Pro Cryptography and Cryptanalysis

Creating Advanced Algorithms with C# and .NET

—

Marius Iulian Mihailescu
Stefania Loredana Nita

Apress®

Pro Cryptography and Cryptanalysis

Creating Advanced Algorithms with C# and .NET

Marius Iulian Mihailescu
Stefania Loredana Nita

Apress®

Pro Cryptography and Cryptanalysis: Creating Advanced Algorithms with C# and .NET

Marius Iulian Mihailescu
Bucharest, Romania

Stefania Loredana Nita
Bucharest, Romania

ISBN-13 (pbk): 978-1-4842-6366-2
ISBN-13 (electronic): 978-1-4842-6367-9
https://doi.org/10.1007/978-1-4842-6367-9

Managing Director, Apress Media LLC: Welmoed Spahr
Acquisitions Editor: Joan Murray
Development Editor: Laura Berendson
Coordinating Editor: Jill Balzano

Cover image designed by Freepik (www.freepik.com)

Distributed to the book trade worldwide by Springer Science+Business Media LLC, 1 New York Plaza, Suite 4600, New York, NY 10004. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail orders-ny@springer-sbm.com, or visit www.springeronline.com. Apress Media, LLC is a California LLC and the sole member (owner) is Springer Science + Business Media Finance Inc (SSBM Finance Inc). SSBM Finance Inc is a **Delaware** corporation.

For information on translations, please e-mail booktranslations@springernature.com; for reprint, paperback, or audio rights, please e-mail bookpermissions@springernature.com.

Apress titles may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Print and eBook Bulk Sales web page at www.apress.com/bulk-sales.

Any source code or other supplementary material referenced by the author in this book is available to readers on GitHub via the book's product page, located at www.apress.com/9781484263662. For more detailed information, please visit www.apress.com/source-code.

Printed on acid-free paper

To our families

Table of Contents

About the Authors

Marius Iulian Mihailescu, PhD is the CEO of Dapyx Solution Ltd., a company focused on security- and cryptography-related research. He has authored and co-authored more than 50 articles, journal contributions, and conference proceedings, and three books related to security and cryptography. He lectures at well-known national and international universities, teaching courses on programming, cryptography, information security, and other technical topics. He holds a PhD (thesis on applied cryptography over biometrics data), an MSc in information security, and and an MSc in software engineering.

Stefania Loredana Nita, PhD is a software developer and researcher at the Institute for Computers. Prior to that she was an assistant lecturer at the University of Bucharest, where she taught courses on advanced programming techniques, simulation methods, and operating systems. She has authored and co-authored more than 15 papers and journals, most recently *Advanced Cryptography and Its Future: Searchable and Homomorphic Encryption,* as well as two books. She holds a PhD (thesis on advanced cryptographic schemes using searchable encryption and homomorphic encryption), an MSc in software engineering, a BSc in computer science, and a BSc in mathematics.

About the Technical Reviewer

Doug Holland is a software engineer and architect at Microsoft Corporation and holds a Masters degree in software engineering from the University of Oxford. Before joining Microsoft, he was awarded the Microsoft MVP and Intel Black Belt Developer awards.

Introduction

Information represents one of the most important aspects that need to be taken into consideration when complex systems are designed and implemented, such as business, organizations, and military operations. Information that falls into the wrong hands can be a disaster and can lead to a huge loss of business or catastrophic results. In order to secure communication, cryptology (cryptography and cryptanalysis) can be used to cipher information.

Due to the rapid growth of electronic communication, the issues in information security are increasing every day. Messages that are exchanged over worldwide, publicly accessible computer networks must be protected and retained and must also have protection mechanisms against manipulation. Electronic business requirements consist of having digital signatures that are recognized by the law. With the help of modern cryptography, we have solutions to all of these problems.

This book was borne from cryptography courses (theoretical and applied cryptography) given to students (graduate and undergraduate levels) in computer science at the University of Bucharest and Titu Maiorescu University; business experience at national and international companies; ethical hacking best practices; and security audits. The book it is intended to cover the most advanced cryptography and cryptanalysis techniques together with their implementations using C# and the .NET Framework, giving a practical perspective, helping readers to think of cryptography and cryptanalysis techniques in terms of practice. Some of the implementations in C# will be given using the new features of C# 8.0 (see Chapter 6). As an advanced and exhaustive book, serving as a comprehensive guide to the most important topics in security information, cryptography, and cryptanalysis, the book can be used for a wide range of purposes and areas by multiple professionals, such as security experts with their audits, military experts and personnel, ethical hackers, teachers in academia, researchers, software developers, and software engineers when security and cryptographic solutions need to be implemented in a real business software environment; student courses (undergraduate and graduate levels, master degree, professional and academic doctoral degree); business analysts, and many more.

