Chen and T.P. Pedersen , “New group signature schemes”, Advances in Cryptology–EUROCRYPT ’94 (LNCS 950), 171–181, 1995.
V. Chepyzhov and B. Smeets , “On a fast correlation attack on certain stream ciphers”, Advances in Cryptology–EUROCRYPT ’91 (LNCS 547), 176–185, 1991.
B. Chor and O. Goldreich , “Unbiased bits from sources of weak randomness and probabilistic communication complexity”, Proceedings of the IEEE 26th Annual Symposium on Foundations of Computer Science, 429–442, 1985.
B. Chor and O. Goldreich , “Unbiased bits from sources of weak randomness and probabilistic communication complexity”, SIAMJournal on Computing,17 (1988), 230–261. An earlier version appeared in [257].
B. Chor , S. Goldwasser , S. Micali , and B. Awerbuch , “Verifiable secret sharing and achieving simultaneity in the presence of faults”, Proceedings of the IEEE 26th Annual Symposium on Foundations of Computer Science, 383–395, 1985.
B. Chor and R.L. Rivest , “A knapsack type public key cryptosystem based on arithmetic in finite fields”, Advances in Cryptology–Proceedings of CRYPTO 84 (LNCS 196), 54–65, 1985.
B. Chor and R.L. Rivest , “A knapsack-type public key cryptosystem based on arithmetic in finite fields”, IEEE Transactions on Information Theory,34 (1988), 901–909. An earlier version appeared in [260].
A. Clark , J. Goli´ , and E. Dawson , “A comparison of fast correlation attacks”, D. Gollmann , editor, Fast Software Encryption, Third International Workshop (LNCS 1039), 145–157, Springer-Verlag, 1996.
H. Cohen , A Course in Computational Algebraic Number Theory, Springer-Verlag, Berlin, 1993.
H. Cohen and A.K. Lenstra , “Implementation of a new primality test”, Mathematics of Computation, 48 (1987), 103–121.
H. Cohen and H.W. Lenstra Jr. , “Primality testing and Jacobi sums”, Mathematics of Computation, 42 (1984), 297–330.
D. Coppersmith , “Fast evaluation of logarithms in fields of characteristic two”, IEEE Transactions on Information Theory,30 (1984), 587–594.
D. Coppersmith , “Another birthday attack”, Advances in Cryptology–CRYPTO ’85 (LNCS 218), 14–17, 1986.
D. Coppersmith , “The real reason for Rivest’s phenomenon”, Advances in Cryptology–CRYPTO ’85 (LNCS 218), 535–536, 1986.
D. Coppersmith , “Modifications to the number field sieve”, Journal of Cryptology, 6 (1993), 169–180.
D. Coppersmith , “Solving linear equations over GF(2): Block Lanczos algorithm”, Linear Algebra and its Applications, 192 (1993), 33–60.
D. Coppersmith , “The Data Encryption Standard (DES) and its strength against attacks”, IBM Journal of Research and Development, 38 (1994), 243–250.
D. Coppersmith , “Solving homogeneous linear equations over GF(2) via block Wiedemann algorithm”, Mathematics of Computation,62 (1994), 333–350.
D. Coppersmith , “Finding a small root of a bivariate integer equation; factoring with high bits known”, Advances in Cryptology–EUROCRYPT ’96 (LNCS 1070), 178–189, 1996.
D. Coppersmith , “Finding a small root of a univariate modular equation”, Advances in Cryptology–EUROCRYPT ’96 (LNCS 1070), 155–165, 1996.
D. Coppersmith , “Analysis of ISO/CCITT Document X.509 Annex D”, memorandum, IBM T.J. Watson Research Center, Yorktown Heights, N.Y., 10598, U.S.A., June 11 1989.
D. Coppersmith , “Two broken hash functions”, IBM Research Report RC 18397, IBM T.J. Watson Research Center, Yorktown Heights, N.Y., 10598, U.S.A., Oct. 6 1992.
D. Coppersmith , M. Franklin , J. Patarin , and M. Reiter , “Low-exponent RSA with related messages”, Advances in Cryptology–EUROCRYPT ’96 (LNCS 1070), 1–9, 1996.
D. Coppersmith , D.B. Johnson , and S.M. Matyas , “A proposed mode for triple-DES encryption”, IBM Journal of Research and Development, 40 (1996), 253–261.
D. Coppersmith , H. Krawczyk , and Y. Mansour , “The shrinking generator”, Advances in Cryptology–CRYPTO ’93 (LNCS 773), 22–39, 1994.
D. Coppersmith , A.M. Odlzyko , and R. Schroeppel , “Discrete logarithms in GF(p)”, Algorithmica, 1 (1986), 1–15.
D. Coppersmith and P. Rogaway , “Software-efficient pseudorandom function and the use thereof for encryption”, U.S. Patent #5,454,039, 26 Sep 1995.

T.H. Cormen , C.E. Leiserson , and R.L. Rivest , Introduction to Algorithms, MIT Press, Cambridge, Massachusetts, 1990.
M.J. Coster , A. Joux , B.A. Lamacchia , A.M. Odlyzko , C.P. Schnorr , and J. Stern , “Improved low-density subset sum algorithms”, Computational Complexity, 2 (1992), 111–128.
J.-M. Couveignes , “Computing a square root for the number field sieve”, A.K. Lenstra and H.W. Lenstra Jr. , editors, The Development of the Number Field Sieve, volume 1554 of Lecture Notes in Mathematics, 95–102, Springer-Verlag, 1993.
T. Cover and R. King , “A convergent gambling estimate of the entropy of English”, IEEE Transactions on Information Theory,24 (1978), 413–421.
R. E. Crandall , “Method and apparatus for public key exchange in a cryptographic system”, U.S. Patent # 5,159,632, 27 Oct 1992.
R. E. Crandall , “Method and apparatus for public key exchange in a cryptographic system”, U.S. Patent # 5, 271, 061, 14 Dec 1993 (continuation-in-part of 5,159,632).
R. A. Croft and S.P. Harris , “Public-key cryptography and re-usable shared secrets”, H. Beker and F. Piper , editors, Cryptography and Coding, Institute of Mathematics & Its Applications (IMA), 189–201, Clarendon Press, 1989.
J. Daemen , Cipher and hash function design, PhD thesis, Katholieke Universiteit Leuven (Belgium), 1995.
J. Daemen , R. Govaerts , and J. Vandewalle , “A new approach to block cipher design”, R. Anderson , editor, Fast Software Encryption, Cambridge Security Workshop (LNCS 809), 18–32, Springer-Verlag, 1994.
J. Daemen , R. Govaerts , and J. Vandewalle , “Resynchronization weaknesses in synchronous stream ciphers”, Advances in Cryptology–EUROCRYPT ’93 (LNCS 765), 159–167, 1994.
J. Daemen , R. Govaerts , and J. VanDewalle , “Weak keys for IDEA”, Advances in Cryptology–CRYPTO ’93 (LNCS 773), 224–231, 1994.
Z.-D. Dai , “Proof of Rueppel’s linear complexity conjecture”, IEEE Transactions on Information Theory, 32 (1986), 440–443.
Z.-D. Dai and J.-H. Yang , “Linear complexity of periodically repeated random sequences”, Advances in Cryptology–EUROCRYPT ’91 (LNCS 547), 168–175, 1991.
I.B. Damgård , “Collision free hash functions and public key signature schemes”, Advances in Cryptology–EUROCRYPT ’87 (LNCS 304), 203–216, 1988.
I.B. Damgard , “A design principle for hash functions”, Advances in Cryptology–CRYPTO ’89 (LNCS 435), 416–427, 1990.
I.B. Damgard , “Towards practical public key systems secure against chosen ciphertext attacks”, Advances in Cryptology–CRYPTO ’91 (LNCS 576), 445–456, 1992.
I.B. Damgard , “Practical and provably secure release of a secret and exchange of signatures”, Advances in Cryptology–EUROCRYPT ’93 (LNCS 765), 200–217, 1994.
I.B. Damgård and P. Landrock , “Improved bounds for the Rabin primality test”, M.J. Ganley , editor, Cryptography and Coding III, volume 45 of Institute of Mathematics & Its Applications (IMA), 117–128, Clarendon Press, 1993.
I.B. Damgård , P. Landrock , and C. Pomerance , “Average case error estimates for the strong probable prime test”, Mathematics of Computation, 61 (1993), 177–194.
H. Davenport , “Bases for finite fields”, The Journal of the London Mathematical Society, 43 (1968), 21–39.
G.I. Davida , “Chosen signature cryptanalysis of the RSA (MIT) public key cryptosystem”, Technical Report TR-CS-82–2, Department of Electrical Engineering and Computer Science, University of Wisconsin, Milwaukee, WI, 1982.
D.W. Davies , “Some regular properties of the ’Data Encryption Standard’ algorithm”, Advances in Cryptology–Proceedings of Crypto 82, 89–96, 1983.
D.W. Davies , “A message authenticator algorithm suitable for a mainframe computer”, Advances in Cryptology–Proceedings of CRYPTO 84 (LNCS 196), 393–400, 1985.
D.W. Davies , “Schemes for electronic funds transfer at the point of sale”, K.M. Jackson and J. Hruska , editors, Computer Security Reference Book, 667–689, CRC Press, 1992.
D.W. Davies and D.O. Clayden , “The message authenticator algorithm (MAA) and its implementation”, Report DITC 109/88, National Physical Laboratory, U.K., February 1988.
D.W. Davies and G.I.P. Parkin , “The average cycle size of the key stream in output feedback encipherment”, Advances in Cryptology–Proceedings of Crypto 82, 97–98, 1983.
D.W. Davies and W.L. Price , Security for Computer Networks, John Wiley & Sons, New York, 2nd edition, 1989.
D. Davis , R. Ihaka , and P. Fenstermacher , “Cryptographic randomness from air turbulence in disk drives”, Advances in Cryptology–CRYPTO ’94 (LNCS 839), 114–120, 1994.
D. Davis and R. Swick , “Network security via private-key certificates”, Operating Systems Review, 24 (1990), 64–67.
J.A. Davis , D.B. Holdridge , and G.J. Simmons , “Status report on factoring (at the Sandia National Labs)”,Advances in Cryptology–Proceedings of EUROCRYPT 84 (LNCS 209), 183–215, 1985.
E. Dawson , “Cryptanalysis of summation generator”, Advances in Cryptology–AUSCRYPT ’92 (LNCS 718), 209–215, 1993.
W. De Jonge and D. Chaum , “Attacks on some RSA signatures”, Advances in Cryptology–CRYPTO ’85 (LNCS 218), 18–27, 1986.
P. De Rooij , “On the security of the Schnorr scheme using preprocessing”, Advances in Cryptology–EUROCRYPT ’91 (LNCS 547), 71–80, 1991.
P. De Rooij , “On Schnorr’s preprocessing for digital signature schemes”, Advances in Cryptology–EUROCRYPT ’93 (LNCS 765), 435–439, 1994.
P. De Rooij , “Efficient exponentiation using precomputation and vector addition chains”, Advances in Cryptology–EUROCRYPT ’94 (LNCS 950), 389–399, 1995.
A. De Santis , S. Micali , and G. Persiano , “Non-interactive zero-knowledge proof systems”, Advances in Cryptology–CRYPTO ’87 (LNCS 293), 52–72, 1988.
A. De Santis and M. Yung , “On the design of provably secure cryptographic hash functions”, Advances in Cryptology–EUROCRYPT ’90 (LNCS 473), 412–431, 1991.
D. De Waleffe and J.-J. Quisquater , “Better login protocols for computer networks”, B. Preneel , R. Govaerts , and J. Vandewalle , editors, Computer Security and Industrial Cryptography: State of the Art and Evolution (LNCS 741), 50–70, Springer-Verlag, 1993.
J. M. Delaurentis , “A further weakness in the common modulus protocol for the RSA cryptoalgorithm”, Cryptologia, 8 (1984), 253–259.
N. Demytko , “A new elliptic curve based analogue of RSA”, Advances in Cryptology–EUROCRYPT ’93 (LNCS 765), 40–49, 1994.
B. Den Boer , “Cryptanalysis of F.E.A.L.”, Advances in Cryptology–EUROCRYPT ’88 (LNCS 330), 293–299, 1988.

B. Den Boer , “Diffie-Hellman is as strong as discrete log for certain primes”, Advances in Cryptology–CRYPTO ’88 (LNCS 403), 530–539, 1990.
B. Den Boer and A. Bosselaers , “An attack on the last two rounds of MD4”, Advances in Cryptology–CRYPTO ’91 (LNCS 576), 194–203, 1992.
B. Den Boer and A. Bosselaers , “Collisions for the compression function of MD5”, Advances in Cryptology–EUROCRYPT ’93 (LNCS 765), 293–304, 1994.
D.E. Denning , Cryptography and Data Security, Addison-Wesley, Reading, Massachusetts, 1983. Reprinted with corrections.
D.E. Denning , “Digital signatures with RSA and other public-key cryptosystems”, Communications of the ACM, 27 (1984), 388–392.
D.E. Denning , “To tap or not to tap”, Communications of the ACM, 36 (1993), 24–44.
D.E. Denning and D.K. Branstad , “A taxonomy for key escrow encryption systems”, Communications of the ACM,39 (1996), 34–40.
D.E. Denning and G.M. Sacco , “Timestamps in key distribution protocols”, Communications of the ACM, 24 (1981), 533–536.
D.E. Denning and M. Smid , “Key escrowing today”, IEEE Communications Magazine, 32 (September 1994), 58–68.
J.B. Dennis and E.C. Van Horn , “Programming semantics for multiprogrammed computations”, Communications of the ACM, 9 (1966), 143–155.
T. Denny , B. Dodson , A.K. Lenstra , and M.S. Manasse , “On the factorization of RSA-120”, Advances in Cryptology–CRYPTO ’93 (LNCS 773), 166–174, 1994.
DEPARTMENT OF DEFENSE (U.S.) , “Department of defense password management guideline”, CSC-STD-002–85, Department of Defense Computer Security Center, Fort Meade, Maryland, 1985.
Y. Desmedt , “Unconditionally secure authentication schemes and practical and theoretical consequences”, Advances in Cryptology–CRYPTO ’85 (LNCS 218), 42–55, 1986.
Y. Desmedt , “Society and group oriented cryptography: A new concept”, Advances in Cryptology–CRYPTO ’87 (LNCS 293), 120–127, 1988.
Y. Desmedt , “Threshold cryptography”, European Transactions on Telecommunications,5 (1994), 449–457.
Y. Desmedt , “Securing traceability of ciphertexts – Towards a secure software key escrow system”, Advances in Cryptology–EUROCRYPT ’95 (LNCS 921), 147–157, 1995.
Y. Desmedt and M. Burmester , “Towards practical ‘proven secure’ authenticated key distribution”, 1st ACM Conference on Computer and Communications Security, 228–231, ACM Press, 1993.
Y. Desmedt , C. Goutier , and S. Bengio , “Special uses and abuses of the Fiat-Shamir passport protocol”, Advances in Cryptology–CRYPTO ’87 (LNCS 293), 21–39, 1988.
Y. Desmedt and A.M. Odlyzko , “A chosen text attack on the RSA cryptosystem and some discrete logarithm schemes”, Advances in Cryptology–CRYPTO ’85 (LNCS 218), 516–522, 1986.
W. Diffie , “The first ten years of public-key cryptography”, Proceedings of the IEEE,76 (1988), 560–577.
W. Diffie , “The first ten years of public key cryptology”, G.J. Simmons , editor, Contemporary Cryptology: The Science of Information Integrity, 135–175, IEEE Press, 1992. An earlier version appeared in [342].
W. Diffie and M.E. Hellman , “Multiuser cryptographic techniques”, Proceedings of AFIPS National Computer Conference, 109–112, 1976.
W. Diffie and M.E. Hellman , “New directions in cryptography”, IEEE Transactions on Information Theory,22 (1976), 644–654.
W. Diffie and M.E. Hellman , “Exhaustive cryptanalysis of the NBS Data Encryption Standard”, Computer,10 (1977), 74–84.
W. Diffie and M.E. Hellman , “Privacy and authentication: An introduction to cryptography”, Proceedings of the IEEE, 67 (1979), 397–427.
W. Diffie , P.C. Van Oorschot , and M.J. Wiener , “Authentication and authenticated key exchanges”, Designs, Codes and Cryptography, 2 (1992), 107–125.
C. Ding , “The differential cryptanalysis and design of natural stream ciphers”, R. Anderson , editor, Fast Software Encryption, Cambridge Security Workshop (LNCS 809), 101–115, Springer-Verlag, 1994.
B. Dixon and A.K. Lenstra , “Massively parallel elliptic curve factoring”, Advances in Cryptology–EUROCRYPT ’92 (LNCS 658), 183–193, 1993.
J.D. Dixon , “Asymptotically fast factorization of integers”, Mathematics of Computation, 36 (1981), 255–260.
H. Dobbertin , “Cryptanalysis of MD4”, Journal of Cryptology, to appear.
H. Dobbertin , “RIPEMD with two-round compress function is not collision-free”, Journal of Cryptology, to appear; announced at rump session, Eurocrypt ’95.
H. Dobbertin , “Cryptanalysis of MD4”, D. Gollmann , editor, Fast Software Encryption, Third International Workshop (LNCS 1039), 53–69, Springer-Verlag, 1996.
H. Dobbertin , A. Bosselaers , and B. Preneel , “RIPEMD-160: a strengthened version of RIPEMD”, D. Gollmann , editor, Fast Software Encryption, Third International Workshop (LNCS 1039), 71–82, Springer-Verlag, 1996.
B. Dodson and A.K. Lenstra , “NFS with four large primes: An explosive experiment”, Advances in Cryptology–CRYPTO ’95 (LNCS 963), 372–385, 1995.
D. Dolev , C. Dwork , and M. Naor , “Non-malleable cryptography”, Proceedings of the 23rd Annual ACM Symposium on Theory of Computing, 542–552, 1991.
D. Dolev and A.C. Yao , “On the security of public key protocols”, Proceedings of the IEEE 22nd Annual Symposium on Foundations of Computer Science, 350–357, 1981.
D. Dolev and A.C. Yao , “On the security of public key protocols”, IEEE Transactions on Information Theory, 29 (1983), 198–208. An earlier version appeared in [358].
P. Downey , B. Leong , and R. Sethi , “Computing sequences with addition chains”, SIAM Journal on Computing, 10 (1981), 638–646.
S.R. Dussé and B.S. Kaliski Jr. , “A cryptographic library for the Motorola DSP 56000”, Advances in Cryptology–EUROCRYPT ’90 (LNCS 473), 230–244, 1991.
H. Eberle , “A high-speed DES implementation for network applications”, Advances in Cryptology–CRYPTO ’92 (LNCS 740), 521–539, 1993.
W. F. Ehrsam , C.H.W. Meyer , R.L. Powers , J.L. Smith , and W.L. Tuchman , “Product block cipher system for data security”, U.S. Patent # 3,962,539, 8 Jun 1976.
W.F. Ehrsam , S.M. Matyas , C.H. Meyer , and W.L. Tuchman , “A cryptographic key management scheme for implementing the Data Encryption Standard”, IBM Systems Journal, 17 (1978), 106–125.

