Preface

The first edition of this book was published in March 1995. At that time, my objective was to produce a general textbook that treated all the essential core areas of cryptography, as well as a selection of more advanced topics. In writing the book, I tried to design it to be flexible enough to permit a wide variety of approaches to the subject, so that it could be used for both undergraduate and graduate university courses in cryptography in mathematics, computer science or engineering.

The following were some of the important features of the first edition of the book, all of which are retained in the second edition.

- Mathematical background was provided where it was needed, in a "just-in-time" fashion.
- Informal descriptions of the cryptosystems were given along with more precise pseudo-code descriptions.
- Examples were presented to illustrate the workings of the algorithms.
- The mathematical underpinnings of the algorithms and cryptosystems were explained carefully and rigorously.
- Numerous exercises were included, some of them quite challenging.

The first edition of the book contained thirteen chapters. When I began to work on this revision a couple of years ago, it soon became clear that there was a wealth of new material I wanted to incorporate into the second edition. In order to keep the book from growing too large, and, also, to allow me to finish the book in a reasonable amount of time, I decided to focus the second edition more tightly on the core areas of cryptography that are most likely to be covered in a course. The result is that the second edition of the book consists of updated, revised, expanded and reorganized versions of the first seven chapters of the first edition. I plan to begin writing a companion volume quite soon, which will contain updated treatments of other chapters from the first edition, as well as chapters covering new topics.

Here is a brief synopsis of the seven chapters in this second edition of "Cryptography Theory and Practice":

• Chapter 1 remains a fairly elementary introduction to simple "classical" cryptosystems. Some topics have been updated or improved, e.g., a simplified cryptanalysis of the *Vigenère Cipher*, based on a suggestion of Dan Velleman, is given.

• Chapter 2 covers the main elements of Shannon's approach to cryptography, including the concept of perfect secrecy and the use of information theory in cryptography. It has not been changed significantly; however, it includes a more careful treatment of elementary probability theory than the first edition did.

• Chapter 3 has been almost completely rewritten. The corresponding chapter in the first edition dealt almost exclusively with the *Data Encryption Standard*, which is now obsolete. I decided to use substitution-permutation networks as a mathematical model to introduce many of the concepts of modern block cipher design and analysis, including differential and linear cryptanalysis. There is more emphasis on general principles than before, and the specific cryptosystems that are discussed (*DES* and the new *Advanced Encryption Standard*) serve to illustrate these general principles.

• Chapter 4 is a significantly improved version of the old Chapter 7. This chapter now contains a unified treatment of keyed and unkeyed hash functions and their application to the construction of message authentication codes. There is an emphasis on mathematical analysis and security proofs. This chapter includes a description of the *Secure Hash Algorithm*.

• Chapter 5 concerns the *RSA Cryptosystem*, together with a considerable amount of background on number-theoretic topics such as primality testing and factoring. It has been expanded to include several new sections, including Pollard's rho algorithm, Wiener's low decryption exponent attack, and semantically secure RSA-based cryptosystems.

• Chapter 6 discusses public-key cryptosystems, such as the *ElGamal Cryptosystem*, that are based on the Discrete Logarithm problem. This chapter also includes a considerable amount of new material, such as the Pollard rho algorithm, lower bounds on the complexity of generic algorithms, an expanded discussion of elliptic curves, semantic security of discrete logarithm cryptosystems and the Diffie-Hellman problems. There is no longer any discussion of knapsack cryptosystems or the *McEliece Cryptosystem* in this chapter.

• Chapter 7 deals with signature schemes. As before, it presents schemes such as the *Digital Signature Algorithm*, and it includes treatment of special types of signature schemes such as undeniable and fail-stop signature schemes. New material includes a careful discussion of security definitions, variants of the *ElGamal Signature Scheme* (such as the *Schnorr Signature Scheme* and the *Elliptic Curve Digital Signature Algorithm*) and provably secure signature schemes such as *Full Domain Hash*.

One of the most difficult things about writing any book in cryptography is deciding how much mathematical background to include. Cryptography is a broad subject, and it requires knowledge of several areas of mathematics, including number theory, groups, rings and fields, linear algebra, probability and information theory. As well, some familiarity with computational complexity, algorithms and NP-completeness theory is useful. In my opinion, it is the breadth of mathematical background required that often creates difficulty for students studying cryptography for the first time.

I tried not to assume too much mathematical background, and thus I developed mathematical tools as they are needed, for the most part. But it would certainly be helpful for the reader to have some familiarity with basic linear algebra and modular arithmetic. On the other hand, a more specialized topic, such as the concept of entropy from information theory, is introduced from scratch.

I apologize to anyone who does not agree with the phrase "Theory and Practice" in the title. I admit that the book is more theory than practice. What I mean by this phrase is that I have tried to select the material to be included in the book both on the basis of theoretical interest and practical importance. Therefore, I include systems that are not of practical use if they are mathematically elegant or illustrate an important concept or technique. But, on the other hand, I do present the most important systems that are used in practice, including several U.S. cryptographic standards.

Many people provided encouragement while I wrote this book, pointed out typos and errors in draft versions of this second edition, and gave me useful suggestions on new material to include and how various topics should be treated. In particular, I would like to thank Howard Heys, Alfred Menezes and Edlyn Teske.

Douglas R. Stinson
Waterloo, Ontario