Cryptography and Cryptanalysis

We consider it useful to define some of the main notions we will work with throughout the book.

CRYPTOGRAPHY represents the defensive side of cryptology. Its main objective is to create and design the cryptographic systems and their rules. Cryptography can be seen as the art of protecting the information by transforming it into an unreadable format called cipher text.

CRYPTANALYSIS represents the offensive side of cryptology. Its main objective is to study the cryptographic systems with the goal of providing necessary characteristics in such a way as to fulfill the function for which they have been designed. Cryptanalysis has the possibility to analyze the cryptographic systems of third parties through the cryptograms realized with them, in such way that breaking them obtains useful information for their business purposes. The people who are dealing with this field are known as cryptanalysts, code breakers, or ethical hackers.

CRYPTOLOGY represents the science or art of secret writings. Its main objective is to protect and defend the secrets of the data and the confidentiality of the information with the help of cryptographic algorithms.

The book examines all three sides from a practical side with references to the theoretical background by illustrating how a theoretical algorithm should be exploited and spread in order to be implemented.

Book Structure

The book has 24 chapters divided within three parts (see Table 1): Part I – Foundational Topics (Chapters 1-9), Part II – Cryptography (Chapters 10-17), and Part III – Cryptanalysis (18-24). Figure 1 shows how to read the book and what chapters depend on each other.

In ***Part I - Foundations (Chapters 1-9)***, the book covers a beginner-to-advanced level, from theoretical to practical: the fundamental concepts of cryptography (*Chapter 1*). In *Chapter 2,* we cover a collection of basic key elements on complexity theory, probability theory, information theory, number theory, abstract algebra, and finite fields.

Chapters 3 and *Chapter 4* deal with integer arithmetic and floating-point arithmetic processing and algorithms. The importance of these chapters is quite vital, and other chapters and algorithm implementations are dependent on the content of these chapters.

In *Chapter 5*, we discuss the newest features and enhancements of C# 8.0. We present how the features and enhancements play an important role in developing cryptography and cryptanalysis algorithms and methods. We cover readonly members, default interface methods, pattern matching enhancements, how to use the new type of declarations, static local functions, disposable ref types, nullable reference types, asynchronous streams, indices and ranges, null-coalescing assignments, unmanaged constructed types, stackalloc in nested expressions, and enhancement of interpolated verbatim strings.

Chapter 6 covers the most important guidelines for secure coding, focusing on the balance between security and usability in most expected scenarios by using trusted code. We also cover sensitive topics such as securing state data, security and user input, security-neutral code, and library codes that expose the protected resources.

Chapter 7 covers the cryptography model and cryptographic services for .NET. Vital topics include .NET Framework basic implementations, object inheritance, how cryptography algorithms are implemented, stream design (the`CryptoStream` class), configuring cryptography classes, how to choose cryptography algorithms, generating the keys for encryption and decryption, storing asymmetric keys in a key container, cryptographic signatures, ensuring data integrity using hash codes and functions, creating and designing cryptographic schemes, encryption of XML elements with symmetric keys, assuring and guaranteeing interoperability of the applications between different platforms, such as Windows to Linux and vice-versa, and many other important related topics.

Chapter 8 covers the architecture of the `System.Security.Cryptography` namespace and how it can be used during coding. The chapter discusses cryptographic services, secure encoding and decoding of data, and operations (hashing, random number generation, message authentication, etc.).

Chapter 9 discusses in detail several cryptographic libraries (e.g. NSec, Bouncy Castle, Inferno, and SecureBlackbox) which are open source and have a higher level of trustiness. They can be used during the development process or as an example and source of inspiration for implementing your own algorithms.

In ***Part II – Pro Cryptography (Chapters 10-17)***, the book covers the most important frameworks that are developed in C# and .NET, such as elliptic-curve cryptography (*Chapter 9*). The discussion is conducted further with advanced cryptography topics (*Chapters 11-17*) by presenting practical implementations and showing how to treat such advanced topics from a theoretical mathematical background to a real-life environment.

Chapter 10 discusses Cryptography Next Generation (CNG), which helps us to implement the Elliptic Curve Diffie-Hellman (ECDH) algorithm and perform the necessary cryptographic operations.