ELECTRONIC INDUSTRIES ASSOCIATION (EIA) , “Dual-mode mobile station – base station compatibility standard”, EIA Interim Standard IS-54 Revision B (Rev. B), 1992.
T. Elgamal , Cryptography and logarithms over finite fields, PhD thesis, Stanford University, 1984.
T. Elgamal , “A public key cryptosystem and a signature scheme based on discrete logarithms”, Advances in Cryptology–Proceedings of CRYPTO 84 (LNCS 196), 10–18, 1985.
T. Elgamal , “A public key cryptosystem and a signature scheme based on discrete logarithms”, IEEE Transactions on Information Theory,31 (1985), 469–472. An earlier version appeared in [367].
T. Elgamal , “A subexponential-time algorithm for computing discrete logarithms over GF(p 2)”, IEEE Transactions on Information Theory,31 (1985), 473–481.
P. Elias , “The efficient construction of an unbiased random sequence”, The Annals of Mathematical Statistics, 43 (1972), 865–870.
P. Elias , “Interval and recency rank source encoding: Two on-line adaptive variable-length schemes”, IEEE Transactions on Information Theory, 33 (1987), 3–10.
E.D. Erdmann , “Empirical tests of binary keystreams”, Master’s thesis, Department of Mathematics, Royal Holloway and Bedford New College, University of London, 1992.
P. Erdös and C. Pomerance , “On the number of false witnesses for a composite number”, Mathematics of Computation,46 (1986), 259–279.
D. Estes , L.M. Adleman , K. Kompella , K.S. Mccurley , and G.L. Miller , “Breaking the Ong-Schnorr-Shamir signature scheme for quadratic number fields”, Advances in Cryptology–CRYPTO ’85 (LNCS 218), 3–13, 1986.
A. Evans Jr., W. Kantrowitz , and E. Weiss , “A user authentication scheme not requiring secrecy in the computer”, Communications of the ACM, 17 (1974), 437–442.
S. Even and O. Goldreich , “On the power of cascade ciphers”, ACMTransactions on Computer Systems, 3 (1985), 108–116.
S. Even , O. Goldreich , and S. Micali , “On-line/off-line digital signatures”, Advances in Cryptology–CRYPTO ’89 (LNCS 435), 263–275, 1990.
S. Even , O. Goldreich , and S. Micali , “On-line/off-line digital signatures”, Journal of Cryptology, 9 (1996), 35–67. An earlier version appeared in [377].
S. Even and Y. Yacobi , “Cryptocomplexity and NP-completeness”, J.W. De Bakker and J. Van Leeuwen , editors, Automata, Languages, and Programming, 7th Colloquium (LNCS 85), 195–207, Springer-Verlag, 1980.
D. Everett , “Identity verification and biometrics”, K.M. Jackson and J. Hruska , editors, Computer Security Reference Book, 37–73, CRC Press, 1992.
J.-H. Evertse and E. Van Heijst , “Which new RSA-signatures can be computed from certain given RSA-signatures?”, Journal of Cryptology, 5 (1992), 41–52.
R.C. Fairfield , R.L. Mortenson , and K.B. Coulthart , “An LSI random number generator (RNG)”, Advances in Cryptology–Proceedings of CRYPTO 84 (LNCS 196), 203–230, 1985.
U. Feige , A. Fiat , and A. Shamir , “Zero-knowledge proofs of identity”, Journal of Cryptology, 1 (1988), 77–94.
U. Feige and A. Shamir , “Witness indistinguishable and witness hiding protocols”, Proceedings of the 22nd Annual ACM Symposium on Theory of Computing, 416–426, 1990.
H. Feistel , “Block cipher cryptographic system”, U.S. Patent # 3,798,359, 19 Mar 1974.
H. Feistel , “Step code ciphering system”, U.S. Patent # 3,798,360, 19 Mar 1974.
H. Feistel , “Cryptography and computer privacy”, Scientific American, 228 (May 1973), 15–23.
H. Feistel , W.A. Notz , and J.L. Smith , “Some cryptographic techniques for machine-to-machine data communications”, Proceedings of the IEEE, 63 (1975), 1545–1554.
F.A. Feldman , “Fast spectral tests for measuring nonrandomness and the DES”, Advances in Cryptology–CRYPTO ’87 (LNCS 293), 243–254, 1988.
P. Feldman , “A practical scheme for non-interactive verifiable secret sharing”, Proceedings of the IEEE 28th Annual Symposium on Foundations of Computer Science, 427–437, 1987.
D.C. Feldmeier and P.R. Karn , “UNIX password security – ten years later”, Advances in Cryptology–CRYPTO ’89 (LNCS 435), 44–63, 1990.
W. Feller , An Introduction to Probability Theory and its Applications, John Wiley & Sons, New York, 3rd edition, 1968.
A. Fiat and M. Naor , “Rigorous time/space tradeoffs for inverting functions”, Proceedings of the 23rd Annual ACM Symposium on Theory of Computing, 534–541, 1991.
A. Fiat and M. Naor , “Broadcast encryption”, Advances in Cryptology–CRYPTO ’93 (LNCS 773), 480–491, 1994.
A. Fiat and A. Shamir , “How to prove yourself: Practical solutions to identification and signature problems”, Advances in Cryptology–CRYPTO ’86 (LNCS 263), 186–194, 1987.
FIPS 46 , “Data encryption standard”, Federal Information Processing Standards Publication 46, U.S. Department of Commerce/National Bureau of Standards, National Technical Information Service, Springfield, Virginia, 1977 (revised as FIPS 46–1:1988; FIPS 46-2:1993).
FIPS 74 , “Guidelines for implementing and using the NBS data encryption standard”, Federal Information Processing Standards Publication 74, U.S. Department of Commerce/National Bureau of Standards, National Technical Information Service, Springfield, Virginia, 1981.
FIPS 81 , “DES modes of operation”, Federal Information Processing Standards Publication 81, U.S. Department of Commerce/National Bureau of Standards, National Technical Information Service, Springfield, Virginia, 1980.
FIPS 112 , “Password usage”, Federal Information Processing Standards Publication 112, U.S. Department of Commerce/National Bureau of Standards, National Technical Information Service, Springfield, Virginia, 1985.
FIPS 113 , “Computer data authentication”, Federal Information Processing Standards Publication 113, U.S. Department of Commerce/National Bureau of Standards, National Technical Information Service, Springfield, Virginia, 1985.
FIPS 140-1 , “Security requirements for cryptographic modules”, Federal Information Processing Standards Publication 140–1, U.S. Department of Commerce/N.I.S.T., National Technical Information Service, Springfield, Virginia, 1994.
FIPS 171 , “Key management using ANSI X9.17”, Federal Information Processing Standards Publication 171, U.S. Department of Commerce/N.I.S.T., National Technical Information Service, Springfield, Virginia, 1992.
FIPS 180 , “Secure hash standard”, Federal Information Processing Standards Publication 180, U.S. Department of Commerce/N.I.S.T., National Technical Information Service, Springfield, Virginia, May 11 1993.

FIPS 180-1 , “Secure hash standard”, Federal Information Processing Standards Publication 180–1, U.S. Department of Commerce/N.I.S.T., National Technical Information Service, Springfield, Virginia, April 17 1995 (supersedes FIPS PUB 180).
FIPS 185 , “Escrowed encryption standard (EES)”, Federal Information Processing Standards Publication 185, U.S. Department of Commerce/N.I.S.T., National Technical Information Service, Springfield, Virginia, 1994.
FIPS 186 , “Digital signature standard”, Federal Information Processing Standards Publication 186, U.S. Department of Commerce/N.I.S.T., National Technical Information Service, Springfield, Virginia, 1994.
FIPS 196 , “Entity authentication using public key cryptography”, U.S. Department of Commerce/N.I.S.T., February 18 1997.
A.M. Fischer , “Public key/signature cryptosystem with enhanced digital signature certification”, U.S. Patent # 4,868,877, 19 Sep 1989.
A.M. Fischer , “Public key/signature cryptosystem with enhanced digital signature certification”, U.S. Patent # 5,005,200, 2 Apr 1991 (continuation-in-part of 4,868,877).
A.M. Fischer , “Electronic document authorization”, Proceedings of the 13th National Computer Security Conference, Washington D.C., sponsored by N.I.S.T. and the National Computer Security Center, USA, 1990.
J.-B. Fischer and J. Stern , “An efficient pseudo-random generator provably as secure as syndrome decoding”, Advances in Cryptology–EUROCRYPT ’96 (LNCS 1070), 245–255, 1996.
M. Fischer , S. Micali , and C. Rackoff , “A secure protocol for oblivious transfer”, unpublished (presented at Eurocrypt’84).
P. Flajolet and A. Odlyzko , “Random mapping statistics”, Advances in Cryptology–EUROCRYPT ’89 (LNCS 434), 329–354, 1990.
W. Ford , Computer Communications Security: Principles, Standard Protocols and Techniques, Prentice Hall, Englewood Cliffs, New Jersey, 1994.
W. Ford , “Standardizing information technology security”, StandardView, 2 (1994), 64–71.
W. Ford , “Advances in public-key certificate standards”, Security, Audit and Control, 13 (1995), ACM Press/SIGSAC, 9–15.
W. Ford and M. Wiener , “A key distribution method for object-based protection”, 2nd ACM Conference on Computer and Communications Security, 193–197, ACM Press, 1994.
R. Forré , “A fast correlation attack on nonlinearly feedforward filtered shift-register sequences”, Advances in Cryptology–EUROCRYPT ’89 (LNCS 434), 586–595, 1990.
Y. Frankel and M. Yung , “Cryptanalysis of the immunized LL public key systems”, Advances in Cryptology–CRYPTO ’95 (LNCS 963), 287–296, 1995.
Y. Frankel and M. Yung , “Escrow encryption systems visited: Attacks, analysis and designs”, Advances in Cryptology–CRYPTO ’95 (LNCS 963), 222–235, 1995.
M.K. Franklin and M.K. Reiter , “Verifiable signature sharing”, Advances in Cryptology–EUROCRYPT ’95 (LNCS 921), 50–63, 1995.
G. Frey and H.-G. Rück , “A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves”, Mathematics of Computation, 62 (1994), 865–874.
W. Friedman , Military Cryptanalysis, U.S. Government Printing Office, Washington DC, 1944. Volume I – Monoalphabetic substitution systems. Volume II – Simpler varieties of polyalphabetic substitution systems. Volume III – Aperiodic substitutions. Volume IV – Transposition systems.
W. Friedman , “Cryptology”, Encyclopedia Brittanica, 6 (1967), 844–851.
W. Friedman , Elements of Cryptanalysis, Aegean Park Press, Laguna Hills, California, 1976. First published in 1923.
W. Friedman , The Index of Coincidence and its Applications in Cryptography, Aegean Park Press, Laguna Hills, California, 1979. First published in 1920.
A.M. Frieze , J. Håstad , R. Kannan , J.C. Lagarias , and A. Shamir , “Reconstructing truncated integer variables satisfying linear congruences”, SIAM Journal on Computing, 17 (1988), 262–280.
A. Fujioka , T. Okamoto , and S. Miyaguchi , “ESIGN: An efficient digital signature implementation for smart cards”, Advances in Cryptology–EUROCRYPT ’91 (LNCS 547), 446–457, 1991.
W. Fumy and P. Landrock , “Principles of key management”, IEEE Journal on Selected Areas in Communications, 11 (1993), 785–793.
W. Fumy and M. Leclerc , “Placement of cryptographic key distribution within OSI: design alternatives and assessment”, Computer Networks and ISDN Systems, 26 (1993), 217–225.
W. Fumy and M. Munzert , “A modular approach to key distribution”, Advances in Cryptology–CRYPTO ’90 (LNCS 537), 274–283, 1991.
W. Fumy and M. Rietenspiess , “Open systems security standards”, A. Kent and J.G. Williams , editors, Encyclopedia of Computer Science and Technology 34, 301–334, Marcel Dekker, 1996.
K. Gaarder and E. Snekkenes , “Applying a formal analysis technique to the CCITT X.509 strong two-way authentication protocol”, Journal of Cryptology, 3 (1991), 81–98.
E.M. Gabidulin , “On public-key cryptosystems based on linear codes: Efficiency and weakness”, P.G. Farrell , editor, Codes and Cyphers: Cryptography and Coding IV, 17–31, Institute of Mathematics & Its Applications (IMA), 1995.
E.M. Gabidulin , A.V. Paramonov , and O.V. Tretjakov , “Ideals over a non-commutative ring and their application in cryptology”, Advances in Cryptology–EUROCRYPT ’91 (LNCS 547), 482–489, 1991.
H. Gaines , Cryptanalysis:A Study of Ciphers and their Solutions, Dover Publications, New York, 1956.
J. Gait , “A new nonlinear pseudorandom number generator”, IEEE Transactions on Software Engineering, 3 (1977), 359–363.
J.M. Galvin , K. Mccloghrie , and J.R. Davin , “Secure management of SNMP networks”, Integrated Network Management, II, 703–714, 1991.
R.A. Games and A.H. Chan , “A fast algorithm for determining the complexity of a binary sequence with period 2n ”, IEEE Transactions on Information Theory, 29 (1983), 144–146.
M. Gardner , “A new kind of cipher that would take millions of years to break”, Scientific American, 237 (Aug 1977), 120–124.
M.R. Garey and D. S. Johnson , Computers and Intractability: A Guide to the Theory of NP-completeness, W.H. Freeman, San Francisco, 1979.
S. Garfinkel , PGP:Pretty Good Privacy, O’Reilly and Associates, Inc., Sebastopol, California, 1995.
H. Garner , “The residue number system”, IRE Transactions on Electronic Computers, EC-8 (1959), 140–147.
C.F. Gauss , Disquisitiones Arithmeticae, 1801. English translation by Arthur A.Clarke, Springer-Verlag, New York, 1986.
K. Geddes , S. Czapor , and G. Labahn , Algorithms for Computer Algebra, Kluwer Academic Publishers, Boston, 1992.
P. Geffe , “How to protect data with ciphers that are really hard to break”, Electronics,46 (1973), 99–101.

J. Georgiades , “Some remarks on the security of the identification scheme based on permuted kernels”, Journal of Cryptology,5 (1992), 133–137.
J. Gerver , “Factoring large numbers with a quadratic sieve”, Mathematics of Computation, 41 (1983), 287–294.
P.J. Giblin , Primes and Programming: An Introduction to Number Theory with Computing, Cambridge University Press, Cambrige, 1993.
J.K. Gibson , “Some comments on Damgård’s hashing principle”, Electronics Letters, 26 (July 19, 1990), 1178–1179.
J.K. Gibson , “Equivalent Goppa codes and trapdoors to McEliece’s public key cryptosystem”, Advances in Cryptology–EUROCRYPT ’91 (LNCS 547), 517–521, 1991.
J.K. Gibson , “Severely denting the Gabidulin version of the McEliece public key cryptosystem”, Designs, Codes and Cryptography, 6 (1995), 37–45.
J.K. Gibson , “The security of the Gabidulin public key cryptosystem”, Advances in Cryptology–EUROCRYPT ’96 (LNCS 1070), 212–223, 1996.
E.N. Gilbert , F.J. Macwilliams , and N.J.A. Sloane , “Codes which detect deception”, Bell System Technical Journal,53 (1974), 405–424.
H. Gilbert and G. Chassé , “A statistical attack of the Feal-8 cryptosystem”, Advances in Cryptology–CRYPTO ’90 (LNCS 537), 22–33, 1991.
H. Gilbert and P. Chauvaud , “A chosen plaintext attack of the 16-round Khufu cryptosystem”, Advances in Cryptology–CRYPTO ’94 (LNCS 839), 359–368, 1994.
M. Girault , “Hash-functions using modulon operations”, Advances in Cryptology–EUROCRYPT ’87 (LNCS 304), 217–226, 1988.
M. Girault , “An identity-based identification scheme based on discrete logarithms modulo a composite number”, Advances in Cryptology–EUROCRYPT ’90 (LNCS 473), 481–486, 1991.
M. Girault , “Self-certified public keys”, Advances in Cryptology–EUROCRYPT ’91 (LNCS 547), 490–497, 1991.
M. Girault , R. Cohen , and M. Campana , “A generalized birthday attack”, Advances in Cryptology–EUROCRYPT ’88 (LNCS 330), 129–156, 1988.
M. Girault and J.C. Paillès , “An identity-based scheme providing zero-knowledge authentication and authenticated key-exchange”, First European Symposium on Research in Computer Security – ESORICS’ 90, 173–184, 1990.
M. Girault and J. Stern , “On the length of cryptographic hash-values used in identification schemes”, Advances in Cryptology–CRYPTO ’94 (LNCS 839), 202–215, 1994.
V.D. Gligor , R. Kailar , S. Stubblebine , and L. Gong , “Logics for cryptographic protocols — virtues and limitations”, The Computer Security Foundations Workshop IV, 219–226, IEEE Computer Security Press, 1991.
C.M. Goldie and R.G.E. Pinch , Communication Theory, Cambridge University Press, Cambridge, 1991.
O. Goldreich , “Two remarks concerning the Goldwasser-Micali-Rivest signature scheme”, Advances in Cryptology–CRYPTO ’86 (LNCS 263), 104–110, 1987.
O. Goldreich , S. Goldwasser , and S. Micali , “How to construct random functions”, Proceedings of the IEEE 25th Annual Symposium on Foundations of Computer Science, 464–479, 1984.
O. Goldreich , S. Goldwasser , and S. Micali , “On the cryptographic applications of random functions”, Advances in Cryptology–Proceedings of CRYPTO 84 (LNCS 196), 276–288, 1985.
O. Goldreich , S. Goldwasser , and S. Micali , “How to construct random functions”, Journal of the Association for Computing Machinery, 33 (1986), 792–807. An earlier version appeared in [466].
O. Goldreich and H. Krawczyk , “On the composition of zero-knowledge proof systems”, M.S. Paterson , editor, Automata, Languages and Programming, 17th International Colloquium (LNCS 443), 268–282, Springer-Verlag, 1990.
O. Goldreich , H. Krawczyk , and M. Luby , “On the existence of pseudorandom generators”, Proceedings of the IEEE 29th Annual Symposium on Foundations of Computer Science, 12–24, 1988.
O. Goldreich and L.A. Levin , “A hardcore predicate for all one-way functions”, Proceedings of the 21st Annual ACM Symposium on Theory of Computing, 25–32, 1989.
O. Goldreich , S. Micali , and A. Wigderson , “Proofs that yield nothing but their validity and a methodology of cryptographic protocol design”, Proceedings of the IEEE 27th Annual Symposium on Foundations of Computer Science, 174–187, 1986.
O. Goldreich , S. Micali , and A. Wigderson , “How to prove all NP statements in zero-knowledge, and a methodology of cryptographic protocol design”, Advances in Cryptology–CRYPTO ’86 (LNCS 263), 171–185, 1987.
O. Goldreich , S. Micali , and A. Wigderson , “Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems”, Journal of the Association for Computing Machinery,38 (1991), 691–729. An earlier version appeared in [472].
O. Goldreich and Y. Oren , “Definitions and properties of zero-knowledge proof systems”, Journal of Cryptology, 7 (1994), 1–32.
S. Goldwasser , “The search for provably secure cryptosystems”, C. Pomerance , editor, Cryptology and Computational Number Theory, volume 42 of Proceedings of Symposia in Applied Mathematics, 89–113, American Mathematical Society, 1990.
S. Goldwasser and J. Kilian , “Almost all primes can be quickly certified”, Proceedings of the 18th Annual ACM Symposium on Theory of Computing, 316–329, 1986.
S. Goldwasser and S. Micali , “Probabilistic encryption & how to play mental poker keeping secret all partial information”, Proceedings of the 14th Annual ACM Symposium on Theory of Computing, 365–377, 1982.
S. Goldwasser and S. Micali , “Probabilistic encryption”, Journal of Computer and System Sciences, 28 (1984), 270–299. An earlier version appeared in [478].
S. Goldwasser , S. Micali , and C. Rackoff , “The knowledge complexity of interactive proof-systems”, Proceedings of the 17th Annual ACM Symposium on Theory of Computing, 291–304, 1985.
S. Goldwasser , S. Micali , and C. Rackoff , “The knowledge complexity of interactive proof systems”, SIAMJournal on Computing, 18 (1989), 186–208. An earlier version appeared in [480].
S. Goldwasser , S. Micali , and R.L. Rivest , “A “paradoxical” solution to the signature problem”, Proceedings of the IEEE 25th Annual Symposium on Foundations of Computer Science, 441–448, 1984.
S. Goldwasser , S. Micali , and R.L. Rivest , “A “paradoxical” solution to the signature problem”, Advances in Cryptology–Proceedings of CRYPTO 84 (LNCS 196), 467, 1985.
S. Goldwasser , S. Micali , and R.L. Rivest , “A digital signature scheme secure against adaptive chosen-message attacks”, SIAM Journal on Computing, 17 (1988), 281–308. Earlier versions appeared in [482] and [483].
J. Golić , “Correlation via linear sequential circuit approximation of combiners with memory”, Advances in Cryptology–EUROCRYPT ’92 (LNCS 658), 113–123, 1993.

