

Preface to the Second Edition

As the field of cryptography expands to include new concepts and techniques, the cryptographic applications of number theory have also broadened. In addition to elementary and analytic number theory, increasing use has been made of algebraic number theory (primality testing with Gauss and Jacobi sums, cryptosystems based on quadratic fields, the number field sieve) and arithmetic algebraic geometry (elliptic curve factorization, cryptosystems based on elliptic and hyperelliptic curves, primality tests based on elliptic curves and abelian varieties). Some of the recent applications of number theory to cryptography — most notably, the number field sieve method for factoring large integers, which was developed since the appearance of the first edition — are beyond the scope of this book. However, by slightly increasing the size of the book, we were able to include some new topics that help convey more adequately the diversity of applications of number theory to this exciting multidisciplinary subject.

The following list summarizes the main changes in the second edition.

- Several corrections and clarifications have been made, and many references have been added.
- A new section on zero-knowledge proofs and oblivious transfer has been added to Chapter IV.
- A section on the quadratic sieve factoring method has been added to Chapter V.
- Chapter VI now includes a section on the use of elliptic curves for primality testing.
- Brief discussions of the following concepts have been added: k -threshold schemes, probabilistic encryption, hash functions, the Chor-Rivest knapsack cryptosystem, and the U.S. government's new Digital Signature Standard.

Seattle, May 1994