Chapter 11 uses the Lattice Cryptography Library for implementation, pointing out the importance for post-quantum cryptography. Implementations of key exchange protocols proposed by Alkim, Ducas, Poppelmann, and Schwabe [1] will be discussed. Also, an instantiation of the Chris Peikert key exchange protocol [2] will be discussed. We reiterate that the implementation is based on a novel technique for computing, known as the Number Theoretic Transform, in order to apply errorless, fast convolution functions over successions of integer numbers.

Chapter 12 and *Chapter 13* discuss two advanced cryptography topics, homomorphic and searchable encryption. For searchable encryption (SE), in *Chapter 12*, we give a brief implementation and solution in C# for SE by pointing out the advantages and disadvantages and by eradicating the most common patterns from encrypted data. In *Chapter 13*, for homomorphic encryption (HE), we examine the implementation of HElib (Homomorphic Encryption Library) by using the design and implementation proposed in 2013 by Shai Halevi and Victor Shoup in [3].

Chapter 14 introduces the issues raised during the implementation of (ring) learning with errors cryptography mechanisms. We give a lattice-based key exchange protocol implementation— a library that is used for experimentation purposes.

Chapter 15 introduces new concepts behind the transposition of the theory of chaos-based cryptography into practice. The results and outputs of the chapter represent an important advance of cryptography as it is a new topic which hasn't received proper attention until now.

Chapter 16 presents solutions for implementing securing methods for big data analytics, access control methods (key management for access control), attributed-based access control, secure search, secure data processing, functional encryption, and multi-party computation.

Chapter 17 discusses the security issues raised about applications that are running in a cloud environment and how they can be resolved during the designing and implementation phase.

In ***Part III – Pro Cryptanalysis (Chapters 18-24)***, we deal with advanced cryptanalysis topics and we show how to pass the barrier between theory and practice, and how to think of cryptanalysis in terms of practice by eliminating the most vulnerable and critical points of a system or software application in a network or distributed environment.

Starting with *Chapter 18* we provide an introduction to cryptanalysis by presenting the most important characteristics of cryptanalysis.

Chapter 19 starts by showing the important criteria and standards used in cryptanalysis, how the tests of cryptographic systems are made, the process of selecting the cryptographic modules, the cryptanalysis operations, and classifications of cryptanalysis attacks.

In *Chapter 20* and *Chapter 21*, we show how to implement and design linear, differential, and integral cryptanalysis. We focus on techniques and strategies whose primary role is to show how to implement scripts for attacking linear and differential attacks.

Chapter 22 presents the most important attacks and how they can be designed and implemented using C# and .NET. We examine the behavior of the software applications when they are exposed to different attacks and we exploit the source code. We discuss software obfuscation and we show why this is a critical aspect that needs to be taken into consideration by the personnel involved in implementing process of the software. Also, we show how this analysis can lead to machine learning and artificial intelligence algorithms that can be used to predict future attacks over the software applications that are running in a distributed or cloud environment.

In *Chapter 23*, we go through text characterization methods and their implementation. We discuss chi-squared statistic; identifying unknown ciphers; index of coincidence; monogram, bigram, and trigram frequency counts; quadgram statistics as a fitness measure; unicity distance; and word statistics as a fitness measure.

Chapter 24 presents the advantages and disadvantages of implementing the cryptanalysis methods, why they should have a special place when applications are developed in distributed environments, and how the data should be protected against such cryptanalysis methods.

Table 1. *Book Structure*

Part	Chapter Number	Chapter Title
Part I Foundations (Foundational Topics)	1	Cryptography Fundamentals
	2	Mathematical Background and Its Applicability in Cryptography
	3	Large Integer Arithmetic
	4	Floating-Point Arithmetic
	5	What's new in C# 8.0
	6	Secure Coding Guidelines
	7	Cryptographic Services in .NET
	8	Overview of the *System.Security.Cryptography* Namespace
	9	Cryptography Libraries in C# and .NET
Part II Pro Cryptography	10	Elliptic-Curve Cryptography
	11	Lattice-Based Cryptography
	12	Searchable Encryption
	13	Homomorphic Encryption
	14	(Ring) Learning with Errors Cryptography
	15	Chaos-Based Cryptography
	16	Big Data Cryptography
	17	Cloud Computing Cryptography
Part III Pro Cryptanalysis	18	Getting Started with Cryptanalysis
	19	Cryptanalysis Attacks and Techniques
	20	Linear and Differential Cryptanalysis
	21	Integral Cryptanalysis
	22	Attacks
	23	Text Characterization
	24	Implementations of Cryptanalysis Methods