J. Golić , “On the security of shift register based keystream generators”, R. Anderson , editor, Fast Software Encryption, Cambridge Security Workshop (LNCS 809), 90–100, Springer-Verlag, 1994.
J. Golić , “Intrinsic statistical weakness of key-stream generators”, Advances in Cryptology–ASIACRYPT ’94 (LNCS 917), 91–103, 1995.
J. Golić , “Linear cryptanalysis of stream ciphers”, B. Preneel , editor, Fast Software Encryption, Second International Workshop (LNCS 1008), 154–169, Springer-Verlag, 1995.
J. Golić , “Towards fast correlation attacks on irregularly clocked shift registers”, Advances in Cryptology–EUROCRYPT ’95 (LNCS 921), 248–262, 1995.
J. Golić , “On the security of nonlinear filter generators”, D. Gollmann , editor, Fast Software Encryption, Third International Workshop (LNCS 1039), 173–188, Springer- Verlag, 1996.
J. Golić and M. Mihaljević , “A generalized correlation attack on a class of stream ciphers based on the Levenshtein distance”, Journal of Cryptology, 3 (1991), 201–212.
J. Golić and L. O’Connor , “Embedding and probabilistic correlation attacks on clock-controlled shift registers”, Advances in Cryptology–EUROCRYPT ’94 (LNCS 950), 230 230–243, 1995.
R.A. Golliver , A.K. Lenstra , and K.S. Mccurley , “Lattice sieving and trial division”, Algorithmic Number Theory (LNCS 877), 18–27, 1994.
D. Gollmann , “Pseudo random properties of cascade connections of clock controlled shift registers”, Advances in Cryptology–Proceedings of EUROCRYPT 84 (LNCS 209), 93–98, 1985.
D. Gollmann , “Cryptanalysis of clock controlled shift registers”, R. Anderson , editor, Fast Software Encryption, Cambridge Security Workshop (LNCS 809), 121–126, Springer-Verlag, 1994.
D. Gollmann and W.G. Chambers , “Clock-controlled shift registers: a review”, IEEE Journal on Selected Areas in Communications, 7 (1989), 525–533.
D. Gollmann , Y. Han , and C. Mitchell , “Redundant integer representations and fast exponentiation”, Designs, Codes and Cryptography, 7 (1996), 135–151.
S.W. Golomb , Shift Register Sequences, Holden-Day, San Francisco, 1967. Reprinted by Aegean Park Press, 1982.
L. Gong , “Using one-way functions for authentication”, Computer Communication Review, 19 (1989), 8–11.
L. Gong , “A security risk of depending on synchronized clocks”, Operating Systems Review, 26 (1992), 49–53.
L. Gong , “Variations on the themes of message freshness and replay”, The Computer Security Foundations Workshop VI, 131–136, IEEE Computer Society Press, 1993.
L. Gong , “New protocols for third-party-based authentication and secure broadcast”, 2nd ACM Conference on Computer and Communications Security, 176–183, ACM Press, 1994.
L. Gong , “Efficient network authentication protocols: lower bounds and optimal implementations”, Distributed Computing, 9 (1995), 131–145.
L. Gong , T.M.A. Lomas , R.M. Needham , and J.H. Saltzer , “Protecting poorly chosen secrets from guessing attacks”, IEEE Journal on Selected Areas in Communications, 11 (1993), 648–656.
L. Gong , R. Needham , and R. Yahalom , “Reasoning about belief in cryptographic protocols”, Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy, 234–248, 1990.
L. Gong and D.J. Wheeler , “A matrix key-distribution scheme”, Journal of Cryptology, 2 (1990), 51–59.
I.J. Good , “The serial test for sampling numbers and other tests for randomness”, Proceedings of the Cambridge Philosophical Society, 49 (1953), 276–284.
I.J. Good , “On the serial test for random sequences”, The Annals of Mathematical Statistics, 28 (1957), 262–264.
D.M. Gordon , “Designing and detecting trapdoors for discrete log cryptosystems”, Advances in Cryptology–CRYPTO ’92 (LNCS 740), 66–75, 1993.
D.M. Gordon , “Discrete logarithms in GF(p) using the number field sieve”, SIAM Journal on Discrete Mathematics, 6 (1993), 124–138.
D.M. Gordon and K.S. Mccurley , “Massively parallel computations of discrete logarithms”, Advances in Cryptology–CRYPTO ’92 (LNCS 740), 312–323, 1993.
J. Gordon , “Very simple method to find the minimum polynomial of an arbitrary nonzero element of a finite field”, Electronics Letters, 12 (December 9, 1976), 663–664.
J. Gordon , “Strong RSA keys”, Electronics Letters, 20 (June 7, 1984), 514–516.
J. Gordon , “Strong primes are easy to find”, Advances in Cryptology–Proceedings of EUROCRYPT 84 (LNCS 209), 216–223, 1985.
J. Gordon , “How to forge RSA key certificates”, Electronics Letters, 21 (April 25, 1985), 377–379.
J. Gordon , “Fast multiplicative inverse in modular arithmetic”, H. Beker and F. Piper , editors, Cryptography and Coding, Institute of Mathematics & Its Applications (IMA), 269–279, Clarendon Press, 1989.
J. Gordon and H. Retkin , “Are big *S*-boxes best?”, Cryptography–Proceedings of the Workshop on Cryptography, Burg Feuerstein (LNCS 149), 257–262, 1983.
M. Goresky and A. Klapper , “Feedback registers based on ramified extensions of the 2-adic numbers”, Advances in Cryptology–EUROCRYPT ’94 (LNCS 950), 215–222, 1995.
K.C. Goss , “Cryptographic method and apparatus for public key exchange with authentication”, U.S. Patent #4,956,863, 11 Sep 1990.
R. Graham , D. Knuth , and O. Patashnik , Concrete Mathematics, Addison-Wesley, Reading, Massachusetts, 2nd edition, 1994.
A. Granville , “Primality testing and Carmichael numbers”, Notices of the American Mathematical Society, 39 (1992), 696–700.
E. Grossman , “Group theoretic remarks on cryptographic systems based on two types of addition”, IBM Research Report RC 4742, IBM T.J. Watson Research Center, Yorktown Heights, N.Y., 10598, U.S.A., Feb. 26 1974.
L.C. Guillou and J.-J. Quisquater , “Method and apparatus for authenticating accreditations and for authenticating and signing messages”, U.S. Patent # 5,140,634, 18 Aug 1992.
L.C. Guillou and J.-J. Quisquater , “A practical zero-knowledge protocol fitted to security microprocessor minimizing both transmission and memory”, Advances in Cryptology–EUROCRYPT ’88 (LNCS 330), 123–128, 1988.
L.C. Guillou , J.-J. Quisquater , M. Walker , P. Landrock , and C. Shaer , “Precautions taken against various potential attacks in ISO/IEC DIS 9796”, Advances in Cryptology–EUROCRYPT ’90 (LNCS 473), 465–473, 1991.
L.C. Guillou and M. Ugon , “Smart card – a highly reliable and portable security device”, Advances in Cryptology–CRYPTO ’86 (LNCS 263), 464–479, 1987.

L.C. Guillou , M. Ugon , and J.-J. Quisquater , “The smart card: A standardized security device dedicated to public cryptology”, G.J. Simmons , editor, Contemporary Cryptology: The Science of Information Integrity, 561–613, IEEE Press, 1992.
C.G. Günther , “Alternating step generators controlled by de Bruijn sequences”, Advances in Cryptology–EUROCRYPT ’87 (LNCS 304), 5–14, 1988.
C.G. Günther , “A universal algorithm for homophonic coding”, Advances in Cryptology–EUROCRYPT ’88 (LNCS 330), 405–414, 1988.
C.G. Günther , “An identity-based key-exchange protocol”, Advances in Cryptology–EUROCRYPT ’89 (LNCS 434), 29–37, 1990.
H. Gustafson , Statistical Analysis of Symmetric Ciphers, PhD thesis, Queensland University of Technology, 1996.
H. Gustafson , E. Dawson , and J. Golić , “Randomness measures related to subset occurrence”, E. Dawson and J. Golić , editors, Cryptography:Policy and Algorithms, International Conference, Brisbane, Queensland, Australia, July 1995 (LNCS 1029), 132–143, 1996.
H. Gustafson , E. Dawson , L. Nielsen , and W. Caelli , “A computer package for measuring the strength of encryption algorithms”, Computers & Security, 13 (1994), 687–697.
A. Guyot , “OCAPI: Architecture of a VLSI coprocessor for the gcd and extended gcd of large numbers”, Proceedings of the 10th IEEE Symposium on Computer Arithmetic, 226–231, IEEE Press, 1991.
S. Haber and W. S. Stornetta , “How to time-stamp a digital document”, Journal of Cryptology, 3 (1991), 99–111.
J.L. Hafner and K.S. Mccurley , “On the distribution of running times of certain integer factoring algorithms”, Journal of Algorithms, 10 (1989), 531–556.
J.L. Hafner and K.S. Mccurley , “A rigorous subexponential algorithm for computation of class groups”, Journal of the American Mathematical Society, 2 (1989), 837–850.
T. Hansen and G.L. Mullen , “Primitive polynomials over finite fields”, Mathematics of Computation, 59 (1992), 639–643.
G.H. Hardy , A Mathematician’s Apology, Cambridge University Press, London, 1967.
G.H. Hardy and E.M. Wright , An Introduction to the Theory of Numbers, Clarendon Press, Oxford, 5th edition, 1979.
C. Harpes , G.G. Kramer , and J.L. Massey , “A generalization of linear cryptanalysis and the applicability of Matsui’s piling-up lemma”, Advances in Cryptology–EUROCRYPT ’95 (LNCS 921), 24–38, 1995.
V. Harris , “An algorithm for finding the greatest common divisor”, Fibonacci Quarterly, 8 (1970), 102–103.
J. Håstad , A.W. Schrift , and A. Shamir , “The discrete logarithm modulo a composite hides O(n) bits”, Journal of Computer and System Sciences, 47 (1993), 376–404.
J. Håstad , “Solving simultaneous modular equations of low degree”, SIAM Journal on Computing, 17 (1988), 336–341.
J. Håstad , “Pseudo-random generators under uniform assumptions”, Proceedings of the 22nd Annual ACM Symposium on Theory of Computing, 395–404, 1990.
R. Heiman , “A note on discrete logarithms with special structure”, Advances in Cryptology–EUROCRYPT ’92 (LNCS 658), 454–457, 1993.
R. Heiman , “Secure audio teleconferencing: A practical solution”, Advances in Cryptology–EUROCRYPT ’92 (LNCS 658), 437–448, 1993.
M.E. Hellman , “An extension of the Shannon theory approach to cryptography”, IEEE Transactions on Information Theory,23 (1977), 289–294.
M.E. Hellman , “A cryptanalytic time-memory tradeoff”, IEEE Transactions on Information Theory, 26 (1980), 401–406.
M.E. Hellman and C.E. Bach , “Method and apparatus for use in public-key data encryption system”, U.S. Patent #4,633,036, 30 Dec 1986.
M.E. Hellman , B.W. Diffie , and R.C. Merkle , “Cryptographic apparatus and method”, U.S. Patent # 4,200,770, 29 Apr 1980.
M.E. Hellman , R. Merkle , R. Schroeppel , L. Washington , W. Diffie , S. Pohlig , and P. Schweitzer , “Results of an initial attempt to cryptanalyze the NBS Data Encryption Standard”, Technical Report SEL 76–042, Information Systems Laboratory, Stanford University, Palo Alto, California, Sept. 9 1976 (revised Nov 10 1976).
M.E. Hellman and R.C. Merkle , “Public key cryptographic apparatus and method”, U.S. Patent #4,218,582, 19 Aug 1980.
M.E. Hellman and S.C. Pohlig , “Exponentiation cryptographic apparatus and method”, U.S. Patent # 4,424,414, 3 Jan 1984.
M.E. Hellman and J.M. Reyneri , “Fast computation of discrete logarithms in GF(q)”, Advances in Cryptology–Proceedings of Crypto 82, 3–13, 1983.
I.N. Herstein , Topics in Algebra, Xerox College Pub., Lexington, Massachusetts, 2nd edition, 1975.
L.S. Hill , “Cryptography in an algebraic alphabet”, American Mathematical Monthly,36 (1929), 306–312.
L.J. Hoffman , Modern Methods for Computer Security and Privacy, Prentice Hall, Englewood Cliffs, New Jersey, 1977.
R.V. Hogg and E.A. Tanis , Probability and statistical inference, Macmillan Publishing Company, New York, 3rd edition, 1988.
W. Hohl , X. Lai , T. Meier , and C. Waldvogel , “Security of iterated hash functions based on block ciphers”, Advances in Cryptology–CRYPTO ’93 (LNCS 773), 379–390, 1994.
S.-M. Hong , S.-Y. Oh , and H. Yoon , “New modular multiplication algorithms for fast modular exponentiation”, Advances in Cryptology–EUROCRYPT ’96 (LNCS 1070), 166–177, 1996.
P. Horster and H.-J. Knobloch , “Discrete logarithm based protocols”, Advances in Cryptology–EUROCRYPT ’91 (LNCS 547), 399–408, 1991.
P. Horster , M. Michels , and H. Petersen , “Meta-message recovery and metablind signature schemes based on the discrete logarithm problem and their applications”, Advances in Cryptology–ASIACRYPT ’94 (LNCS 917), 224–237, 1995.
P. Horster and H. Petersen , “Generalized ElGamal signatures (in German)”, Sicherheit in Informationssystemen, Proceedings der Fachtagung SIS’94, 89–106, Verlag der Fachvereine Zürich, 1994.
T.W. Hungerford , Algebra, Holt, Rinehart and Winston, New York, 1974.
K. Hwang , Computer Arithmetic, Principles, Architecture and Design, John Wiley & Sons, New York, 1979.
C. I’anson and C. Mitchell , “Security defects in CCITT Recommendation X.509 – The directory authentication framework”, Computer Communication Review, 20 (1990), 30–34.
R. Impagliazzo , L. Levin , and M. Luby , “Pseudo-random generation from one-way functions”, Proceedings of the 21st Annual ACM Symposium on Theory of Computing, 12–24, 1989.
R. Impagliazzo and M. Naor , “Efficient cryptographic schemes provably as secure as subset sum”, Proceedings of the IEEE 30th Annual Symposium on Foundations of Computer Science, 236–241, 1989.
I. Ingemarsson and G.J. Simmons , “A protocol to set up shared secret schemes without the assistance of a mutually trusted party”, Advances in Cryptology–EUROCRYPT ’90 (LNCS 473), 266–282, 1991.

I. Ingemarsson , D.T. Tang , and C.K. Wong , “A conference key distribution system”, IEEE Transactions on Information Theory, 28 (1982), 714–720.
K. Ireland and M. Rosen , A Classical Introduction to Modern Number Theory, Springer-Verlag, New York, 2nd edition, 1990.
ISO 7498-2 , “Information processing systems – Open Systems Interconnection – Basic reference model – Part 2: Security architecture”, International Organization for Standardization, Geneva, Switzerland, 1989 (first edition) (equivalent to ITU-T Rec. X.800).
ISO 8372 , “Information processing – Modes of operation for a 64-bit block cipher algorithm”, International Organization for Standardization, Geneva, Switzerland, 1987 (first edition; confirmed 1992).
ISO 8730 , “Banking – Requirements for message authentication (wholesale)”, International Organization for Standardization, Geneva, Switzerland, 1990 (second edition).
ISO 8731-1 , “Banking – Approved algorithms for message authentication – Part 1: DEA”, International Organization for Standardization, Geneva, Switzerland, 1987 (first edition; confirmed 1992).
ISO 8731-2 , “Banking – Approved algorithms for message authentication – Part 2: Message authenticator algorithm”, International Organization for Standardization, Geneva, Switzerland, 1992 (second edition).
ISO 8732 , “Banking – Key management (wholesale)”, International Organization for Standardization, Geneva, Switzerland, 1988 (first edition).
ISO 9564-1 , “Banking – Personal Identification Number management and security – Part 1: PIN protection principles and techniques”, International Organization for Standardization, Geneva, Switzerland, 1990.
ISO 9564-2 , “Banking – Personal Identification Number management and security – Part 2: Approved algorithm(s) for PIN encipherment”, International Organization for Standardization, Geneva, Switzerland, 1991.
ISO 9807 , “Banking and related financial services – Requirements for message authentication (retail)”, International Organization for Standardization, Geneva, Switzerland, 1991.
ISO 10126-1 , “Banking – Procedures for message encipherment (wholesale) – Part 1: General principles”, International Organization for Standardization, Geneva, Switzerland, 1991.
ISO 10126-2 , “Banking – Procedures for message encipherment (wholesale) – Part 2: Algorithms”, International Organization for Standardization, Geneva, Switzerland, 1991.
ISO 10202-7 , “Financial transaction cards – Security architecture of financial transaction systems using integrated circuit cards – Part 7: Key management”, draft (DIS), 1994.
ISO 11131 , “Banking – Financial institution sign-on authentication”, International Organization for Standardization, Geneva, Switzerland, 1992.
ISO 11166-1 , “Banking – Key management by means of asymmetric algorithms – Part 1: Principles, procedures and formats”, International Organization for Standardization, Geneva, Switzerland, 1994.
ISO 11166-2 , “Banking – Key management by means of asymmetric algorithms – Part 2: Approved algorithms using the RSA cryptosystem”, International Organization for Standardization, Geneva, Switzerland, 1995.
ISO 11568-1 , “Banking – Key management (retail) – Part 1: Introduction to key management”, International Organization for Standardization, Geneva, Switzerland, 1994.
ISO 11568-2 , “Banking – Key management (retail) – Part 2: Key management techniques for symmetric ciphers”, International Organization for Standardization, Geneva, Switzerland, 1994.
ISO 11568-3 , “Banking – Key management (retail) – Part 3: Key life cycle for symmetric ciphers”, International Organization for Standardization, Geneva, Switzerland, 1994.
ISO 11568-4 , “Banking – Key management (retail) – Part 4: Key management techniques using public key cryptography”, draft (DIS), 1996.
ISO 11568-5 , “Banking – Key management (retail) – Part 5: Key life cycle for public key cryptosystems”, draft (DIS), 1996.
ISO 11568-6 , “Banking – Key management (retail) – Part 6: Key management schemes”, draft (CD), 1996.
ISO/IEC 9594-1 , “Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models, and services”, International Organization for Standardization, Geneva, Switzerland, 1995 (equivalent to ITU-T Rec. X.500, 1993).
ISO/IEC 9594-8 , “Information technology – Open Systems Interconnection – The Directory: Authentication framework”, International Organization for Standardization, Geneva, Switzerland, 1995 (equivalent to ITU-T Rec. X.509, 1993).
ISO/IEC 9796 , “Information technology – Security techniques – Digital signature scheme giving message recovery”, International Organization for Standardization, Geneva, Switzerland, 1991 (first edition).
ISO/IEC 9797 , “Information technology – Security techniques – Data integrity mechanism using a cryptographic check function employing a block cipher algorithm”, International Organization for Standardization, Geneva, Switzerland, 1994 (second edition).
ISO/IEC 9798-1 , “Information technology – Security techniques – Entity authentication mechanisms – Part 1: General model”, International Organization for Standardization, Geneva, Switzerland, 1991 (first edition).
ISO/IEC 9798-2 , “Information technology – Security techniques – Entity authentication – Part 2: Mechanisms using symmetric encipherment algorithms”, International Organization for Standardization, Geneva, Switzerland, 1994 (first edition).
ISO/IEC 9798-3 , “Information technology – Security techniques – Entity authentication mechanisms – Part 3: Entity authentication using a public-key algorithm”, International Organization for Standardization, Geneva, Switzerland, 1993 (first edition).
ISO/IEC 9798-4 , “Information technology – Security techniques – Entity authentication – Part 4: Mechanisms using a cryptographic check function”, International Organization for Standardization, Geneva, Switzerland, 1995 (first edition).
ISO/IEC 9798-5 , “Information technology – Security techniques – Entity authentication – Part 5: Mechanisms using zero knowledge techniques”, draft (CD), 1996.
ISO/IEC 9979 , “Data cryptographic techniques – Procedures for the registration of cryptographic algorithms”, International Organization for Standardization, Geneva, Switzerland, 1991 (first edition).
ISO/IEC 10116 , “Information processing – Modes of operation for an n-bit block cipher algorithm”, International Organization for Standardization, Geneva, Switzerland, 1991 (first edition).
ISO/IEC 10118-1 , “Information technology – Security techniques – Hash-functions – Part 1: General”, International Organization for Standardization, Geneva, Switzerland, 1994.
ISO/IEC 10118-2 , “Information technology – Security techniques – Hash-functions – Part 2: Hash-functions using an n-bit block cipher algorithm”, International Organization for Standardization, Geneva, Switzerland, 1994.

ISO/IEC 10118-3 , “Information technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions”, draft (CD), 1996.
ISO/IEC 10118-4 , “Information technology – Security techniques – Hash-functions – Part 4: Hash-functions using modular arithmetic”, draft (CD), 1996.
ISO/IEC 10181-1 , “Information technology – Open Systems Interconnection – Security frameworks for open systems – Part 1: Overview”, International Organization for Standardization, Geneva, Switzerland, 1996 (equivalent to ITU-T Rec. X.810, 1995).
ISO/IEC 10181-2 , “Information technology – Open Systems Interconnection – Security frameworks for open systems – Part 2: Authentication framework”, International Organization for Standardization, Geneva, Switzerland, 1996 (equivalent to ITU-T Rec. X.811, 1995).
ISO/IEC 10181-3 , “Information technology – Open Systems Interconnection – Security frameworks for open systems – Part 3: Access control framework”, 1996.
ISO/IEC 10181-4 , “Information technology – Open Systems Interconnection – Security frameworks for open systems – Part 4: Non-repudiation framework”, 1996.
ISO/IEC 10181-5 , “Information technology – Open Systems Interconnection – Security frameworks for open systems – Part 5: Confidentiality framework”, 1996.
ISO/IEC 10181-6 , “Information technology – Open Systems Interconnection – Security frameworks for open systems – Part 6: Integrity framework”, 1996.
ISO/IEC 10181-7 , “Information technology – Open Systems Interconnection – Security frameworks for open systems – Part 7: Security audit and alarms framework”, 1996.
ISO/IEC 11770-1 , “Information technology – Security techniques – Key management – Part 1: Framework”, draft (DIS), 1996.
ISO/IEC 11770-2 , “Information technology – Security techniques – Key management – Part 2: Mechanisms using symmetric techniques”, International Organization for Standardization, Geneva, Switzerland, 1996 (first edition).
ISO/IEC 11770-3 , “Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques”, draft (DIS), 1996.
ISO/IEC 13888-1 , “Information technology – Security techniques – Non-repudiation – Part 1: General model”, draft (CD), 1996.
ISO/IEC 13888-2 , “Information technology – Security techniques – Non-repudiation – Part 2: Using symmetric encipherment algorithms”, draft (CD), 1996.
ISO/IEC 13888-3 , “Information technology – Security techniques – Non-repudiation – Part 3: Using asymmetric techniques”, draft (CD), 1996.
ISO/IEC 14888-1 , “Information technology – Security techniques – Digital signatures with appendix – Part 1: General”, draft (CD), 1996.
ISO/IEC 14888-2 , “Information technology – Security techniques – Digital signatures with appendix – Part 2: Identity-based mechanisms”, draft (CD), 1996.
ISO/IEC 14888-3 , “Information technology – Security techniques – Digital signatures with appendix – Part 3: Certificate-based mechanisms”, draft (CD), 1996.
M. Ito , A. Saito , and T. Nishizeki , “Secret sharing scheme realizing general access structure”, IEEE Global Telecommunications Conference, 99–102, 1987.
ITU-T REC. X.509 (REVISED) , “The Directory – Authentication framework”, International Telecommunication Union, Geneva, Switzerland, 1993 (equivalent to ISO/IEC 9594–8:1994).
ITU-T REC. X.509 (1993) TECHNICAL CORRIGENDUM 1 , “The Directory – Authentication framework”, International Telecommunication Union, Geneva, Switzerland, July 1995 (equivalent to Technical Corrigendum 1 to ISO/IEC 9594–8:1994).
ITU-T REC. X. 509(1993) AMENDMENT 1: CERTIFICATE EXTENSIONS , “The Directory – Authentication framework”, International Telecommunication Union, Geneva, Switzerland, July 1995 draft for JCT1 letter ballot (equivalent to Ammendment 1 to ISO/IEC 9594–8:1994).
W.-A. Jackson , K.M. Martin , and C.M. O’keefe , “Multisecret threshold schemes”, Advances in Cryptology–CRYPTO ’93 (LNCS 773), 126–135, 1994.
G. Jaeschke , “On strong pseudoprimes to several bases”, Mathematics of Computation, 61 (1993), 915–926.
C.J.A. Jansen and D.E. Boekee , “On the significance of the directed acyclic word graph in cryptology”, Advances in Cryptology–AUSCRYPT ’90 (LNCS 453), 318–326, 1990.
C.J.A. Jansen and D.E. Boekee , “The shortest feedback shift register that can generate a given sequence”, Advances in Cryptology–CRYPTO ’89 (LNCS 435), 90–99, 1990.
T. Jebelean , “Comparing several gcd algorithms”, Proceedings of the 11th Symposium on Computer Arithmetic, 180–185, IEEE Press, 1993.
J. Jedwab and C. Mitchell , “Minimum weight modified signed-digit representations and fast exponentiation”, Electronics Letters, 25 (August 17, 1989), 1171–1172.
N. Jefferies , C. Mitchell , and M. Walker , “A proposed architecture for trusted third party services”, E. Dawson and J. Golić , editors, Cryptography:Policy and Algorithms, International Conference, Brisbane, Queensland, Australia, July 1995 (LNCS 1029), 98–104, 1996.
H.N. Jendal , Y.J.B. Kuhn , and J.L. Massey , “An information-theoretic treatment of homophonic substitution”, Advances in Cryptology–EUROCRYPT ’89 (LNCS 434), 382–394, 1990.
S.M. Jennings , “Multiplexed sequences: Some properties of the minimum polynomial”, Cryptography–Proceedings of the Workshop on Cryptography, Burg Feuerstein (LNCS 149), 189–206, 1983.
T. Johansson , G. Kabatianskii , and B. Smeets , “On the relation between A-codes and codes correcting independent errors”, Advances in Cryptology–EUROCRYPT ’93 (LNCS 765), 1–11, 1994.
D.B. Johnson , A. Le , W. Martin , S. Matyas , and J. Wilkins , “Hybrid key distribution scheme giving key record recovery”, IBM Technical Disclosure Bulletin,37 (1994), 5–16.
D.B. Johnson and S.M. Matyas , “Asymmetric encryption: Evolution and enhancements”, CryptoBytes, 2 (Spring 1996), 1–6.
D.S. Johnson , “The NP-completeness column: an ongoing guide”, Journal of Algorithms, 9 (1988), 426–444.
R.W. Jones , “Some techniques for handling encipherment keys”, ICL Technical Journal,3 (1982), 175–188.
R.R. Jueneman , “Analysis of certain aspects of output feedback mode”, Advances in Cryptology–Proceedings of Crypto 82, 99–127, 1983.
R.R. Jueneman , “A high speed manipulation detection code”, Advances in Cryptology–CRYPTO ’86 (LNCS 263), 327–346, 1987.

R.R. Jueneman , S.M. Matyas , and C.H. Meyer , “Message authentication with manipulation detection codes”, Proceedings of the 1983 IEEE Symposium on Security and Privacy, 33–54, 1984.
D. Jungnickel , Finite Fields: Structure and Arithmetics, Bibliographisches Institut – Wissenschaftsverlag, Mannheim, 1993.
M. Just , E. Kranakis , D. Krizanc , and P. Van Oorschot , “On key distribution via true broadcasting”, 2nd ACM Conference on Computer and Communications Security, 81–88, ACM Press, 1994.
D. Kahn , The Codebreakers, Macmillan Publishing Company, New York, 1967.
B.S. Kaliski Jr. , “A chosen message attack on Demytko’s elliptic curve cryptosystem”, Journal of Cryptology, to appear.
B.S. Kaliski Jr. , “A pseudo-random bit generator based on elliptic logarithms”, Advances in Cryptology–CRYPTO ’86 (LNCS 263), 84–103, 1987.
B.S. Kaliski Jr. , Elliptic curves and cryptography: a pseudorandom bit generator and other tools, PhD thesis, MIT Department of Electrical Engineering and Computer Science, 1988.
B.S. Kaliski Jr. , “Anderson’s RSA trapdoor can be broken”, Electronics Letters, 29 (July 22, 1993), 1387–1388.
B.S. Kaliski Jr. , “The Montgomery inverse and its applications”, IEEE Transactions on Computers, 44 (1995), 1064–1065.
B.S. Kaliski Jr., R.L. Rivest , and A.T. Sherman , “Is the Data Encryption Standard a group? (Results of cycling experiments on DES)”, Journal of Cryptology, 1 (1988), 3–36.
B.S. Kaliski Jr . and M. Robshaw , “The secure use of RSA”, CryptoBytes, 1 (Autumn 1995), 7–13.
B.S. Kaliski Jr. and Y.L. Yin , “On differential and linear cryptanalysis of the RC5 encryption algorithm”, Advances in Cryptology–CRYPTO ’95 (LNCS 963), 171–184, 1995.
E. Kaltofen , “Analysis of Coppersmith’s block Wiedemann algorithm for the parallel solution of sparse linear systems”, Mathematics of Computation, 64 (1995), 777–806.
E. Kaltofen and V. Shoup , “Subquadratic-time factoring of polynomials over finite fields”, Proceedings of the 27th Annual ACM Symposium on Theory of Computing, 398–406, 1995.
J. Kam and G. Davida , “Structured design of substitution-permutation encryption networks”, IEEE Transactions on Computers, 28 (1979), 747–753.
N. Kapidzic and A. Davidson , “A certificate management system: structure, functions and protocols”, Proceedings of the Internet Society Symposium on Network and Distributed System Security, 153–160, IEEE Computer Society Press, 1995.
A. Karatsuba and Yu. Ofman , “Multiplication of multidigit numbers on automata”, Soviet Physics – Doklady, 7 (1963), 595–596.
E.D. Karnin , J.W. Greene , and M.E. Hellman , “On secret sharing systems”, IEEE Transactions on Information Theory,29 (1983), 35–41.
A. Kehne , J. Schöwälder , and H. Langendörfer , “A nonce-based protocol for multiple authentications”, Operating Systems Review, 26 (1992), 84–89.
R. Kemmerer , C. Meadows , and J. Millen , “Three systems for cryptographic protocol analysis”, Journal of Cryptology,7 (1994), 79–130.
S. Kent , “Encryption-based protection protocols for interactive user-computer communication”, MIT/LCS/TR-162 (M. Sc. thesis), MIT Laboratory for Computer Science, 1976.
S. Kent , “Internet privacy enhanced mail”, Communications of the ACM, 36 (1993), 48–60.
S. Kent , “Internet security standards: past, present and future”, StandardView, 2 (1994), 78–85.
A. Kerckhoffs , “La cryptographie militaire”, Journal des Sciences Militaires,9th Series (February 1883), 161–191.
I. Kessler and H. Krawczyk , “Minimum buffer length and clock rate for the shrinking generator cryptosystem”, IBM Research Report RC 19938, IBM T.J. Watson Research Center, Yorktown Heights, N.Y., 10598, U.S.A., 1995.
E. Key , “An analysis of the structure and complexity of nonlinear binary sequence generators”, IEEE Transactions on Information Theory, 22 (1976), 732–736.
J. Kilian and T. Leighton , “Fair cryptosystems, revisited: A rigorous approach to key-escrow”, Advances in Cryptology–CRYPTO ’95 (LNCS 963), 208–221, 1995.
J. Kilian and P. Rogaway , “How to protect DES against exhaustive key search”, Advances in Cryptology–CRYPTO ’96 (LNCS 1109), 252–267, 1996.
S.-H. Kim and C. Pomerance , “The probability that a random probable prime is composite”, Mathematics of Computation,53 (1989), 721–741.
M. Kimberley , “Comparison of two statistical tests for keystream sequences”, Electronics Letters, 23 (April 9, 1987), 365–366.
A. Klapper , “The vulnerability of geometric sequences based on fields of odd characteristic”, Journal of Cryptology, 7 (1994), 33–51.
A. Klapper and M. Goresky , “Feedback shift registers, combiners with memory, and 2-adic span”, Journal of Cryptology, to appear.
A. Klapper and M. Goresky , “2-Adic shift registers”, R. Anderson , editor, Fast Software Encryption, Cambridge Security Workshop (LNCS 809), 174–178, Springer-Verlag, 1994.
A. Klapper and M. Goresky , “Cryptanalysis based on 2-adic rational approximation”, Advances in Cryptology–CRYPTO ’95 (LNCS 963), 262–273, 1995.
A. Klapper and M. Goresky , “Large period nearly de Bruijn FCSR sequences”, Advances in Cryptology–EUROCRYPT ’95 (LNCS 921), 263–273, 1995.
D.V. Klein , “Foiling the cracker: a survey of, and improvements to, password security”, Proceedings of the 2nd USENIX UNIX Security Workshop, 5–14, 1990.
H.-J. Knobloch , “A smart card implementation of the Fiat-Shamir identification scheme”, Advances in Cryptology–EUROCRYPT ’88 (LNCS 330), 87–95, 1988.
L.R. Knudsen , “Cryptanalysis of LOKI”, Advances in Cryptology–ASIACRYPT ’91 (LNCS 739), 22–35, 1993.
L.R. Knudsen , “Cryptanalysis of LOKI91”, Advances in Cryptology–AUSCRYPT ’92 (LNCS 718), 196–208, 1993.
L.R. Knudsen , Block Ciphers – Analysis, Design and Applications, PhD thesis, Computer Science Department, Aarhus University (Denmark), 1994.
L.R. Knudsen , “A key-schedule weakness in SAFER K-64”, Advances in Cryptology–CRYPTO ’95 (LNCS 963), 274–286, 1995.
L.R. Knudsen , “Truncated and higher order differentials”, B. Preneel , editor, Fast Software Encryption, Second International Workshop (LNCS 1008), 196–211, Springer-Verlag, 1995.
L.R. Knudsen and T. Berson , “Truncated differentials of SAFER”, D. Gollmann , editor, Fast Software Encryption, Third International Workshop (LNCS 1039), 15–26, Springer-Verlag, 1996.

L.R. Knudsen and X. Lai , “New attacks on all double block length hash functions of hash rate 1, including the parallel-DM”, Advances in Cryptology–EUROCRYPT ’94 (LNCS 950), 410–418, 1995.
L.R. Knudsen and W. Meier , “Improved differential attacks on RC5”, Advances in Cryptology–CRYPTO ’96 (LNCS 1109), 216–228, 1996.
L.R. Knudsen and T. Pedersen , “On the difficulty of software key escrow”, Advances in Cryptology–EUROCRYPT ’96 (LNCS 1070), 237–244, 1996.
D.E. Knuth , The Art of Computer Programming – Fundamental Algorithms, volume 1, Addison-Wesley, Reading, Massachusetts, 2nd edition, 1973.
D.E. Knuth , The Art of Computer Programming – Seminumerical Algorithms, volume 2, Addison-Wesley, Reading, Massachusetts, 2nd edition, 1981.
D.E. Knuth , The Art of Computer Programming – Sorting and Searching, volume 3, Addison-Wesley, Reading, Massachusetts, 1973.
D.E. Knuth and L. Trabb Pardo , “Analysis of a simple factorization algorithm”, Theoretical Computer Science, 3 (1976), 321–348.
N. Koblitz , “Elliptic curve cryptosystems”, Mathematics of Computation, 48 (1987), 203–209.
N. Koblitz , “Hyperelliptic cryptosystems”, Journal of Cryptology, 1 (1989), 139–150.
N. Koblitz , A Course in Number Theory and Cryptography, Springer-Verlag, New York, 2nd edition, 1994.
C. Koç , “High-speed RSA implementation”, Technical Report, RSA Laboratories, 1994.
C. Koç , “RSA hardware implementation”, Technical Report TR-801, RSA Laboratories, 1996.
C. Koç , T. Acar , and B.S. Kaliski Jr. , “Analyzing and comparing Montgomery multiplication algorithms”, IEEE Micro, 16 (1996), 26–33.
J.T. Kohl , “The use of encryption in Kerberos for network authentication”, Advances in Cryptology–CRYPTO ’89 (LNCS 435), 35–43, 1990.
L. M. Kohnfelder , “A method for certification”, MIT Laboratory for Computer Science, unpublished (essentially pp. 39–43 of [703]), 1978.
L. M. Kohnfelder , Toward a practical public-key cryptosystem, B. Sc. thesis, MIT Department of Electrical Engineering, 1978.
A. Kolmogorov , “Three approaches to the definition of the concept ‘quantity of information”’, Problemy Peredachi Informatsii,1 (1965), 3–11.
A.G. Konheim , Cryptography, A Primer, John Wiley & Sons, New York, 1981.
I. Koren , Computer Arithmetic Algorithms, Prentice Hall, Englewood Cliffs, New Jersey, 1993.
V.I. Korzhik and A.I. Turkin , “Cryptanalysis of McEliece’s public-key cryptosystem”, Advances in Cryptology–EUROCRYPT ’91 (LNCS 547), 68–70, 1991.
K. Koyama , U. Maurer , T. Okamoto , and S.A. Vanstone , “New public-key schemes based on elliptic curves over the ring Zn”, Advances in Cryptology–CRYPTO ’91 (LNCS 576), 252–266, 1992.
K. Koyama and R. Terada , “How to strengthen DES-like cryptosystems against differential cryptanalysis”, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Science, E76-A (1993), 63–69.
E. Kranakis , Primality and Cryptography, John Wiley & Sons, Stuttgart, 1986.
D.W. Kravitz , “Digital signature algorithm”, U.S. Patent #5,231,668, 27 Jul 1993.
H. Krawczyk , “How to predict congruential generators”, Advances in Cryptology–CRYPTO ’89 (LNCS 435), 138–153, 1990.
H. Krawczyk , “How to predict congruential generators”, Journal of Algorithms, 13 (1992), 527–545. An earlier version appeared in [712].
H. Krawczyk , “LFSR-based hashing and authentication”, Advances in Cryptology–CRYPTO ’94 (LNCS 839), 129–139, 1994.
H. Krawczyk , “Secret sharing made short”, Advances in Cryptology–CRYPTO ’93 (LNCS 773), 136–146, 1994.
H. Krawczyk , “The shrinking generator: Some practical considerations”, R. Anderson , editor, Fast Software Encryption, Cambridge Security Workshop (LNCS 809), 45–46, Springer- Verlag, 1994.
H. Krawczyk , “New hash functions for message authentication”, Advances in Cryptology–EUROCRYPT ’95 (LNCS 921), 301–310, 1995.
H. Krawczyk , “SKEME: A versatile secure key exchange mechanism for Internet”, Proceedings of the Internet Society Symposium on Network and Distributed System Security, 114–127, IEEE Computer Society Press, 1996.
Y. Kurita and M. Matsumoto , “Primitive t-nomials (t = 3,5) over GF(2) whose degree is a Mersenne exponent < 44497”, Mathematics of Computation, 56 (1991), 817–821.
K. Kurosawa , T. Ito , and M. Takeuchi , “Public key cryptosystem using a reciprocal number with the same intractability as factoring a large number”, Cryptologia, 12 (1988), 225–233.
K. Kurosawa , K. Okada , and S. Tsujii , “Low exponent attack against elliptic curve RSA”, Advances in Cryptology–ASIACRYPT ’94 (LNCS 917), 376–383, 1995.
K. Kusuda and T. Matsumoto , “Optimization of time-memory trade-off cryptanalysis and its application to DES, FEAL-32, and Skipjack”, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Science, E79-A (1996), 35–48.
J.C. Lagarias , “Knapsack public key cryptosystems and diophantine approximation”, Advances in Cryptology–Proceedings of Crypto 83, 3–23, 1984.
J.C. Lagarias , “Pseudorandom number generators in cryptography and number theory”, C. Pomerance , editor, Cryptology and Computational Number Theory, volume 42 of Proceedings of Symposia in Applied Mathematics, 115–143, American Mathematical Society, 1990.
X. Lai , “Condition for the nonsingularity of a feedback shift-register over a general finite field”, IEEE Transactions on Information Theory, 33 (1987), 747–749.
X. Lai , “On the design and security of block ciphers”, ETH Series in Information Processing, J.L. Massey (editor), vol. 1, Hartung-Gorre Verlag Konstanz, Technische Hochschule (Zurich), 1992.
X. Lai and L.R. Knudsen , “Attacks on double block length hash functions”, R. Anderson , editor, Fast Software Encryption, Cambridge Security Workshop (LNCS 809), 157–165, Springer-Verlag, 1994.
X. Lai and J.L. Massey , “A proposal for a new block encryption standard”, Advances in Cryptology–EUROCRYPT ’90 (LNCS 473), 389–404, 1991.
X. Lai and J.L. Massey , “Hash functions based on block ciphers”, Advances in Cryptology–EUROCRYPT ’92 (LNCS 658), 55–70, 1993.
X. Lai , J.L. Massey , and S. Murphy , “Markov ciphers and differential cryptanalysis”, Advances in Cryptology–EUROCRYPT ’91 (LNCS 547), 17–38, 1991.
X. Lai , R.A. Rueppel , and J. Woollven , “A fast cryptographic checksum algorithm based on stream ciphers”, Advances in Cryptology–AUSCRYPT ’92 (LNCS 718), 339–348, 1993.

C.-S. Laih , L. Harn , J.-Y. Lee , and T. Hwang , “Dynamic threshold scheme based on the definition of cross-product in an n-dimensional linear space”, Advances in Cryptology–CRYPTO ’89 (LNCS 435), 286–298, 1990.
C.-S. Laih , F.-K. Tu , and W.-C. Tai , “On the security of the Lucas function”, Information Processing Letters, 53 (1995), 243–247.
K.-Y. Lam and T. Beth , “Timely authentication in distributed systems”, Y. Deswarte , G. Eizenberg , and J.-J. Quisquater , editors, Second European Symposium on Research in Computer Security – ESORICS’92 (LNCS 648), 293–303, Springer-Verlag, 1992.
K.-Y. Lam and L.C.K. Hui , “Efficiency of SS(I) square-and-multiply exponentiation algorithms”, Electronics Letters, 30 (December 8, 1994), 2115–2116.
B.A. Lamacchia and A.M. Odlyzko , “Computation of discrete logarithms in prime fields”, Designs, Codes and Cryptography,1 (1991), 47–62.
B.A. Lamacchia and A.M. Odlyzko , “Solving large sparse linear systems over finite fields”, Advances in Cryptology–CRYPTO ’90 (LNCS 537), 109–133, 1991.
L. Lamport , “Constructing digital signatures from a one-way function”, Technical report CSL-98, SRI International, Palo Alto, 1979.
L. Lamport , “Password authentication with insecure communication”, Communications of the ACM, 24 (1981), 770–772.
B. Lampson , M. Abadi , M. Burrows , and E. Wobber , “Authentication in distributed systems: Theory and practice”, ACM Transactions on Computer Systems,10 (1992), 265–310.
S.K. Langford and M.E. Hellman , “Differential-linear cryptanalysis”, Advances in Cryptology–CRYPTO ’94 (LNCS 839), 17–25, 1994.
P.J. Lee and E.F. Brickell , “An observation on the security of McEliece’s public-key cryptosystem”, Advances in Cryptology–EUROCRYPT ’88 (LNCS 330), 275–280, 1988.
D.H. Lehmer , “Euclid’s algorithm for large numbers”, American Mathematical Monthly, 45 (1938), 227–233.
D.H. Lehmer and R.E. Powers , “On factoring large numbers”, Bulletin of the AMS,37 (1931), 770–776.
T. Leighton and S. Micali , “Secret-key agreement without public-key cryptography”, Advances in Cryptology–CRYPTO ’93 (LNCS 773), 456–479, 1994.
A.K. Lenstra , “Posting to sci.crypt”, April 11 1996.
A.K. Lenstra , “Primality testing”, C. Pomerance , editor, Cryptology and Computational Number Theory, volume 42 of Proceedings of Symposia in Applied Mathematics, 13–25, American Mathematical Society, 1990.
A.K. Lenstra and H.W. Lenstra Jr. , “Algorithms in number theory”, J. Van Leeuwen , editor, Handbook of Theoretical Computer Science, 674–715, Elsevier Science Publishers, 1990.
A.K. Lenstra and H.W. Lenstra Jr. , The Development of the Number Field Sieve, Springer-Verlag, Berlin, 1993.
A.K. Lenstra , H.W. Lenstra Jr., and L. Lovász , “Factoring polynomials with rational coefficients”, Mathematische Annalen, 261 (1982), 515–534.
A.K. Lenstra , H.W. Lenstra Jr., M.S. Manasse , and J.M. Pollard , “The factorization of the ninth Fermat number”, Mathematics of Computation, 61 (1993), 319–349.
A.K. Lenstra , H.W. Lenstra Jr., M.S. Manasse , and J.M. Pollard , “The number field sieve”, A.K. Lenstra and H.W. Lenstra Jr., editors, The Development of the Number Field Sieve, volume 1554 of Lecture Notes in Mathematics, 11–42, Springer-Verlag, 1993.
A.K. Lenstra and M.S. Manasse , “Factoring by electronic mail”, Advances in Cryptology–EUROCRYPT ’89 (LNCS 434), 355–371, 1990.
A.K. Lenstra and M.S. Manasse “Factoring with two large primes”, Mathematics of Computation, 63 (1994), 785–798.
A.K. Lenstra , P. Winkler , and Y. Yacobi , “A key escrow system with warrant bounds”, Advances in Cryptology–CRYPTO ’95 (LNCS 963), 197–207, 1995.
H.W. Lenstra Jr. , “Factoring integers with elliptic curves”, Annals of Mathematics, 126 (1987), 649–673.
H.W. Lenstra Jr. , “Finding isomorphisms between finite fields”, Mathematics of Computation,56 (1991), 329–347.
H.W. Lenstra Jr. “On the Chor-Rivest knapsack cryptosystem”, Journal of Cryptology, 3 (1991), 149–155.
H.W. Lenstra Jr. and C. Pomerance , “A rigorous time bound for factoring integers”, Journal of the American Mathematical Society, 5 (1992), 483–516.
H.W. Lenstra Jr. and R.J. Schoof , “Primitive normal bases for finite fields”, Mathematics of Computation, 48 (1987), 217–231.
L.A. Levin , “One-way functions and pseudorandom generators”, Proceedings of the 17th Annual ACM Symposium on Theory of Computing, 363–365, 1985.
J. Levine , United States Cryptographic Patents 1861–1981, Cryptologia, Inc., Terre Haute, Indiana, 1983.
R. Lidl and W.B. Müller , “Permutation polynomials in RSA-cryptosystems”, Advances in Cryptology–Proceedings of Crypto 83, 293–301, 1984.
R. Lidl and H. Niederreiter , Finite Fields, Cambridge University Press, Cambridge, 1984.
A. Liebl , “Authentication in distributed systems: A bibliography”, Operating Systems Review, 27 (1993), 31–41.
C.H. Lim and P.J. Lee , “Another method for attaining security against adaptively chosen ciphertext attacks”, Advances in Cryptology–CRYPTO ’93 (LNCS 773), 420–434, 1994.
C.H. Lim and P.J. Lee , “More flexible exponentiation with precomputation”, Advances in Cryptology–CRYPTO ’94 (LNCS 839), 95–107, 1994.
C.H. Lim and P.J. Lee , “Server (prover/signer)-aided verification of identity proofs and signatures”, Advances in Cryptology–EUROCRYPT ’95 (LNCS 921), 64–78, 1995.
S. Lin and D. Costello , Error Control Coding: Fundamentals and Applications, Prentice Hall, Englewood Cliffs, New Jersey, 1983.
J. Lipson , Elements of Algebra and Algebraic Computing, Addison-Wesley, Reading, Massachusetts, 1981.
T.M.A. Lomas , L. Gong , J.H. Saltzer , and R.M. Needham , “Reducing risks from poorly chosen keys”, Operating Systems Review, 23 (Special issue), 14–18. (Presented at: 12th ACM Symposium on Operating Systems Principles, Litchfield Park, Arizona, Dec. 1989).
D.L. Long and A. Wigderson , “The discrete logarithm hides O(log n) bits”, SIAM Journal on Computing, 17 (1988), 363–372.
R. Lovorn , Rigorous, subexponential algorithms for discrete logarithms over finite fields, PhD thesis, University of Georgia, 1992.
M. Luby , Pseudorandomness and Cryptographic Applications, Princeton University Press, Princeton, New Jersey, 1996.
M. Luby and C. Rackoff , “Pseudorandom permutation generators and cryptographic composition”, Proceedings of the 18th Annual ACM Symposium on Theory of Computing, 356–363, 1986.
M. Luby and C. Rackoff , “How to construct pseudorandom permutations from pseudorandom functions”, SIAM Journal on Computing, 17 (1988), 373–386. An earlier version appeared in [775].