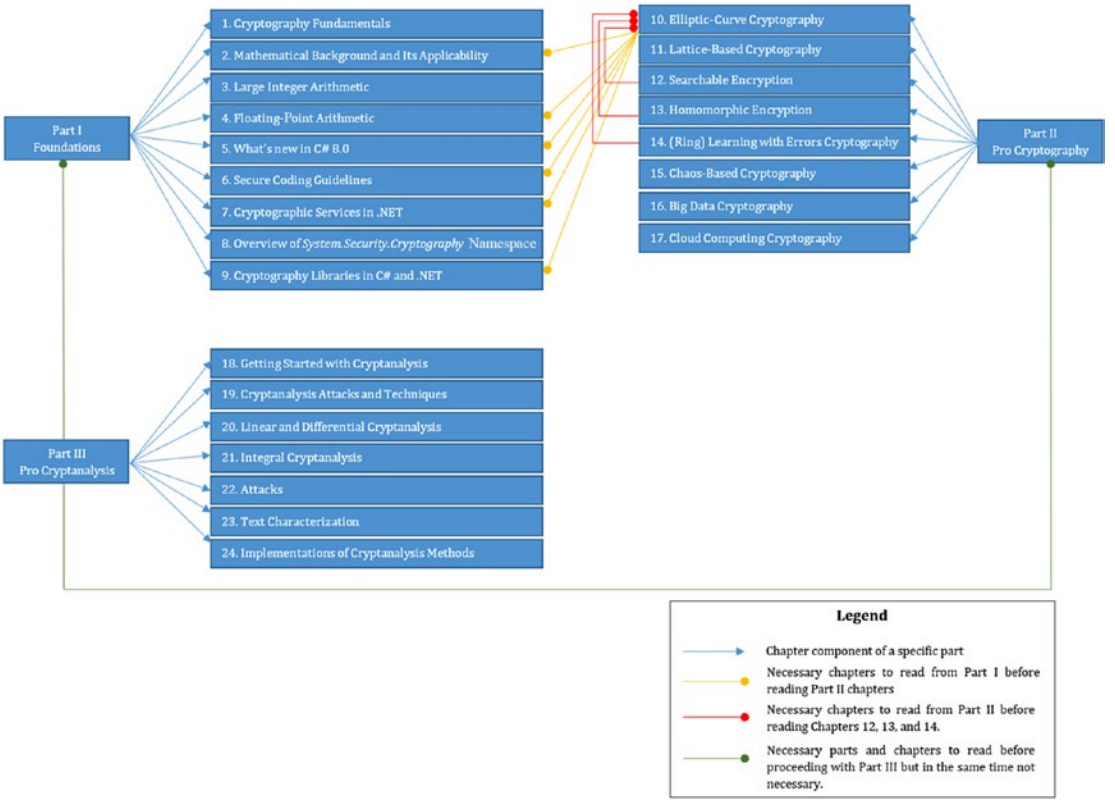

Figure 1. *A roadmap for readers and professionals*

Internet Resources

There are a number of very important resources available on the Web that can be useful for this book and help the readers keep up with the advancements and progress in the field.

- Bill's Security Site, `https://asecuritysite.com/`, contains multiple implementations of cryptographic algorithms. The website is maintained by Bill Buchanan, Professor at the School of Computing at Edinburgh Napier University.
- Books by William Stallings [4] including *Cryptography and Network Security*, `http://williamstallings.com/Cryptography/`. The site includes various important sets of tools and resources that the author updates frequently, keeping in step with the most important advances in the field of cryptography.

- Schneier on Security, www.schneier.com/. The website contains sections on books, essays, accurate news, talks, and academic resources.

Forums and Newsgroups

A number of USENET (being deprecated but it still contains useful information) newsgroups are dedicated to some of the important aspects of cryptography and network security. The most important are

- `sci.crypt.research` is one of the best groups to follow. It is a moderated newsgroup and its main purpose is to deal with research topics. Most of the topics are related to the technical aspects of cryptology.
- `sci.crypt` is a group where we can find general discussions about cryptology and related topics.
- `sci.crypt.random-numbers` offers discussions about random number generators.
- `alt.security` offers general discussions on security topics.
- `comp.security.misc` has general discussions on computer security topics.
- `comp.security.firewalls` has discussions about firewalls and other related products.
- `comp.security.announce` is a source for CERT news and announcements.
- `comp.risks` holds discussions about the public risks from computers and users.
- `comp.virus` offers moderated discussions about computer viruses.