S. Lucks , “Faster Luby-Rackoff ciphers”, D. Gollmann , editor, Fast Software Encryption, Third International Workshop (LNCS 1039), 189–203, Springer-Verlag, 1996.
F.J. Macwilliams and N.J.A. Sloane , The Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1977 (fifth printing: 1986).
W. Madryga , “A high performance encryption algorithm”, J. Finch and E. Dougall , editors, Computer Security: A Global Challenge, Proceedings of the Second IFIP International Conference on Computer Security, 557–570, North-Holland, 1984.
D.P. Maher , “Crypto backup and key escrow”, Communications of the ACM,39 (1996), 48–53.
W. Mao and C. Boyd , “On the use of encryption in cryptographic protocols”, P.G. Farrell , editor, Codes and Cyphers: Cryptography and Coding IV, 251–262, Institute of Mathematics & Its Applications (IMA), 1995.
G. Marsaglia , “A current view of random number generation”, L. Billard , editor, Computer Science and Statistics: Proceedings of the Sixteenth Symposium on the Interface,3–10, North-Holland, 1985.
P. Martin-Löf , “The definition of random sequences”, Information and Control,9 (1966), 602–619.
J.L. Massey , “Shift-register synthesis and BCH decoding”, IEEE Transactions on Information Theory, 15 (1969), 122–127.
J.L. Massey , “An introduction to contemporary cryptology”, Proceedings of the IEEE,76 (1988), 533–549.
J.L. Massey , “Contemporary cryptology: An introduction”, G.J. Simmons , editor, Contemporary Cryptology: The Science of Information Integrity, 1–39, IEEE Press, 1992. An earlier version appeared in [785].
J.L. Massey , “SAFER K-64: A byte-oriented block-ciphering algorithm”, R. Anderson , editor, Fast Software Encryption, Cambridge Security Workshop (LNCS 809), 1–17, Springer-Verlag, 1994.
J.L. Massey , “SAFER K-64: One year later”, B. Preneel , editor, Fast Software Encryption, Second International Workshop (LNCS 1008), 212–241, Springer-Verlag, 1995.
J.L. Massey and I. Ingemarsson , “The Rip Van Winkle cipher – A simple and provably computationally secure cipher with a finite key”, IEEE International Symposium on Information Theory (Abstracts), p. 146, 1985.
J.L. Massey and X. Lai , “Device for converting a digital block and the use thereof”, European Patent # 482,154, 29 Apr 1992.
J.L. Massey and X. Lai , “Device for the conversion of a digital block and use of same”, U.S. Patent # 5,214,703, 25 May 1993.
J.L. Massey and J.K. Omura , “Method and apparatus for maintaining the privacy of digital messages conveyed by public transmission”, U.S. Patent # 4,567,600, 28 Jan 1986.
J.L. Massey and R.A. Rueppel , “Linear ciphers and random sequence generators with multiple clocks”, Advances in Cryptology–Proceedings of EUROCRYPT 84 (LNCS 209), 74–87, 1985.
J.L. Massey and S. Serconek , “A Fourier transform approach to the linear complexity of nonlinearly filtered sequences”, Advances in Cryptology–CRYPTO ’94 (LNCS 839), 332–340, 1994.
M. Matsui , “The first experimental cryptanalysis of the Data Encryption Standard”, Advances in Cryptology–CRYPTO ’94 (LNCS 839), 1–11, 1994.
M. Matsui , “Linear cryptanalysis method for DES cipher”, Advances in Cryptology–EUROCRYPT ’93 (LNCS 765), 386–397, 1994.
M. Matsui , “On correlation between the order of S-boxes and the strength of DES”, Advances in Cryptology–EUROCRYPT ’94 (LNCS 950), 366–375, 1995.
M. Matsui and A. Yamagishi , “A new method for known plaintext attack of FEAL cipher”, Advances in Cryptology–EUROCRYPT ’92 (LNCS 658), 81–91, 1993.
T. Matsumoto and H. Imai , “On the key predistribution system: A practical solution to the key distribution problem”, Advances in Cryptology–CRYPTO ’87 (LNCS 293), 185–193, 1988.
T. Matsumoto , Y. Takashima , and H. Imai , “On seeking smart public-key-distribution systems”, The Transactions of the IECE of Japan, E69 (1986), 99–106.
S.M. Matyas , “Digital signatures – an overview”, Computer Networks, 3 (1979), 87–94.
S.M. Matyas , “Key handling with control vectors”, IBM Systems Journal, 30 (1991), 151–174.
S.M. Matyas “Key processing with control vectors”, Journal of Cryptology, 3 (1991), 113–136.
S.M. Matyas and C.H. Meyer , “Generation, distribution, and installation of cryptographic keys”, IBM Systems Journal,17 (1978), 126–137.
S.M. Matyas , C.H. Meyer , and J. Oseas , “Generating strong one-way functions with cryptographic algorithm”, IBM Technical Disclosure Bulletin, 27 (1985), 5658–5659.
S.M. Matyas , C.H.W. Meyer , and B.O. Brachtl , “Controlled use of cryptographic keys via generating station established control values”, U.S. Patent # 4,850,017, 18 Jul 1989.
U. Maurer , “Fast generation of secure RSA-moduli with almost maximal diversity”, Advances in Cryptology–EUROCRYPT ’89 (LNCS 434), 636–647, 1990.
U. Maurer , “New approaches to the design of self-synchronizing stream ciphers”, Advances in Cryptology–EUROCRYPT ’91 (LNCS 547), 458–471, 1991.
U. Maurer , “A provably-secure strongly-randomized cipher”, Advances in Cryptology–EUROCRYPT ’90 (LNCS 473), 361–373, 1991.
U. Maurer , “A universal statistical test for random bit generators”, Advances in Cryptology–CRYPTO ’90 (LNCS 537), 409–420, 1991.
U. Maurer , “Conditionally-perfect secrecy and a provably-secure randomized cipher”, Journal of Cryptology, 5 (1992), 53–66. An earlier version appeared in [809].
U. Maurer , “Some number-theoretic conjectures and their relation to the generation of cryptographic primes”, C. Mitchell , editor, Cryptography and Coding II, volume 33 of Institute of Mathematics & Its Applications (IMA), 173–191, Clarendon Press, 1992.
U. Maurer , “A universal statistical test for random bit generators”, Journal of Cryptology,5 (1992), 89–105. An earlier version appeared in [810].
U. Maurer , “Factoring with an oracle”, Advances in Cryptology–EUROCRYPT ’92 (LNCS 658), 429–436, 1993.
U. Maurer , “Secret key agreement by public discussion from common information”, IEEE Transactions on Information Theory,39 (1993), 733–742.
U. Maurer , “A simplified and generalized treatment of Luby-Rackoff pseudorandom permutation generators”, Advances in Cryptology–EUROCRYPT ’92 (LNCS 658), 239–255, 1993.
U. Maurer , “Towards the equivalence of breaking the Diffie-Hellman protocol and computing discrete logarithms”, Advances in Cryptology–CRYPTO ’94 (LNCS 839), 271–281, 1994.
U. Maurer , “Fast generation of prime numbers and secure public-key cryptographic parameters”, Journal of Cryptology, 8 (1995), 123–155. An earlier version appeared in [807].

U. Maurer , “The role of information theory in cryptography”, P.G. Farrell , editor, Codes and Cyphers: Cryptography and Coding IV, 49–71, Institute of Mathematics & Its Applications (IMA), 1995.
U. Maurer and J.L. Massey , “Perfect local randomness in pseudo-random sequences”, Advances in Cryptology–CRYPTO ’89 (LNCS 435), 100–112, 1990.
U. Maurer and J.L. Massey , “Local randomness in pseudorandom sequences”, Journal of Cryptology, 4 (1991), 135–149. An earlier version appeared in [820].
U. Maurer and J.L. Massey , “Cascade ciphers: The importance of being first”, Journal of Cryptology, 6 (1993), 55–61.
U. Maurer and Y. Yacobi , “Non-interactive public-key cryptography”, Advances in Cryptology–EUROCRYPT ’91 (LNCS 547), 498–507, 1991.
U. Maurer and J.L. Massey , “A remark on a non-interactive public-key distribution system”, Advances in Cryptology–EUROCRYPT ’92 (LNCS 658), 458–460, 1993.
K.S. Mccurley , “A key distribution system equivalent to factoring”, Journal of Cryptology, 1 (1988), 95–105.
K.S. Mccurley , “Cryptographic key distribution and computation in class groups”, R.A. Mollin , editor, Number Theory and Applications, 459–479, Kluwer Academic Publishers, 1989.
K.S. Mccurley , “The discrete logarithm problem”, C. Pomerance , editor, Cryptology and Computational Number Theory, volume 42 of Proceedings of Symposia in Applied Mathematics, 49–74, American Mathematical Society, 1990.
R.J. Mceliece , “A public-key cryptosystem based on algebraic coding theory”, DSN progress report #42–44, Jet Propulsion Laboratory, Pasadena, California, 1978.
R.J. Mceliece , The Theory of Information and Coding: A Mathematical Framework for Communication, Cambridge University Press, Cambridge, 1984.
R.J. Mceliece , Finite Fields for Computer Scientists and Engineeers, Kluwer Academic Publishers, Boston, 1987.
C.A. Meadows , “Formal verification of cryptographic protocols: a survey”, Advances in Cryptology–ASIACRYPT ’94 (LNCS 917), 133–150, 1995.
W. Meier , “On the security of the IDEA block cipher”, Advances in Cryptology–EUROCRYPT ’93 (LNCS 765), 371–385, 1994.
W. Meier and O. Staffelbach , “Fast correlation attacks on stream ciphers”, Advances in Cryptology–EUROCRYPT ’88 (LNCS 330), 301–314, 1988.
W. Meier and O. Staffelbach , “Fast correlation attacks on certain stream ciphers”, Journal of Cryptology,1 (1989), 159–176. An earlier version appeared in [833].
W. Meier and O. Staffelbach , “Analysis of pseudo random sequences generated by cellular automata”, Advances in Cryptology–EUROCRYPT ’91 (LNCS 547), 186–199, 1991.
W. Meier and O. Staffelbach , “Correlation properties of combiners with memory in stream ciphers”, Advances in Cryptology–EUROCRYPT ’90 (LNCS 473), 204–213, 1991.
W. Meier and O. Staffelbach , “Correlation properties of combiners with memory in stream ciphers”, Journal of Cryptology, 5 (1992), 67–86. An earlier version appeared in [836].
W. Meier and O. Staffelbach , “The self-shrinking generator”, Advances in Cryptology–EUROCRYPT ’94 (LNCS 950), 205–214, 1995.
S. Mendes and C. Huitema , “A new approach to the X.509 framework: allowing a global authentication infrastructure without a global trust model”, Proceedings of the Internet Society Symposium on Network and Distributed System Security, 172–189, IEEE Computer Society Press, 1995.
A. Menezes , Elliptic Curve Public Key Cryptosystems, Kluwer Academic Publishers, Boston, 1993.
A. Menezes , I. Blake , X. Gao , R. Mullin , S. Vanstone , and T. Yaghoobian , Applications of Finite Fields, Kluwer Academic Publishers, Boston, 1993.
A. Menezes , T. Okamoto , and S. Vanstone , “Reducing elliptic curve logarithms to logarithms in a finite field”, Proceedings of the 23rd Annual ACM Symposium on Theory of Computing, 80–89, 1991.
A. Menezes , T. Okamoto , and S. Vanstone , “Reducing elliptic curve logarithms to logarithms in a finite field”, IEEE Transactions on Information Theory, 39 (1993), 1639–1646. An earlier version appeared in [842].
A. Menezes , M. Qu , and S. Vanstone , “Some new key agreement protocols providing implicit authentication”, workshop record, 2nd Workshop on Selected Areas in Cryptography (SAC’95), Ottawa, Canada, May 18–19 1995.
R. Menicocci , “Cryptanalysis of a two-stage Gollmann cascade generator”, W. Wolfowicz , editor, Proceedings of the 3rd Symposium on State and Progress of Research in Cryptography, Rome, Italy, 62–69, 1993.
R.C. Merkle , “Digital signature system and method based on a conventional encryption function”, U.S. Patent # 4,881,264, 14 Nov 1989.
R.C. Merkle , “Method and apparatus for data encryption”, U.S. Patent # 5,003,597, 26 Mar 1991.
R.C. Merkle , “Method of providing digital signatures”, U. S. Patent # 4,309,569, 5 Jan 1982.
R.C. Merkle , “Secure communications over insecure channels”, Communications of the ACM, 21 (1978), 294–299.
R.C. Merkle , Secrecy, Authentication, and Public Key Systems, UMI Research Press, Ann Arbor, Michigan, 1979.
R.C. Merkle , “Secrecy, authentication, and public key systems”, Technical Report No.1979–1, Information Systems Laboratory, Stanford University, Palo Alto, California, 1979. Also available as [850].
R.C. Merkle , “Protocols for public key cryptosystems”, Proceedings of the 1980 IEEE Symposium on Security and Privacy, 122–134, 1980.
R.C. Merkle , “A certified digital signature”, Advances in Cryptology–CRYPTO ’89 (LNCS 435), 218–238, 1990.
R.C. Merkle , “A fast software one-way hash function”, Journal of Cryptology, 3 (1990), 43–58.
R.C. Merkle , “One way hash functions and DES”, Advances in Cryptology–CRYPTO ’89 (LNCS 435), 428–446, 1990.
R.C. Merkle , “Fast software encryption functions”, Advances in Cryptology–CRYPTO ’90 (LNCS 537), 476–501, 1991.
R.C. Merkle and M.E. Hellman , “Hiding information and signatures in trapdoor knapsacks”, IEEE Transactions on Information Theory, 24 (1978), 525–530.
R.C. Merkle and M.E. Hellman , “On the security of multiple encryption”, Communications of the ACM,24 (1981), 465–467.
C.H. Meyer and S.M. Matyas , Cryptography:A New Dimension in Computer Data Security, John Wiley & Sons, New York, 1982 (third printing).
C.H. Meyer and M. Schilling , “Secure program load with manipulation detection code”, Proceedings of the 6th Worldwide Congress on Computer and Communications Security and Protection (SECURICOM’88), 111–130, 1988.

S. Micali , “Fair cryptosystems and methods of use”, U. S. Patent # 5,276,737, 4 Jan 1994.
S. Micali , “Fair cryptosystems and methods of use”, U.S. Patent # 5,315,658, 24 May 1994 (continuation-in-part of 5,276,737).
S. Micali , “Fair public-key cryptosystems”, Advances in Cryptology–CRYPTO ’92 (LNCS 740), 113–138, 1993.
S. Micali , O. Goldreich , and S. Even , “On-line/off-line digital signing”, U.S. Patent # 5,016,274, 14 May 1991.
S. Micali , C. Rackoff , and B. Sloan , “The notion of security for probabilistic cryptosystems”, SIAM Journal on Computing,17 (1988), 412–426.
S. Micali and C.P. Schnorr , “Efficient, perfect random number generators”, Advances in Cryptology–CRYPTO ’88 (LNCS 403), 173–198, 1990.
S. Micali and C.P. Schnorr , “Efficient, perfect polynomial random number generators”, Journal of Cryptology,3 (1991), 157–172. An earlier version appeared in [866].
S. Micali and A. Shamir , “An improvement of the Fiat-Shamir identification and signature scheme”, Advances in Cryptology–CRYPTO ’88 (LNCS 403), 244–247, 1990.
S. Micali and R. Sidney , “A simple method for generating and sharing pseudorandom functions, with applications to Clipper-like key escrow systems”, Advances in Cryptology–CRYPTO ’95 (LNCS 963), 185–196, 1995.
P. Mihailescu , “Fast generation of provable primes using search in arithmetic progressions”, Advances in Cryptology–CRYPTO ’94 (LNCS 839), 282–293, 1994.
M.J. Mihaljević , “A security examination of the self-shrinking generator”, presentation at 5th IMA Conference on Cryptography and Coding, Cirencester, U.K., December 1995.
M.J. Mihaljević , “An approach to the initial state reconstruction of a clock-controlled shift register based on a novel distance measure”, Advances in Cryptology–AUSCRYPT ’92 (LNCS 718), 349–356, 1993.
M.J. Mihaljević , “A correlation attack on the binary sequence generators with time-varying output function”, Advances in Cryptology–ASIACRYPT ’94 (LNCS 917), 67–79, 1995.
M.J. Mihaljević and J.D. Golić , “A fast iterative algorithm for a shift register initial state reconstruction given the noisy output sequence”, Advances in Cryptology–AUSCRYPT ’90 (LNCS 453), 165–175, 1990.
M.J. Mihaljević and J.D. Golić , “Convergence of a Bayesian iterative error-correction procedure on a noisy shift register sequence”, Advances in Cryptology–EUROCRYPT ’92 (LNCS 658), 124–137, 1993.
G.L. Miller , “Riemann’s hypothesis and tests for primality”, Journal of Computer and System Sciences, 13 (1976), 300–317.
S.P. Miller , B.C. Neuman , J.I. Schiller , and J.H. Saltzer , “Kerberos authentication and authorization system”, Section E.2.1 of Project Athena Technical Plan, MIT, Cambridge, Massachusetts, 1987.
V. S. Miller , “Use of elliptic curves in cryptography”, Advances in Cryptology–CRYPTO ’85 (LNCS 218), 417–426, 1986.
C. Mitchell , “A storage complexity based analogue of Maurer key establishment using public channels”, C. Boyd , editor, Cryptography and Coding, 5th IMA Conference, Proceedings, 84–93, Institute of Mathematics & Its Applications (IMA), 1995.
C. Mitchell , “Limitations of challenge-response entity authentication”, Electronics Letters, 25 (August 17, 1989), 1195–1196.
C. Mitchell and F. Piper , “Key storage in secure networks”, Discrete Applied Mathematics, 21 (1988), 215–228.
C. Mitchell , F. Piper , and P. Wild , “Digital signatures”, G.J. Simmons , editor, Contemporary Cryptology: The Science of Information Integrity, 325–378, IEEE Press, 1992.
A. Mitropoulos and H. Meijer , “Zero knowledge proofs – a survey”, Technical Report No. 90-IR-05, Queen’s University at Kingston, Kingston, Ontario, Canada, 1990.
S. Miyaguchi , “The FEAL cipher family”, Advances in Cryptology–CRYPTO ’90 (LNCS 537), 627–638, 1991.
S. Miyaguchi , S. Kurihara , K. Ohta , and H. Morita , “Expansion of FEAL cipher”, NTT Review, 2 (1990), 117–127.
S. Miyaguchi , K. Ohta , and M. Iwata , “128-bit hash function (N-hash)”, NTT Review, 2 (1990), 128–132.
S. Miyaguchi , A. Shiraishi , and A. Shimizu , “Fast data encipherment algorithm FEAL-8”, Review of the Electrical Communications Laboratories, 36 (1988), 433–437.
A. Miyaji and M. Tatebayashi , “Public key cryptosystem with an elliptic curve”, U.S. Patent # 5,272,755, 21 Dec 1993.
A. Miyaji and M. Tatebayashi , “Method of privacy communication using elliptic curves”, U.S. Patent # 5,351,297, 27 Sep 1994 (continuation-in-part of 5,272,755).
S.B. Mohan and B.S. Adiga , “Fast algorithms for implementing RSA public key cryptosystem”, Electronics Letters,21 (August 15, 1985), 761.
R. Molva , G. Tsudik , E. Van Herreweghen , and S. Zatti , “KryptoKnight authentication and key distribution system”, Y. Deswarte , G. Eizenberg , and J.-J. Quisquater , editors, Second European Symposium on Research in Computer Security – ESORICS’92 (LNCS 648), 155–174, Springer-Verlag, 1992.
L. Monier , “Evaluation and comparison of two efficient probabilistic primality testing algorithms”, Theoretical Computer Science,12 (1980), 97–108.
P. Montgomery , “Modular multiplication without trial division”, Mathematics of Computation, 44 (1985), 519–521.
P. Montgomery , “Speeding the Pollard and elliptic curve methods of factorization”, Mathematics of Computation, 48 (1987), 243–264.
P. Montgomery and R. Silverman , “An FFT extension to the P – 1 factoring algorithm”, Mathematics of Computation,54 (1990), 839–854.
P.L. Montgomery , “A block Lanczos algorithm for finding dependencies over GF(2)”, Advances in Cryptology–EUROCRYPT ’95 (LNCS 921), 106–120, 1995.
A.M. Mood , “The distribution theory of runs”, The Annals of Mathematical Statistics, 11 (1940), 367–392.
J.H. Moore , “Protocol failures in cryptosystems”, Proceedings of the IEEE, 76 (1988), 594–602.
J.H. Moore , “Protocol failures in cryptosystems”, G.J. Simmons , editor, Contemporary Cryptology: The Science of Information Integrity, 541–558, IEEE Press, 1992. Appeared earlier as [898].
J.H. Moore and G.J. Simmons , “Cycle structure of the DES for keys having palindromic (or antipalindromic) sequences of round keys”, IEEE Transactions on Software Engineering, 13 (1987), 262–273. An earlier version appeared in [901].
J.H. Moore and G.J. Simmons , “Cycle structure of the DES with weak and semi-weak keys”, Advances in Cryptology–CRYPTO ’86 (LNCS 263), 9–32, 1987.
F. Morain , “Distributed primality proving and the primality of (23539 + 1)/3”, Advances in Cryptology–EUROCRYPT ’90 (LNCS 473), 110–123, 1991.

F. Morain , “Prime values of partition numbers and the primality of *p* 1840926 ”, LIX Research Report LIX/RR/92/11, Laboratoire d’Informatique de l’Ecole Polytechnique, France, June 1992.
F. Morain and J. Olivos , “Speeding up the computations on an elliptic curve using addition-subtraction chains”, Theoretical Informatics and Applications, 24 (1990), 531–543.
I.H. Morgan and G.L. Mullen , “Primitive normal polynomials over finite fields”, Mathematics of Computation, 63 (1994), 759–765.
R. Morris , “The Hagelin cipher machine (M-209), Reconstruction of the internal settings”, Cryptologia, 2 (1978), 267–278.
R. Morris and K. Thompson , “Password security: a case history”, Communications of the ACM, 22 (1979), 594–597.
M.A. Morrison and J. Brillhart , “A method of factoring and the factorization of F7”, Mathematics of Computation, 29 (1975), 183–205.
W.B. Müller and R. Nöbauer , “Cryptanalysis of the Dickson-scheme”, Advances in Cryptology–EUROCRYPT ’85 (LNCS 219), 50–61, 1986.
W.B. Müller and R. Nöbauer , “Some remarks on public-key cryptosystems”, Studia Scientiarum Mathematicarum Hungarica,16 (1981), 71–76.
R. Mullin , I. Onyszchuk , S. Vanstone , and R. Wilson , “Optimal normal bases in GF(pn)”, Discrete Applied Mathematics,22 (1988/89), 149–161.
S. Mund , “Ziv-Lempel complexity for periodic sequences and its cryptographic application”, Advances in Cryptology–EUROCRYPT ’91 (LNCS 547), 114–126, 1991.
S. Murphy , “The cryptanalysis of FEAL-4 with 20 chosen plaintexts”, Journal of Cryptology, 2 (1990), 145–154.
D. Naccache , “Can O.S.S. be repaired? – proposal for a new practical signature scheme”, Advances in Cryptology–EUROCRYPT ’93 (LNCS 765), 233–239, 1994.
D. Naccache , D. M’raïhi , and D. Raphaeli , “Can Montgomery parasites be avoided? A design methodology based on key and cryptosystem modifications”, Designs, Codes and Cryptography, 5 (1995), 73–80.
D. Naccache , D. M’raïhi , S. Vaudenay , and D. Raphaeli , “Can D.S.A. be improved? Complexity trade-offs with the digital signature standard”, Advances in Cryptology–EUROCRYPT ’94 (LNCS 950), 77–85, 1995.
D. Naccache and H. M’silti , “A new modulo computation algorithm”, Recherche Opérationnelle – Operations Research (RAIRO-OR), 24 (1990), 307–313.
K. Nagasaka , J.-S. Shiue , and C.-W. Ho , “A fast algorithm of the Chinese remainder theorem and its application to Fibonacci number”, G.E. Bergum , A.N. Philippou , and A.F. Horadam , editors, Applications of Fibonacci Numbers, Proceedings of the Fourth International Conference on Fibonacci Numbers and their Applications, 241–246, Kluwer Academic Publishers, 1991.
M. Naor and A. Shamir , “Visual cryptography”, Advances in Cryptology–EUROCRYPT ’94 (LNCS 950), 1–12, 1995.
M. Naor and M. Yung , “Universal oneway hash functions and their cryptographic applications”, Proceedings of the 21st Annual ACM Symposium on Theory of Computing, 33–43, 1989.
M. Naor and M. Yung , “Public-key cryptosystems provably secure against chosen ciphertext attacks”, Proceedings of the 22nd Annual ACM Symposium on Theory of Computing, 427–437, 1990.
J. Nechvatal , “Public key cryptography”, G.J. Simmons , editor, Contemporary Cryptology: The Science of Information Integrity, 177–288, IEEE Press, 1992.
R.M. Needham and M.D. Schroeder , “Using encryption for authentication in large networks of computers”, Communications of the ACM, 21 (1978), 993–999.
R.M. Needham and M.D. Schroeder , “Authentication revisited”, Operating Systems Review, 21 (1987), 7.
B.C. Neuman and S.G. Stubblebine , “A note on the use of timestamps as nonces”, Operating Systems Review, 27 (1993), 10–14.
B.C. Neuman and T. Ts’o , “Kerberos: an authentication service for computer networks”, IEEE Communications Magazine,32 (September 1994), 33–38.
H. Niederreiter , “The probabilistic theory of linear complexity”, Advances in Cryptology–EUROCRYPT ’88 (LNCS 330), 191–209, 1988.
H. Niederreiter , “A combinatorial approach to probabilistic results on the linear-complexity profile of random sequences”, Journal of Cryptology, 2 (1990), 105–112.
H. Niederreiter , “Keystream sequences with a good linear complexity profile for every starting point”, Advances in Cryptology–EUROCRYPT ’89 (LNCS 434), 523–532, 1990.
H. Niederreiter , “The linear complexity profile and the jump complexity of keystream sequences”, Advances in Cryptology–EUROCRYPT ’90 (LNCS 473), 174–188, 1991.
K. Nishimura and M. Sibuya , “Probability to meet in the middle”, Journal of Cryptology, 2 (1990), 13–22.
I.M. Niven and H.S. Zuckerman , An Introduction to the Theory of Numbers, John Wiley & Sons, New York, 4th edition, 1980.
M.J. Norris and G.J. Simmons , “Algorithms for high-speed modular arithmetic”, Congressus Numerantium, 31 (1981), 153–163.
G. Norton , “Extending the binary gcd algorithm”, J. Calmet , editor, Algebraic Algorithms and Error-Correcting Codes, 3rd International Conference, AAECC-3 (LNCS 229), 363–372, Springer-Verlag, 1986.
K. Nyberg , “On one-pass authenticated key establishment schemes”, workshop record, 2nd Workshop on Selected Areas in Cryptography (SAC’95), Ottawa, Canada, May 18–19 1995.
K. Nyberg and R. Rueppel , “A new signature scheme based on the DSA giving message recovery”, 1st ACM Conference on Computer and Communications Security, 58–61, ACM Press, 1993.
K. Nyberg and R. Rueppel , “Weaknesses in some recent key agreement protocols”, Electronics Letters,30 (January 6, 1994), 26–27.
K. Nyberg and R. Rueppel , “Message recovery for signature schemes based on the discrete logarithm problem”, Designs, Codes and Cryptography,7 (1996), 61–81.
A.M. Odlyzko , “Cryptanalytic attacks on the multiplicative knapsack cryptosystem and on Shamir’s fast signature scheme”, IEEE Transactions on Information Theory,30 (1984), 594–601.
A.M. Odlyzko , “Discrete logarithms in finite fields and their cryptographic significance”, Advances in Cryptology–Proceedings of EUROCRYPT 84 (LNCS 209), 224–314, 1985.
A.M. Odlyzko , “The rise and fall of knapsack cryptosystems”, C. Pomerance , editor, Cryptology and Computational Number Theory, volume 42 of Proceedings of Symposia in Applied Mathematics, 75–88, American Mathematical Society, 1990.
A.M. Odlyzko , “Discrete logarithms and smooth polynomials”, G.L. Mullen and P.J- S. Shiue , editors, Finite Fields: Theory, Applications, and Algorithms, volume 168 of Contemporary Mathematics, 269–278, American Mathematical Society, 1994.

K. Ohta and K. Aoki , “Linear cryptanalysis of the Fast Data Encipherment Algorithm”, Advances in Cryptology–CRYPTO ’94 (LNCS 839), 12–16, 1994.
K. Ohta and T. Okamoto , “Practical extension of Fiat-Shamir scheme”, Electronics Letters, 24 (July 21, 1988), 955–956.
K. Ohta and T. Okamoto , “A modification of the Fiat-Shamir scheme”, Advances in Cryptology–CRYPTO ’88 (LNCS 403), 232–243, 1990.
E. Okamoto and K. Tanaka , “Key distribution system based on identification information”, IEEE Journal on Selected Areas in Communications, 7 (1989), 481–485.
T. Okamoto , “A single public-key authentication scheme for multiple users”, Systems and Computers in Japan, 18 (1987), 14–24. Translated from Denshi Tsushin Gakkai Ronbunshi vol. 69-D no. 10, October 1986, 1481–1489.
T. Okamoto , “A fast signature scheme based on congruential polynomial operations”, IEEE Transactions on Information Theory,36 (1990), 47–53.
T. Okamoto , “Provably secure and practical identification schemes and corresponding signature schemes”, Advances in Cryptology–CRYPTO ’92 (LNCS 740), 31–53, 1993.
T. Okamoto , “Designated confirmer signatures and public-key encryption are equivalent”, Advances in Cryptology–CRYPTO ’94 (LNCS 839), 61–74, 1994.
T. Okamoto , “An efficient divisible electronic cash scheme”, Advances in Cryptology–CRYPTO ’95 (LNCS 963), 438–451, 1995.
T. Okamoto , S. Miyaguchi , A. Shiraishi , and T. Kawaoka , “Signed document transmission system”, U.S. Patent # 4,625,076, 25 Nov 1986.
T. Okamoto and A. Shiraishi , “A fast signature scheme based on quadratic inequalities”, Proceedings of the 1985 IEEE Symposium on Security and Privacy, 123–132, 1985.
T. Okamoto , A. Shiraishi , and T. Kawaoka , “Secure user authentication without password files”, Technical Report NI83–92, I.E.C.E., Japan, January 1984. In Japanese.
J. Olivos , “On vectorial addition chains”, Journal of Algorithms, 2 (1981), 13–21.
J.K. Omura and J.L. Massey , “Computational method and apparatus for finite field arithmetic”, U.S. Patent # 4,587,627, 6 May 1986.
H. Ong and C.P. Schnorr , “Fast signature generation with a Fiat Shamir-like scheme”, Advances in Cryptology–EUROCRYPT ’90 (LNCS 473), 432–440, 1991.
H. Ong and C.P. Schnorr , and A. Shamir , “An efficient signature scheme based on quadratic equations”, Proceedings of the 16th Annual ACM Symposium on Theory of Computing, 208–216, 1984.
I.M. Onyszchuk , R.C. Mullin , and S.A. Vanstone , “Computational method and apparatus for finite field multiplication”, U.S. Patent # 4,745,568, 17 May 1988.
G. Orton , “A multiple-iterated trapdoor for dense compact knapsacks”, Advances in Cryptology–EUROCRYPT ’94 (LNCS 950), 112–130, 1995.
D. Otway and O. Rees , “Efficient and timely mutual authentication”, Operating Systems Review, 21 (1987), 8–10.
J. C. Paillès and M. Girault , “CRIPT: A public-key based solution for secure data communications”, Proceedings of the 7th Worldwide Congress on Computer and Communications Security and Protection (SECURICOM’89), 171–185, 1989.
C.H. Papadimitriou , Computational Complexity, Addison-Wesley, Reading, Massachusetts, 1994.
S.-J. Park , S.-J. Lee , and S.-C. Goh , “On the security of the Gollmann cascades”, Advances in Cryptology–CRYPTO ’95 (LNCS 963), 148–156, 1995.
J. Patarin , “Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms”, Advances in Cryptology–EUROCRYPT ’96 (LNCS 1070), 33–48, 1996.
J. Patarin and P. Chauvaud , “Improved algorithms for the permuted kernel problem”, Advances in Cryptology–CRYPTO ’93 (LNCS 773), 391–402, 1994.
W. Penzhorn and G. Kühn , “Computation of low-weight parity checks for correlation attacks on stream ciphers”, C. Boyd , editor, Cryptography and Coding, 5th IMA Conference, Proceedings, 74–83, Institute of Mathematics & Its Applications (IMA), 1995.
R. Peralta , “Simultaneous security of bits in the discrete log”, Advances in Cryptology–EUROCRYPT ’85 (LNCS 219), 62–72, 1986.
R. Peralta and V. Shoup , “Primality testing with fewer random bits”, Computational Complexity, 3 (1993), 355–367.
A. Pfitzmann and R. Assmann , “More efficient software implementations of (generalized) DES”, Computers & Security,12 (1993), 477–500.
B. Pfitzmann and M. Waidner , “Fail-stop signatures and their applications”, Proceedings of the 9th Worldwide Congress on Computer and Communications Security and Protection (SECURICOM’91), 145–160, 1991.
B. Pfitzmann and M. Waidner , “Formal aspects of fail-stop signatures”, Interner Bericht 22/90, Universität Karlsruhe, Germany, December 1990.
S.J.D. Phoenix and P.D. Townsend , “Quantum cryptography: protecting our future networks with quantum mechanics”, C. Boyd , editor, Cryptography and Coding, 5th IMA Conference, Proceedings, 112–131, Institute of Mathematics & Its Applications (IMA), 1995.
R. Pinch , “The Carmichael numbers up to 1015”, Mathematics of Computation,61 (1993), 381–391.
R. Pinch , “Some primality testing algorithms”, Notices of the American Mathematical Society, 40 (1993), 1203–1210.
R. Pinch , “Extending the Håstad attack to LUC”, Electronics Letters, 31 (October 12, 1995), 1827–1828.
R. Pinch , “Extending the Wiener attack to RSA- type cryptosystems”, Electronics Letters,31 (September 28, 1995), 1736–1738.
V. Pless , “Encryption schemes for computer confidentiality”, IEEE Transactions on Computers, 26 (1977), 1133–1136.
J. B. Plumstead , “Inferring a sequence generated by a linear congruence”, Proceedings of the IEEE 23rd Annual Symposium on Foundations of Computer Science, 153–159, 1982.
J. B. Plumstead , “Inferring a sequence produced by a linear congruence”, Advances in Cryptology–Proceedings of Crypto 82, 317–319, 1983.
H.C. Pocklington , “The determination of the prime or composite nature of large numbers by Fermat’s theorem”, Proceedings of the Cambridge Philosophical Society, 18 (1914), 29–30.
S.C. Pohlig and M.E. Hellman , “An improved algorithm for computing logarithms over GF(p) and its cryptographic significance”, IEEE Transactions on Information Theory, 24 (1978), 106–110.
D. Pointcheval , “A new identification scheme based on the perceptrons problem”, Advances in Cryptology–EUROCRYPT ’95 (LNCS 921), 319–328, 1995.

J.M. Pollard , “Theorems on factorization and primality testing”, Proceedings of the Cambridge Philosophical Society, 76 (1974), 521–528.
J.M. Pollard , “A Monte Carlo method for factorization”, BIT, 15 (1975), 331–334.
J.M. Pollard , “Monte Carlo methods for index computation (mod p)”, Mathematics of Computation, 32 (1978), 918–924.
J.M. Pollard , “Factoring with cubic integers”, A.K. Lenstra and H.W. Lenstra Jr., editors, The Development of the Number Field Sieve, volume 1554 of Lecture Notes in Mathematics, 4–10, Springer-Verlag, 1993.
J.M. Pollard and C. Schnorr , “An efficient solution of the congruence x2 + ky2 = m (mod n)”, IEEE Transactions on Information Theory, 33 (1987), 702–709.
C. Pomerance , “Analysis and comparison of some integer factoring algorithms”, H.W. Lenstra Jr. and R. Tijdeman , editors, Computational Methods in Number Theory, Part 1, 89–139, Mathematisch Centrum, 1982.
C. Pomerance , “The quadratic sieve factoring algorithm”, Advances in Cryptology–Proceedings of EUROCRYPT 84 (LNCS 209), 169–182, 1985.
C. Pomerance , “Fast, rigorous factorization and discrete logarithm algorithms”, Discrete Algorithms and Complexity, 119–143, Academic Press, 1987.
C. Pomerance , “Very short primality proofs”, Mathematics of Computation, 48 (1987), 315–322.
C. Pomerance , editor, Cryptology and Computational Number Theory, American Mathematical Society, Providence, Rhode Island, 1990.
C. Pomerance , “Factoring”, C. Pomerance , editor, Cryptology and Computational Number Theory, volume 42 of Proceedings of Symposia in Applied Mathematics, 27–47, American Mathematical Society, 1990.
C. Pomerance , “The number field sieve”, W. Gautschi , editor, Mathematics of Computation, 1943–1993: A Half-Century of Computation Mathematics, volume 48 of Proceedings of Symposia in Applied Mathematics, 465–480, American Mathematical Society, 1994.
C. Pomerance , J.L. Selfridge , and S.S. Wagstaff JR., “The pseudoprimes to 25 · 109 ”, Mathematics of Computation,35 (1980), 1003–1026.
C. Pomerance and J. Sorenson , “Counting the integers factorable via cyclotomic methods”, Journal of Algorithms, 19 (1995), 250–265.
G.J. Popek and C.S. Kline , “Encryption and secure computer networks”, ACM Computing Surveys, 11 (1979), 331–356.
E. Prange , “An algorism for factoring xn — 1 over a finite field”, AFCRC-TN-59–775, Air Force Cambridge Research Center, 1959.
V.R. Pratt , “Every prime has a succinct certificate”, SIAM Journal on Computing,4 (1975), 214–220.
B. Preneel , “Standardization of cryptographic techniques”, B. Preneel , R. Govaerts , and J. Vandewalle , editors, Computer Security and Industrial Cryptography: State of the Art and Evolution (LNCS 741), 162–173, Springer-Verlag, 1993.
B. Preneel , “Cryptographic hash functions”, European Transactions on Telecommunications, 5(1994), 431–448.
B. Preneel , Analysis and design of cryptographic hash functions, PhD thesis, Katholieke Universiteit Leuven (Belgium), Jan. 1993.
B. Preneel , Cryptographic Hash Functions, Kluwer Academic Publishers, Boston, (to appear). Updated and expanded from [1003].
B. Preneel , R. Govaerts , and J. Vandewalle , “Differential cryptanalysis of hash functions based on block ciphers”, 1st ACM Conference on Computer and Communications Security, 183–188, ACM Press, 1993.
B. Preneel , R. Govaerts , and J. Vandewalle , “Information authentication: Hash functions and digital signatures”, B. Preneel , R. Govaerts , and J. Vandewalle , editors, Computer Security and Industrial Cryptography: State of the Art and Evolution (LNCS 741), 87–131, Springer-Verlag, 1993.
B. Preneel , R. Govaerts , and J. Vandewalle , “Hash functions based on block ciphers: A synthetic approach”, Advances in Cryptology–CRYPTO ’93 (LNCS 773), 368–378, 1994.
B. Preneel , M. Nuttin , V. Rijmen , and J. Buelens , “Cryptanalysis of the CFB mode of the DES with a reduced number of rounds”, Advances in Cryptology–CRYPTO ’93 (LNCS 773), 212–223, 1994.
B. Preneel and P. Van Oorschot , “MDx-MAC and building fast MACs from hash functions”, Advances in Cryptology–CRYPTO ’95 (LNCS 963), 1–14, 1995.
B. Preneel and P. Van Oorschot , “On the security of two MAC algorithms”, Advances in Cryptology–EUROCRYPT’96 (LNCS 1070), 19–32, 1996.
N. Proctor , “A self-synchronizing cascaded cipher system with dynamic control of error propagation”, Advances in Cryptology–Proceedings of CRYPTO 84 (LNCS 196), 174–190, 1985.
G.B. Purdy , “A high security log-in procedure”, Communications of the ACM,17 (1974), 442–445.
M. Qu and S.A. Vanstone , “The knapsack problem in cryptography”, Contemporary Mathematics, 168 (1994), 291–308.
K. Quinn , “Some constructions for key distribution patterns”, Designs, Codes and Cryptography, 4 (1994), 177–191.
J.-J. Quisquater , “A digital signature scheme with extended recovery”, preprint, 1995.
J.-J. Quisquater and C. Couvreur , “Fast decipherment algorithm for RSA public-key cryptosystem”, Electronics Letters,18 (October 14, 1982), 905–907.
J.-J. Quisquater and J.-P. Delescaille , “How easy is collision search? Application to DES”, Advances in Cryptology–EUROCRYPT ’89 (LNCS 434), 429–434, 1990.
J.-J. Quisquater and J.-P. Delescaille , “How easy is collision search. New results and applications to DES”, Advances in Cryptology–CRYPTO ’89 (LNCS 435), 408–413, 1990.
J.-J. Quisquater and M. Girault , “2n-bit hash-functions using n-bit symmetric block cipher algorithms”, Advances in Cryptology–EUROCRYPT ’89 (LNCS 434), 102–109, 1990.
J.-J. Quisquater , L. Guillou , and T. Berson , “How to explain zero-knowledge protocols to your children”, Advances in Cryptology–CRYPTO ’89 (LNCS 435), 628–631, 1990.
M.O. Rabin , “Probabilistic algorithms”, J.F. Traub , editor, Algorithms and Complexity, 21–40, Academic Press, 1976.
M.O. Rabin , “Digitalized signatures”, R. Demillo , D. Dobkin , A. Jones , and R. Lipton , editors, Foundations of Secure Computation, 155–168, Academic Press, 1978.
M.O. Rabin , “Digitalized signatures and public-key functions as intractable as factorization”, MIT/LCS/TR-212, MIT Laboratory for Computer Science, 1979.
M.O. Rabin , “Probabilistic algorithm for testing primality”, Journal of Number Theory,12 (1980), 128–138.
M.O. Rabin , “Probabilistic algorithms in finite fields”, SIAM Journal on Computing,9 (1980), 273–280.
M.O. Rabin , “Fingerprinting by random polynomials”, TR-15–81, Center for Research in Computing Technology, Harvard University, 1981.
M.O. Rabin , “Efficient dispersal of information for security, load balancing, and fault tolerance”, Journal of the Association for Computing Machinery, 36 (1989), 335–348.