Also, there are a number of forums that deal with cryptography topics and news that are available on the Internet. The most important are

- Reddit – Cryptography News and Discussions [5]: This forum group contains general information and news about different topics related to cryptography and information security.
- Security forums [6] cover a vast amount of topics and discussions about computer security and cryptography.
- TechnGenix – Security [7]: One of the most updated forums with news related to cryptography and information security. The group is maintained by leading security professionals in the field.
- Wilders Security Forum [8]: The forum contains discussions and news about the vulnerabilities of software applications due to bad implementations of cryptographic solutions.
- Security Focus [9]: The forum contains a series of discussions about the vulnerabilities raised by implementations of cryptographic algorithms.
- Security InfoWatch [10]: The discussions are related to data and information loss.
- TechRepublic – Security [11]: The forum contains discussions about practical aspects and methodologies that can be used when software applications are designed and implemented.
- Information Security Forum [12]: A world-leading forum in the fields of information security and cryptography. The forum contains conferences, hands-on and practical tutorials, solving solutions to security and cryptographic issues.

Standards

Many of the cryptographic techniques and implementations described in this book are in accordance with the following standards. These standards have been developed and designed to cover management practices and the entire architecture of security mechanisms, strategies, and services.

The most important standards covered by the current book are

- **National Institute of Standards and Technology (NIST)**: NIST represents the U.S. federal agency that deals with standards, science, and technologies that are related to the U.S. government. Excepting the national goal, the NIST Federal Information Processing Standards (FIPS) and the Special Publications (SP) have a very important worldwide impact.
- **Internet Society**: ISOC represents one of the most important professional membership societies with organizational and individual membership worldwide. The society provides leadership on issues relating to the future perspective of the Internet and applications that are developed using security and cryptographic mechanisms, with respect for the groups that are responsible, such as the Internet Engineering Task Force (IETF) and the Internet Architecture Board (IAB). The mentioned organizations develop Internet standards, known and published as RFCs (Requests for Comments).
- **ITU-T**: The International Telecommunication Union (ITU) represents one of the most powerful organizations within the United Nations System. Together with governments and the private sector, it coordinates and administrates the global telecom networks and services. ITU-T represents one of the three sectors of ITU. The mission of ITU-T consists of the production of the standards that cover all the fields of telecommunications. The standards proposed by ITU-T are known as Recommendations.
- **ISO:** The International Organizations for Standardization (ISO) represents a world-wide federation that contains national standards bodies from over 140 countries. ISO is a nongovernmental organization with the goal of promoting the development of standardization and activities that are related with a view to facilitate the international exchange of services to develop cooperation with intellectual, scientific, and technological activities. The results of the ISO are as international agreements published as International Standards.

Conclusions

We are living in the era of unimaginable evolution and incredible technologies that enable the instant flow of information at any time and to any place. The secret lies in the convergence process of the computer with the networks—a very important key force in the evolution and development of these incredible technologies.

In this introduction, we outlined the objectives of the book and their benefits. We successfully showed the mission of the book, addressing the practical aspects of cryptography and information security and its main intention of using the current work. The process of using systems that build advanced information technologies has been shown to have a deep impact on our lives every day. All the technologies prove to be pervasive and ubiquitous.

The book represents the first practical step of translating the most important theoretical cryptography algorithms and mechanisms into practice through one of the most powerful programming languages, C#).

In this introduction, you learned the following:

- The difference between cryptography, cryptanalysis, and cryptology was explained in order to eliminate confusion.
- The book structure was discussed in order to help the reader to easily follow the content. Also, a roadmap was presented to the reader with the goal of showing the dependencies of each chapter and what is necessary for each chapter to be followed. Each chapter was presented in detail, presenting its main objective.
- This chapter included a list of newsgroups, websites, and USENETs, resources where the readers can keep themselves updated with the latest news in fields of cryptography and information security.
- This chapter listed the most important standards used in the fields of cryptography and information security. The reader is now familiar with the process and how each standard works.

Bibliography

[1] Alkim, E., Ducas, L., Pöppelmann, T., & Schwabe, P. (2016). Post-quantum key exchange—a new hope. In 25th {USENIX} Security Symposium ({USENIX} Security 16) (pp. 327-343).