T. Rabin and M. Ben-Or , “Verifiable secret sharing and multiparty protocols with honest majority”, Proceedings of the 21st Annual ACM Symposium on Theory of Computing, 73–85, 1989.
C. Rackoff and D.R. Simon , “Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack”, Advances in Cryptology–CRYPTO ’91 (LNCS 576), 433–444, 1992.
G. Rawlins , Compared to What? An Introduction to the Analysis of Algorithms, Computer Science Press, New York, 1992.
G. Reitwiesner , “Binary arithmetic”, Advances in Computers, 1 (1960), 231–308.
T. Renji , “On finite automaton one-key cryptosystems”, R. Anderson , editor, Fast Software Encryption, Cambridge Security Workshop (LNCS 809), 135–148, Springer-Verlag, 1994.
RFC 1319, “The MD2 message-digest algorithm”, Internet Request for Comments 1319, B. Kaliski , April 1992 (updates RFC 1115, August 1989, J. Linn).
RFC 1320, “The MD4 message-digest algorithm”, Internet Request for Comments 1320, R.L. Rivest , April 1992 (obsoletes RFC 1186, October 1990, R. Rivest).
RFC 1321, “The MD5 message-digest algorithm”, Internet Request for Comments 1321, R.L. Rivest , April 1992 (presented at Rump Session of Crypto’91).
RFC 1421, “Privacy enhancement for Internet electronic mail – Part I: Message encryption and authentication procedures”, Internet Request for Comments 1421, J. Linn , February 1993 (obsoletes RFC 1113 – September 1989; RFC 1040 – January 1988; and RFC 989 – February 1987, J. Linn).
RFC 1422, “Privacy enhancement for Internet electronic mail – Part II: Certificate-based key management”, Internet Request for Comments 1422, S. Kent , February 1993 (obsoletes RFC 1114, August 1989, S. Kent and J. Linn).
RFC 1423, “Privacy enhancement for Internet electronic mail – Part III: Algorithms, modes, and identifiers”, Internet Request for Comments 1423, D. Balenson , February 1993 (obsoletes RFC 1115, September 1989, J. Linn).
RFC 1424, “Privacy enhancement for Internet electronic mail – Part IV: Key certification and related services”, Internet Request for Comments 1424, B. Kaliski , February 1993.
RFC 1508, “Generic security service application program interface”, Internet Request for Comments 1508, J. Linn , September 1993.
RFC 1510, “The Kerberos network authentication service (V5)”, Internet Request for Comments 1510, J. Kohl and C. Neuman , September 1993.
RFC 1521, “MIME (Multipurpose Internet Mail Extensions) Part One: Mechanisms for specifying and describing the format of Internet message bodies”, Internet Request for Comments 1521, N. Borenstein and N. Freed , September 1993 (obsoletes RFC 1341).
RFC 1750, “Randomness requirements for security”, Internet Request for Comments 1750, D. Eastlake , S. Crocker and J. Schiller , December 1994.
RFC 1828, “IP authentication using keyed MD5”, Internet Request for Comments 1828, P. Metzger and W. Simpson , August 1995.
RFC 1847, “Security multiparts for MIME: Multipart/signed and multipart/encrypted”, Internet Request for Comments 1847, J. Galvin , S. Murphy , S. Crocker and N. Freed , October 1995.
RFC 1848, “MIME object security services”, Internet Request for Comments 1848, S. Crocker , N. Freed , J. Galvin and S. Murphy , October 1995.
RFC 1938, “A one-time password system”, Internet Request for Comments 1938, N. Haller and C. Metz , May 1996.
V. Rijmen , J. Daemen , B. Preneel , A. Bosselaers , and E. De Win , “The cipher SHARK”, D. Gollmann , editor, Fast Software Encryption, Third International Workshop (LNCS 1039), 99–111, Springer-Verlag, 1996.
V. Rijmen and B. Preneel , “On weaknesses of non-surjective round functions”, presented at the 2nd Workshop on Selected Areas in Cryptography (SAC’95), Ottawa, Canada, May 18–19 1995.
V. Rijmen and B. Preneel , “Improved characteristics for differential cryptanalysis of hash functions based on block ciphers”, B. Preneel , editor, Fast Software Encryption, Second International Workshop (LNCS 1008), 242–248, Springer-Verlag, 1995.
R.L. Rivest , “Are ‘strong’ primes needed for RSA?”, unpublished manuscript, 1991.
R.L. Rivest , “Remarks on a proposed cryptanalytic attack on the M.I.T. public-key cryptosystem”, Cryptologia, 2 (1978), 62–65.
R.L. Rivest , “Statistical analysis of the Hagelin cryptograph”, Cryptologia, 5 (1981), 27–32.
R.L. Rivest , “Cryptography”, J. Van Leeuwen , editor, Handbook of Theoretical Computer Science, 719–755, Elsevier Science Publishers, 1990.
R.L. Rivest , “The MD4 message digest algorithm”, Advances in Cryptology–CRYPTO ’90 (LNCS 537), 303–311, 1991.
R.L. Rivest , “The RC5 encryption algorithm”, B. Preneel , editor, Fast Software Encryption, Second International Workshop(LNCS 1008), 86–96, Springer-Verlag, 1995.
R.L. Rivest and A. Shamir , “How to expose an eavesdropper”, Communications of the ACM, 27 (1984), 393–395.
R.L. Rivest and A. Shamir , “Efficient factoring based on partial information”, Advances in Cryptology–EUROCRYPT ’85 (LNCS 219), 31–34, 1986.
R.L. Rivest , A. Shamir , and L.M. Adleman , “Cryptographic communications system and method”, U.S. Patent # 4,405,829, 20 Sep 1983.
R.L. Rivest , A. Shamir , and L.M. Adleman , “A method for obtaining digital signatures and public-key cryptosystems”, Communications of the ACM, 21 (1978), 120–126.
R.L. Rivest , A. Shamir , and L.M. Adleman , “Randomized encryption techniques”, Advances in Cryptology–Proceedings of Crypto 82, 145–163, 1983.
M.J.B. Robshaw , “On evaluating the linear complexity of a sequence of least period 2n ”, Designs, Codes and Cryptography, 4 (1994), 263–269.
M.J.B. Robshaw , “Stream ciphers”, Technical Report TR-701 (version 2.0), RSA Laboratories, 1995.
M. Roe , “How to reverse engineer an EES device”, B. Preneel , editor, Fast Software Encryption, Second International Workshop (LNCS 1008), 305–328, Springer-Verlag, 1995.
P. Rogaway , “Bucket hashing and its application to fast message authentication”, Advances in Cryptology–CRYPTO ’95 (LNCS 963), 29–42, 1995.
P. Rogaway and D. Coppersmith , “A software-optimized encryption algorithm”, R. Anderson , editor, Fast Software Encryption, Cambridge Security Workshop (LNCS 809), 56–63, Springer-Verlag, 1994.
N. Rogier and P. Chauvaud , “The compression function of MD2 is not collision free”, workshop record, 2nd Workshop on Selected Areas in Cryptography (SAC’95), Ottawa, Canada, May 18–19 1995.

J. Rompel , “One-way functions are necessary and sufficient for secure signatures”, Proceedings of the 22nd Annual ACMSymposium on Theory of Computing, 387–394, 1990.
K.H. Rosen , Elementary Number Theory and its Applications, Addison-Wesley, Reading, Massachusetts, 3rd edition, 1992.
J. Rosser and L. Schoenfeld , “Approximate formulas for some functions of prime numbers”, Illinois Journal of Mathematics, 6 (1962), 64–94.
RSA LABORATORIES , “The Public-Key Cryptography Standards – PKCS #11: Cryptographic token interface standard”, RSA Data Security Inc., Redwood City, California, April 28 1995.
RSA LABORATORIES , “The Public-Key Cryptography Standards (PKCS)”, RSA Data Security Inc., Redwood City, California, November 1993 Release.
A.D. Rubin and P. Honeyman , “Formal methods for the analysis of authentication protocols”, CITI Technical Report 93–7, Information Technology Division, University of Michigan, 1993.
F. Rubin , “Decrypting a stream cipher based on J-K flip-flops”, IEEE Transactions on Computers, 28 (1979), 483–487.
R.A. Rueppel , Analysis and Design of Stream Ciphers, Springer-Verlag, Berlin, 1986.
R.A. Rueppel , “Correlation immunity and the summation generator”, Advances in Cryptology–CRYPTO ’85 (LNCS 218), 260–272, 1986.
R.A. Rueppel , “Linear complexity and random sequences”, Advances in Cryptology–EUROCRYPT ’85 (LNCS 219), 167–188, 1986.
R.A. Rueppel , “Key agreements based on function composition”, Advances in Cryptology–EUROCRYPT ’88 (LNCS 330), 3–10, 1988.
R.A. Rueppel , “On the security of Schnorr’s pseudo random generator”, Advances in Cryptology–EUROCRYPT ’89 (LNCS 434), 423–428, 1990.
R.A. Rueppel , “A formal approach to security architectures”, Advances in Cryptology–EUROCRYPT ’91 (LNCS 547), 387–398, 1991.
R.A. Rueppel , “Stream ciphers”, G.J. Simmons , editor, Contemporary Cryptology: The Science of Information Integrity, 65–134, IEEE Press, 1992.
R.A. Rueppel , “Criticism of ISO CD 11166 banking — key management by means of asymmetric algorithms”, W. Wolfowicz , editor, Proceedings of the 3rd Symposium on State and Progress of Research in Cryptography, Rome, Italy, 191–198, 1993.
R.A. Rueppel , A. Lenstra , M. Smid , K. Mccurley , Y. Desmedt , A. Odlyzko , and P. Landrock , “The Eurocrypt ’92 controversial issue: trapdoor primes and moduli”, Advances in Cryptology–EUROCRYPT ’92 (LNCS 658), 194–199, 1993.
R.A. Rueppel and J.L. Massey , “The knapsack as a non-linear function”, IEEE International Symposium on Information Theory (Abstracts), p. 46, 1985.
R.A. Rueppel and O.J. Staffelbach , “Products of linear recurring sequences with maximum complexity”, IEEE Transactions on Information Theory, 33 (1987), 124–131.
R.A. Rueppel and P.C. Van Oorschot , “Modern key agreement techniques”, Computer Communications, 17 (1994), 458–465.
A. Russell , “Necessary and sufficient conditions for collision-free hashing”, Advances in Cryptology–CRYPTO ’92 (LNCS 740), 433–441, 1993.
A. Russell , “Necessary and sufficient conditions for collision-free hashing”, Journal of Cryptology, 8 (1995), 87–99. An earlier version appeared in [1087].
A. Salomaa , Public-key Cryptography, Springer-Verlag, Berlin, 1990.
M. Santha and U.V. Vazirani , “Generating quasi-random sequences from slightly-random sources”, Proceedings of the IEEE 25th Annual Symposium on Foundations of Computer Science, 434–440, 1984.
M. Santha and U.V. Vazirani , “Generating quasi-random sequences from semi-random sources”, Journal of Computer and System Sciences, 33 (1986), 75–87. An earlier version appeared in [1090].
O. Schirokauer , “Discrete logarithms and local units”, Philosophical Transactions of the Royal Society of London A, 345 (1993), 409–423.
B. Schneier , “Description of a new variable-length key, 64-bit block cipher (Blowfish)”, R. Anderson , editor, Fast Software Encryption, Cambridge Security Workshop (LNCS 809), 191–204, Springer-Verlag, 1994.
B. Schneier , Applied Cryptography: Protocols, Algorithms, and Source Code in C, John Wiley & Sons, New York, 2nd edition, 1996.
C.P. Schnorr , “Method for identifying subscribers and for generating and verifying electronic signatures in a data exchange system”, U.S. Patent # 4,995,082, 19 Feb 1991.
C.P. Schnorr , “On the construction of random number generators and random function generators”, Advances in Cryptology–EUROCRYPT ’88 (LNCS 330), 225–232, 1988.
C.P. Schnorr , “Efficient identification and signatures for smart cards”, Advances in Cryptology–CRYPTO ’89 (LNCS 435), 239–252, 1990.
C.P. Schnorr , “Efficient signature generation by smart cards”, Journal of Cryptology, 4 (1991), 161–174.
C.P. Schnorr and M. Euchner , “Lattice basis reduction: Improved practical algorithms and solving subset sum problems”, L. Budach , editor, Fundamentals of Computation Theory (LNCS 529), 68–85, Springer-Verlag, 1991.
C.P. Schnorr and H.H. Hörner , “Attacking the Chor-Rivest cryptosystem by improved lattice reduction”, Advances in Cryptology–EUROCRYPT ’95 (LNCS 921), 1–12, 1995.
A. Schönhage , “A lower bound for the length of addition chains”, Theoretical Computer Science, 1 (1975), 1–12.
A.W. Schrift and A. Shamir , “On the universality of the next bit test”, Advances in Cryptology–CRYPTO ’90 (LNCS 537), 394–408, 1991.
A.W. Schrift and A. Shamir , “Universal tests for nonuniform distributions”, Journal of Cryptology, 6 (1993), 119–133. An earlier version appeared in [1102].
F. Schwenk and J. Eisfeld , “Public key encryption and signature schemes based on polynomials over Zn”, Advances in Cryptology–EUROCRYPT ’96 (LNCS 1070), 60–71, 1996.
R. Sedgewick , Algorithms, Addison-Wesley, Reading, Massachusetts, 2nd edition, 1988.
R. Sedgewick , T.G. Szymanski , and A.C. Yao , “The complexity of finding cycles in periodic functions”, SIAMJournal on Computing, 11 (1982), 376–390.
E.S. Selmer , “Linear recurrence relations over finite fields”, Department of Mathematics, University of Bergen, Norway, 1966.
J. Shallit , “On the worst case of three algorithms for computing the Jacobi symbol”, Journal of Symbolic Computation, 10 (1990), 593–610.
A. Shamir , “A fast signature scheme”, MIT/LCS/TM-107, MIT Laboratory for Computer Science, 1978.
A. Shamir , “How to share a secret”, Communications of the ACM, 22 (1979), 612–613.
A. Shamir , “On the generation of cryptographically strong pseudo-random sequences”, S. Even and O. Kariv , editors, Automata, Languages, and Programming, 8th Colloquium (LNCS 115), 544–550, Springer-Verlag, 1981.

A. Shamir , “On the generation of cryptographically strong pseudorandom sequences”, ACM Transactions on Computer Systems, 1 (1983), 38–44. An earlier version appeared in [1111].
A. Shamir , “A polynomial time algorithm for breaking the basic Merkle-Hellman cryptosystem”, Advances in Cryptology–Proceedings of Crypto82, 279–288, 1983.
A. Shamir , “A polynomial-time algorithm for breaking the basic Merkle-Hellman cryptosystem”, IEEE Transactions on Information Theory, 30 (1984), 699–704. An earlier version appeared in [1113].
A. Shamir , “Identity-based cryptosystems and signature schemes”, Advances in Cryptology–Proceedings of CRYPTO 84 (LNCS 196), 47–53, 1985.
A. Shamir , “An efficient identification scheme based on permuted kernels”, Advances in Cryptology–CRYPTO ’89 (LNCS 435), 606–609, 1990.
A. Shamir , “RSA for paranoids”, CryptoBytes, 1 (Autumn 1995), 1–4.
A. Shamir and A. Fiat , “Method, apparatus and article for identification and signature”, U.S. Patent #4,748,668, 31 May 1988.
M. Shand and J. Vuillemin , “Fast implementations of RSA cryptography”, Proceedings of the 11th IEEE Symposium on Computer Arithmetic, 252–259, 1993.
C.E. Shannon , “A mathematical theory of communication”, Bell System Technical Journal, 27 (1948), 379–423, 623–656.
C.E. Shannon , “Communication theory of secrecy systems”, Bell System Technical Journal,28 (1949), 656–715.
C.E. Shannon , “Prediction and entropy of printed English”, Bell System Technical Journal,30 (1951), 50–64.
J. Shawe-Taylor , “Generating strong primes”, Electronics Letters, 22 (July 31, 1986), 875–877.
S. Shepherd , “A high speed software implementation of the Data Encryption Standard”, Computers & Security, 14 (1995), 349–357.
A. Shimizu and S. Miyaguchi , “Data randomization equipment”, U.S. Patent # 4,850,019, 18 Jul 1989.
A. Shimizu and S. Miyaguchi , “Fast data encipherment algorithm FEAL”, Advances in Cryptology–EUROCRYPT ’87 (LNCS 304), 267–278, 1988.
Z. Shmuely , “Composite Diffie-Hellman public-key generating systems are hard to break”, Technical Report #356, TECHNION – Israel Institute of Technology, Computer Science Department, 1985.
P.W. Shor , “Algorithms for quantum computation: discrete logarithms and factoring”, Proceedings of the IEEE 35th Annual Symposium on Foundations of Computer Science, 124–134, 1994.
V. Shoup , “New algorithms for finding irreducible polynomials over finite fields”, Mathematics of Computation, 54 (1990), 435–447.
V. Shoup , “Searching for primitive roots in finite fields”, Mathematics of Computation,58 (1992), 369–380.
V. Shoup , “Fast construction of irreducible polynomials over finite fields”, Journal of Symbolic Computation, 17 (1994), 371–391.
T. Siegenthaler , “Correlation-immunity of nonlinear combining functions for cryptographic applications”, IEEE Transactions on Information Theory, 30 (1984), 776–780.
T. Siegenthaler , “Decrypting a class of stream ciphers using ciphertext only”, IEEE Transactions on Computers, 34 (1985), 81–85.
T. Siegenthaler , “Cryptanalysts representation of non-linearly filtered ML-sequences”, Advances in Cryptology–EUROCRYPT ’85 (LNCS 219), 103–110, 1986.
R.D. Silverman , “The multiple polynomial quadratic sieve”, Mathematics of Computation, 48 (1987), 329–339.
R.D. Silverman and S.S. Wagstaff JR., “A practical analysis of the elliptic curve factoring algorithm”, Mathematics of Computation, 61 (1993), 445–462.
G.J. Simmons , “A “weak” privacy protocol using the RSA crypto algorithm”, Cryptologia, 7 (1983), 180–182.
G.J. Simmons , “Authentication theory/coding theory”, Advances in Cryptology–Proceedings of CRYPTO 84 (LNCS 196), 411–431, 1985.
G.J. Simmons , “The subliminal channel and digital signatures”, Advances in Cryptology–Proceedings of EUROCRYPT 84 (LNCS 209), 364–378, 1985.
G.J. Simmons , “A secure subliminal channel (?)”, Advances in Cryptology–CRYPTO ’85 (LNCS 218), 33–41, 1986.
G.J. Simmons , “How to (really) share a secret”, Advances in Cryptology–CRYPTO ’88 (LNCS 403), 390–448, 1990.
G.J. Simmons , “Prepositioned shared secret and/or shared control schemes”, Advances in Cryptology–EUROCRYPT ’89 (LNCS 434), 436–467, 1990.
G.J. Simmons , “Contemporary cryptology: a foreword”, G.J. Simmons , editor, Contemporary Cryptology: The Science of Information Integrity, vii–xv, IEEE Press, 1992.
G.J. Simmons , “A survey of information authentication”, G.J. Simmons , editor, Contemporary Cryptology: The Science of Information Integrity, 379–419, IEEE Press, 1992.
G.J. Simmons , “An introduction to shared secret and/or shared control schemes and their application”, G.J. Simmons , editor, Contemporary Cryptology: The Science of Information Integrity, 441–497, IEEE Press, 1992.
G.J. Simmons , “How to insure that data acquired to verify treaty compliance are trustworthy”, G.J. Simmons , editor, Contemporary Cryptology: The Science of Information Integrity, 615–630, IEEE Press, 1992.
G.J. Simmons , “The subliminal channels in the U.S. Digital Signature Algorithm (DSA)”, W. Wolfowicz , editor, Proceedings of the 3rd Symposium on State and Progress of Research in Cryptography, Rome, Italy, 35–54, 1993.
G.J. Simmons , “Proof of soundness (integrity) of cryptographic protocols”, Journal of Cryptology, 7 (1994), 69–77.
G.J. Simmons , “Subliminal communication is easy using the DSA”, Advances in Cryptology–EUROCRYPT ’93 (LNCS 765), 218–232, 1994.
G.J. Simmons , “Protocols that ensure fairness”, P.G. Farrell , editor, Codes and Cyphers: Cryptography and Coding IV, 383–394, Institute of Mathematics & Its Applications (IMA), 1995.
G.J. Simmons and M.J. Norris , “Preliminary comments on the M.I.T. public-key cryptosystem”, Cryptologia, 1 (1977), 406–414.
A. Sinkov , Elementary Cryptanalysis: A Mathematical Approach, Random House, New York, 1968.
M.E. Smid , “Integrating the Data Encryption Standard into computer networks”, IEEE Transactions on Communications, 29 (1981), 762–772.
M.E. Smid and D.K. Branstad , “Cryptographic key notarization methods and apparatus”, U.S. Patent #4,386,233, 31 May 1983.
M.E. Smid and D.K. Branstad , “The Data Encryption Standard: Past and future”, Proceedings of the IEEE,76 (1988), 550–559.
M.E. Smid and D.K. Branstad , “The Data Encryption Standard: Past and future”, G.J. Simmons , editor, Contemporary Cryptology: The Science of Information Integrity, 43–64, IEEE Press, 1992. Appeared earlier as [1155].

M.E. Smid and D.K. Branstad , “Response to comments on the NIST proposed digital signature standard”, Advances in Cryptology–CRYPTO ’92 (LNCS 740), 76–88, 1993.
D.R. Smith and J.T. Palmer , “Universal fixed messages and the Rivest-Shamir-Adleman cryptosystem”, Mathematika,26 (1979), 44–52.
J.L. Smith , “Recirculating block cipher cryptographic system”, U.S. Patent # 3,796,830, 12 Mar 1974.
J.L. Smith , “The design of Lucifer: A cryptographic device for data communications”, IBM Research Report RC 3326, IBM T.J. Watson Research Center, Yorktown Heights, N.Y., 10598, U.S.A., Apr. 15 1971.
P. Smith and M. Lennon , “LUC: A new public key system”, E. Dougall , editor, Proceedings of the IFIP TC11 Ninth International Conference on Information Security, IFIP/Sec 93, 103–117, North-Holland, 1993.
P. Smith and C. Skinner , “A public-key cryptosystem and a digital signature system based on the Lucas function analogue to discrete logarithms”, Advances in Cryptology–ASIACRYPT ’94 (LNCS 917), 357–364, 1995.
R. Solovay and V. Strassen , “A fast Monte-Carlo test for primality”, SIAM Journal on Computing, 6 (1977), 84–85. Erratum in ibid, 7 (1978), 118.
J. Sorenson , “Two fast gcd algorithms”, Journal of Algorithms, 16 (1994), 110–144.
A. Sorkin , “Lucifer, a cryptographic algorithm”, Cryptologia, 8 (1984), 22–35.
M. Stadler , J.-M. Piveteau , and J. Camenisch , “Fair blind signatures”, Advances in Cryptology–EUROCRYPT ’95 (LNCS 921), 209–219, 1995.
O. Staffelbach and W. Meier , “Cryptographic significance of the carry for ciphers based on integer addition”, Advances in Cryptology–CRYPTO ’90 (LNCS 537), 601–614, 1991.
W. Stahnke , “Primitive binary polynomials”, Mathematics of Computation, 27 (1973), 977–980.
D.G. Steer , L. Strawczynski , W. Diffie , and M. Wiener , “A secure audio teleconference system”, Advances in Cryptology–CRYPTO ’88 (LNCS 403), 520–528, 1990.
J. Stein , “Computational problems associated with Racah algebra”, Journal of Computational Physics, 1 (1967), 397–405.
J.G. Steiner , C. Neuman , and J.I. Schiller , “Kerberos: an authentication service for open network systems”, Proceedings of the Winter 1988 Usenix Conference, 191–201, 1988.
M. Steiner , G. Tsudik , and M. Waidner , “Refinement and extension of encrypted key exchange”, Operating Systems Review, 29:3 (1995), 22–30.
J. Stern , “Secret linear congruential generators are not cryptographically secure”, Proceedings of the IEEE 28th Annual Symposium on Foundations of Computer Science, 421–426, 1987.
J. Stern , “An alternative to the Fiat-Shamir protocol”, Advances in Cryptology–EUROCRYPT ’89 (LNCS 434), 173–180, 1990.
J. Stern , “Designing identification schemes with keys of short size”, Advances in Cryptology–CRYPTO ’94 (LNCS 839), 164–173, 1994.
J. Stern , “A new identification scheme based on syndrome decoding”, Advances in Cryptology–CRYPTO ’93 (LNCS 773), 13–21, 1994.
D.R. Stinson , “An explication of secret sharing schemes”, Designs, Codes and Cryptography, 2 (1992), 357–390.
D.R. Stinson , Cryptography:Theory and Practice, CRC Press, Boca Raton, Florida, 1995.
S.G. Stubblebine and V.D. Gligor , “On message integrity in cryptographic protocols”, Proceedings of the 1992 IEEE Computer Society Symposium on Research in Security and Privacy, 85–104, 1992.
D.J. Sykes , “The management of encryption keys”, D.K. Branstad , editor, Computer security and the Data Encryption Standard, 46–53, NBS Special Publication 500–27, U.S. Department of Commerce, National Bureau of Standards, Washington, D.C., 1977.
P. Syverson , “Knowledge, belief and semantics in the analysis of cryptographic protocols”, Journal of Computer Security, 1 (1992), 317–334.
P. Syverson , “A taxonomy of replay attacks”, Proceedings of the Computer Security Foundations Workshop VII (CSFW 1994), 187–191, IEEE Computer Society Press, 1994.
P. Syverson and P. Van Oorschot , “On unifying some cryptographic protocol logics”, Proceedings of the 1994 IEEE Computer Society Symposium on Research in Security and Privacy, 14–28, 1994.
K. Tanaka and E. Okamoto , “Key distribution using id-related information directory suitable for mail systems”, Proceedings of the 8th Worldwide Congress on Computer and Communications Security and Protection (SECURICOM’90), 115–122, 1990.
A. Tarah and C. Huitema , “Associating metrics to certification paths”, Y. Deswarte , G. Eizenberg , and J.-J. Quisquater , editors, Second European Symposium on Research in Computer Security – ESORICS’92 (LNCS 648), 175–189, Springer-Verlag, 1992.
J.J. Tardo and K. Alagappan , “SPX: Global authentication using public key certificates”, Proceedings of the IEEE Symposium on Research in Security and Privacy, 232–244, 1991.
A. Tardy-Corfdir and H. Gilbert , “A known plaintext attack of FEAL-4 and FEAL-6”, Advances in Cryptology–CRYPTO ’91 (LNCS 576), 172–182, 1992.
M. Tatebayashi , N. Matsuzaki , and D.B. Newman JR., “Key distribution protocol for digital mobile communication systems”, Advances in Cryptology–CRYPTO ’89 (LNCS 435), 324–334, 1990.
R. Taylor , “An integrity check value algorithm for stream ciphers”, Advances in Cryptology–CRYPTO ’93 (LNCS 773), 40–48, 1994.
J.A. Thiong Ly , “A serial version of the Pohlig-Hellman algorithm for computing discrete logarithms”, Applicable Algebra in Engineering, Communication and Computing,4 (1993), 77–80.
J. Thompson , “S/MIME message specification – PKCS security services for MIME”, RSA Data Security Inc., Aug. 29 1995, http://www.rsa.com/.
T. Tokita , T. Sorimachi , and M. Matsui , “Linear cryptanalysis of LOKI and s2DES”, Advances in Cryptology–ASIACRYPT ’94 (LNCS 917), 293–303, 1995.
T. Tokita , T. Sorimachi , and M. Matsui , “On applicability of linear cryptanalysis to DES-like cryptosystems – LOKI89, LOKI91 and *s* 2DES”, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Science, E78-A (1995), 1148–1153. An earlier version appeared in [1192].
M. Tompa and H. Woll , “Random self-reducibility and zero-knowledge interactive proofs of possession of information”, Proceedings of the IEEE 28th Annual Symposium on Foundations of Computer Science, 472–482, 1987.
M. Tompa and H. Woll , “How to share a secret with cheaters”, Journal of Cryptology, 1 (1988), 133–138.
G. Tsudik , “Message authentication with one-way hash functions”, Computer Communication Review, 22 (1992), 29–38.
S. Tsujii and J. Chao , “A new ID-based key sharing system”, Advances in Cryptology–CRYPTO ’91 (LNCS 576), 288–299, 1992.

W. Tuchman , “Integrated system design”, D.K. Branstad , editor, Computer security and the Data Encryption Standard, 94–96, NBS Special Publication 500–27, U.S. Department of Commerce, National Bureau of Standards, Washington, D.C., 1977.
W. Tuchman , “Hellman presents no shortcut solutions to the DES”, IEEE Spectrum, 16 (1979), 40–41.
J. Van De Graaf and R. Peralta , “A simple and secure way to show the validity of your public key”, Advances in Cryptology–CRYPTO ’87 (LNCS 293), 128–134, 1988.
E. Van Heijst and T.P. Pedersen , “How to make efficient fail-stop signatures”, Advances in Cryptology–EUROCRYPT ’92 (LNCS 658), 366–377, 1993.
E. Van Heijst , T.P. Pedersen , and B. Pfitzmann , “New constructions of fail-stop signatures and lower bounds”, Advances in Cryptology–CRYPTO ’92 (LNCS 740), 15–30, 1993.
P. Van Oorschot , “A comparison of practical public key cryptosystems based on integer factorization and discrete logarithms”, G.J. Simmons , editor, Contemporary Cryptology: The Science of Information Integrity, 289–322, IEEE Press, 1992.
P. Van Oorschot , “Extending cryptographic logics of belief to key agreement protocols”, 1st ACM Conference on Computer and Communications Security, 232–243, ACM Press, 1993.
P. Van Oorschot , “An alternate explanation of two BAN-logic “failures””, Advances in Cryptology–EUROCRYPT ’93 (LNCS 765), 443–447, 1994.
P. Van Oorschot and M. Wiener , “A known-plaintext attack on two-key triple encryption”, Advances in Cryptology–EUROCRYPT ’90 (LNCS 473), 318–325, 1991.
P. Van Oorschot and M. Wiener , “Parallel collision search with applications to hash functions and discrete logarithms”, 2nd ACM Conference on Computer and Communications Security, 210–218, ACM Press, 1994.
P. Van Oorschot and M. Wiener , “Improving implementable meet-in-the-middle attacks by orders of magnitude”, Advances in Cryptology–CRYPTO ’96 (LNCS 1109), 229–236, 1996.
P. Van Oorschot and M. Wiener , “On Diffie-Hellman key agreement with short exponents”, Advances in Cryptology–EUROCRYPT ’96 (LNCS 1070), 332–343, 1996.
H.C.A. van Tilborg , An Introduction to Cryptology, Kluwer Academic Publishers, Boston, 1988.
H.C.A. van Tilborg , “Authentication codes: an area where coding and cryptology meet”, C. Boyd , editor, Cryptography and Coding, 5th IMA Conference, Proceedings, 169–183, Institute of Mathematics & Its Applications (IMA), 1995.
J. Van Tilburg , “On the McEliece public-key cryptosystem”, Advances in Cryptology–CRYPTO ’88 (LNCS 403), 119–131, 1990.
S.A. Vanstone and R.J. Zuccherato , “Elliptic curve cryptosystems using curves of smooth order over the ring n ”, IEEE Transactions on Information Theory, to appear.
S.A. Vanstone and R.J. Zuccherato , “Short RSA keys and their generation”, Journal of Cryptology, 8 (1995), 101–114.
S. Vaudenay , “On the need for multipermutations: Cryptanalysis of MD4 and SAFER”, B. Preneel , editor, Fast Software Encryption, Second International Workshop (LNCS 1008), 286–297, Springer-Verlag, 1995.
S. Vaudenay , “On the weak keys of Blowfish”, D. Gollmann , editor, Fast Software Encryption, Third International Workshop (LNCS 1039), 27–32, Springer-Verlag, 1996.
U.V. Vazirani , “Towards a strong communication complexity theory, or generating quasi-random sequences from two communicating slightly-random sources”, Proceedings of the 17th Annual ACM Symposium on Theory of Computing, 366–378, 1985.
U.V. Vazirani and V. V. Vazirani , “Efficient and secure pseudo-random number generation”, Proceedings of the IEEE 25th Annual Symposium on Foundations of Computer Science, 458–463, 1984. This paper also appeared in [1219].
U.V. Vazirani and V. V. Vazirani , “Efficient and secure pseudorandom number generation”, Advances in Cryptology–Proceedings of CRYPTO 84 (LNCS 196), 193–202, 1985.
K. Vedder , “Security aspects of mobile communications”, B. Preneel , R. Govaerts , and J. Vandewalle , editors, Computer Security and Industrial Cryptography: State of the Art and Evolution (LNCS 741), 193–210, Springer-Verlag, 1993.
G.S. Vernam , “Secret signaling system”, U.S. Patent # 1,310,719, 22 Jul 1919.
G.S. Vernam , “Cipher printing telegraph systems for secret wire and radio telegraphic communications”, Journal of the American Institute for Electrical Engineers, 55 (1926), 109–115.
J. Von Neumann , “Various techniques used in connection with random digits”, Applied Mathematics Series, U.S. National Bureau of Standards, 12 (1951), 36–38.
J. Von Zur Gathen and V. Shoup , “Computing Frobenius maps and factoring polynomials”, Computational Complexity, 2 (1992), 187–224.
V.L. Voydock and S.T. Kent , “Security mechanisms in high-level network protocols”, Computing Surveys, 15 (1983), 135–171.
D. Wackerly , W. Mendenhall Iii , and R. Scheaffer , Mathematical Statistics with Applications, Duxbury Press, Belmont, California, 5th edition, 1996.
M. Waidner and B. Pfitzmann , “The dining cryptographers in the disco: Unconditional sender and recipient untraceability with computationally secure serviceability”, Advances in Cryptology–EUROCRYPT ’89 (LNCS 434), 690, 1990.
C.P. Waldvogel and J.L. Massey , “The probability distribution of the Diffie-Hellman key”, Advances in Cryptology–AUSCRYPT ’92 (LNCS 718), 492–504, 1993.
S.T. Walker , S.B. Lipner , C.M. Ellison , and D.M. Balenson , “Commercial key recovery”, Communications of the ACM, 39 (1996), 41–47.
C.D. Walter , “Faster modular multiplication by operand scaling”, Advances in Cryptology–CRYPTO ’91 (LNCS 576), 313–323, 1992.
P.C. Wayner , “Content-addressable search engines and DES-like systems”, Advances in Cryptology–CRYPTO ’92 (LNCS 740), 575–586, 1993.
D. Weber , “An implementation of the general number field sieve to compute discrete logarithms mod p”, Advances in Cryptology–EUROCRYPT’95 (LNCS 921), 95–105, 1995.
A.F. Webster and S.E. Tavares , “On the design of S-boxes”, Advances in Cryptology–CRYPTO ’85 (LNCS 218), 523–534, 1986.
M.N. Wegman and J.L. Carter , “New hash functions and their use in authentication and set equality”, Journal of Computer and System Sciences, 22 (1981), 265–279.
D. Welsh , Codes and Cryptography, Clarendon Press, Oxford, 1988.
A.E. Western and J.C.P. Miller , Tables of Indices and Primitive Roots, volume 9, Royal Society Mathematical Tables, Cambridge University Press, 1968.
D.J. Wheeler , “A bulk data encryption algorithm”, R. Anderson , editor, Fast Software Encryption, Cambridge Security Workshop (LNCS 809), 127–134, Springer-Verlag, 1994.

D.J. Wheeler and R.M. Needham , “TEA, a tiny encryption algorithm”, B. Preneel , editor, Fast Software Encryption, Second International Workshop (LNCS 1008), 363–366, Springer-Verlag, 1995.
D.H. Wiedemann , “Solving sparse linear equations over finite fields”, IEEE Transactions on Information Theory, 32 (1986), 54–62.
M.J. Wiener , “Cryptanalysis of short RSA secret exponents”, IEEE Transactions on Information Theory, 36 (1990), 553–558.
M.J. Wiener , “Efficient DES key search”, Technical Report TR-244, School of Computer Science, Carleton University, Ottawa, 1994. Presented at Crypto ’93 rump session.
S. Wiesner , “Conjugate coding”, SIGACT News, 15 (1983), 78–88. Original manuscript (circa 1970).
H.S. Wilf , “Backtrack: An O(1) expected time algorithm for the graph coloring problem”, Information Processing Letters,18 (1984), 119–121.
M.V. Wilkes , Time-Sharing Computer Systems, American Elsevier Pub. Co., New York, 3rd edition, 1975.
F. Willems , “Universal data compression and repetition times”, IEEE Transactions on Information Theory, 35 (1989), 54–58.
H.C. Williams , “A modification of the RSA public-key encryption procedure”, IEEE Transactions on Information Theory,26 (1980), 726–729.
H.C. Williams , “A $p + 1$ method of factoring”, Mathematics of Computation, 39 (1982), 225–234.
H.C. Williams , “Some public-key crypto-functions as intractable as factorization”, Cryptologia,9 (1985), 223–237.
H.C. Williams and B. Schmid , “Some remarks concerning the M.I.T. public-key cryptosystem”, BIT, 119 (1979), 525–538.
R.S. Winternitz , “A secure one-way hash function built from DES”, Proceedings of the 1984 IEEE Symposium on Security and Privacy, 88–90, 1984.
S. Wolfram , “Cryptography with cellular automata”, Advances in Cryptology–CRYPTO ’85 (LNCS 218), 429–432, 1986.
S. Wolfram , “Random sequence generation by cellular automata”, Advances in Applied Mathematics, 7 (1986), 123–169.
H. Woll , “Reductions among number theoretic problems”, Information and Computation, 72 (1987), 167–179.
A.D. Wyner , “The wire-tap channel”, Bell System Technical Journal, 54 (1975), 1355–1387.
Y. Yacobi , “A key distribution “paradox””, Advances in Cryptology–CRYPTO ’90 (LNCS 537), 268–273, 1991.
Y. Yacobi and Z. Shmuely , “On key distribution systems”, Advances in Cryptology–CRYPTO ’89 (LNCS 435), 344–355, 1990.
A.C. Yao , “On the evaluation of powers”, SIAM Journal on Computing, 5 (1976), 100–103.
A.C. Yao , “Theory and applications of trapdoor functions”, Proceedings of the IEEE 23rd Annual Symposium on Foundations of Computer Science, 80–91, 1982.
S.-M. Yen and C.-S. Laih , “New digital signature scheme based on discrete logarithm”, Electronics Letters, 29 (June 10, 1993), 1120–1121.
C. Yuen , “Testing random number generators by Walsh transform”, IEEE Transactions on Computers, 26 (1977), 329–333.
D. Yun , “Fast algorithm for rational function integration”, Information Processing 77: Proceedings of IFIP Congress 77, 493–498, 1977.
G. Yuval , “How to swindle Rabin”, Cryptologia, 3 (1979), 187–190.
K. Zeng and M. Huang , “On the linear syndrome method in cryptanalysis”, Advances in Cryptology–CRYPTO ’88 (LNCS 403), 469–478, 1990.
K. Zeng , C.-H. Yang , and T.R.N. Rao , “On the linear consistency test (LCT) in cryptanalysis with applications”, Advances in Cryptology–CRYPTO ’89 (LNCS 435), 164–174, 1990.
K. Zeng , C.-H. Yang , and T.R.N. Rao , “An improved linear syndrome algorithm in cryptanalysis with applications”, Advances in Cryptology–CRYPTO ’90 (LNCS 537), 34–47, 1991.
K. Zeng , C.-H. Yang , D.-Y. Wei , and T. R. N. Rao , “Pseudorandom bit generators in stream-cipher cryptography”, Computer, 24(1991), 8–17.
C. Zhang , “An improved binary algorithm for RSA”, Computers and Mathematics with Applications, 25:6 (1993), 15–24.
Y. Zheng , J. Pieprzyk , and J. Seberry , “HAVAL – a one-way hashing algorithm with variable length of output”, Advances in Cryptology–AUSCRYPT ’92 (LNCS 718), 83–104, 1993.
Y. Zheng and J. Seberry , “Immunizing public key cryptosystems against chosen ciphertext attacks”, IEEE Journal on Selected Areas in Communications, 11 (1993), 715–724.
N. Zierler , “Primitive trinomials whose degree is a Mersenne exponent”, Information and Control, 15 (1969), 67–69.
N. Zierler and J. Brillhart , “On primitive trinomials (mod 2)”, Information and Control, 13 (1968), 541–554.
P.R. Zimmermann , The Official PGP User’s Guide, MIT Press, Cambridge, Massachusetts, 1995 (second printing).
J. Ziv and A. Lempel , “On the complexity of finite sequences”, IEEE Transactions on Information Theory, 22 (1976), 75–81.
M. ŽIvkovlć , “An algorithm for the initial state reconstruction of the clock-controlled shift register”, IEEE Transactions on Information Theory, 37 (1991), 1488–1490.
M. ŽIvkovlć , “A table of primitive binary polynomials”, Mathematics of Computation, 62 (1994), 385–386.
M. ŽIvkovlć , “Table of primitive binary polynomials. II”, Mathematics of Computation, 63 (1994), 301–306.