[2] Peikert, C. (2014, October). Lattice cryptography for the internet. In international workshop on post-quantum cryptography (pp. 197-219). Springer, Cham.

[3] Halevi, S., & Shoup, V. (2013). Design and implementation of a homomorphic-encryption library. IBM Research (Manuscript), 6, 12-15.

[4] Stallings, W., Cryptography and Network Security - Principles and Practice. 5 ed. 2010: Pearson. 744.

[5] Reddit. Cryptography News and Discussions. Available from: www.reddit.com/r/crypto/.

[6] Forums, Security. Available from: www.security-forums.com/index.php?sid=acc302c71bb3ea3a7d631a357223e261.

[7] TechGenix, Security. Available from: http://techgenix.com/security/.

[8] Wilders Security Forums. Available from: www.wilderssecurity.com/.

[9] Security Focus. Available from: www.securityfocus.com/.

[10] Security InfoWatch. Available from: https://forums.securityinfowatch.com/.

[11] TechRepublic – Security. Available from: www.techrepublic.com/forums/security/.

[12] Information Security Forum. Available from: www.securityforum.org/.

PART I

Foundational Topics

CHAPTER 1

Cryptography Fundamentals

Introduction

The history of cryptography is very long and interesting. For a complete non-technical reference of cryptography, we recommend *The Codebreakers* [1]. The book presents cryptography from its initial use by the Egyptians around 4,000 years ago to recent history when it played a vital role in the outcome of both world wars. The book was written in **1963** and covers aspects of history that were significant in terms of the development of cryptography. Cryptography is seen as an art and it is associated with diplomatic services, military personnel, and governments. Cryptography has been used as a tool for protecting strategies and different secrets related to national security.

The most important development in the history of cryptography was in **1976** when Diffie and Hellman [2] published the work paper entitled "New Directions in Cryptography." The paper introduced the concept that revolutionized how cryptography was seen: public-key cryptography. The authors also introduced a new and ingenious method for key exchange. The security of the method is based on the intractability of the discrete logarithm problem. At that time, the authors didn't have a practical implementation of the public-key encryption scheme, an idea that was very clear and started to generate significant interest in the cryptographic community. Starting in **1978**, the first implementation of a public-key encryption and signature scheme was proposed by Rivest, Shamir, and Adleman (nowadays known as RSA [3]). The RSA scheme is based on the intractability of factoring large integers. If we are doing a parallel between integer factorization from RSA and Shor's Algorithm, we will observe that the last algorithm will run in polynomial time for quantum computers and it will represent an important challenge to any cryptography approach that is based on the hardness assumption of

M. I. Mihailescu and S. L. Nita, *Pro Cryptography and Cryptanalysis*,
https://doi.org/10.1007/978-1-4842-6367-9_1

factoring large integers [62]. The application of factoring large integers and its purpose has increased the number of the methods for factoring. In **1980,** there were important advancements in this area but none of them showed any improvements for the security of RSA. A very important class of practical public-key schemes was found and proposed in **1985** by ElGamal [4]. His schemes are also based on the problem of the discrete logarithm.

The most important and significant contribution provided by public-key cryptography is represented by the digital signature. In **1991**, the ISO/IEC 9796 international standard for digital signatures was adopted [5]. The standard is based on the RSA public-key scheme. In **1994**, the United States government adopted the Digital Signature Standard, a powerful scheme based on the problem of the discrete logarithm.

Nowadays, searching for new public-key scheme, improvements on the current cryptographic mechanisms, and designing new proofs for security are still happening and continue to bring significant improvements.

The goal and purpose of this book is to explain the latest updates of the principles, techniques, algorithms, and implementations of the most important aspects of cryptography in practice. The focus is on the aspects that are most practical and applied. You will learn about the aspects that represent issues and we will point to references in literature and best practices that provide solutions. Due to the large volume of material covered, most of the results will be accompanied by implementations. This also serves to not obscure the real nature of cryptography. The book offers strong material for both implementers and researchers. The book describes algorithms and software systems with their interactions.

Information Security and Cryptography

In this book, the term and concept of *information* can be understood as *quantity*. In order to make an introduction to cryptography and its applications through algorithms and implementation technologies (such as C#), you need to understand the issues that are related to information security. All parties who participate in a certain transaction must have the confidence that specific objectives that are associated with the information security have been followed. The objectives are listed in Table 1-1.