**Preface. Introduction.**   
Applications of number theory. An outline of this book.   
  
**Stream Ciphers.**   
Stream cipher systems. Additive synchronous stream ciphers. Nonadditive synchronous stream ciphers. Stream ciphering with block ciphers. Cooperative distributed ciphering. Some keystream generators. Generators based on counters. Some number-theoretic generators. Cryptographic aspects of sequences. Minimal polynominal and linear complexity. Pattern distribution of key streams. Correlation functions. Sphere complexity and linear cryptanalysis. Higher order complexities. Harmony on binary NSGs. Security attacks.   
  
**Primes, Primitive Roots and Sequences.**   
Cyclotomic polynominals. Two basic problems from stream ciphers. A basic theorem and main bridge. Primes, primitive roots and binary sequences. Primes, primitive roots and ternary sequences. Primes, negord and sequences. Prime powers, primitive roots and sequences. Prime products and sequences. Binary sequences and primes. Ternary sequences and primes. On cryptographic primitive roots. Linear complexity of sequences over *Zm*. Period and its cryptographic importance.   
  
**Cyclotomy and Cryptographic Functions.**   
Cyclotomic numbers. Cyclotomy and cryptography. Cyclotomy and difference parameters. Cyclotomy and the differential cryptanalysis. Cryptographic cyclotomic numbers. Cryptographic functions from *Zp*to *Zd*. The case *d* = 2. The case *d* = 3. The case *d* = 4. The case *d* = 5. The case *d*= 6. The case *d* = 8. The case *d* = 10. The case *d* = 12. Cryptographic functions from *Zpq*to *Zd*. Whiteman's generalized cyclotomy and cryptography. Cryptographic functions from *Zpq*to *Z2*. Cryptographic functions from *Zpq*to *Z4*. Cryptographic functions from *Zp2*to *Z2*. Cryptographic functions defined on *GF(pm)*. The origin of cyclotomic numbers.   
  
**Special Primes and Sequences.**   
Sophie Germain primes and sequences. Their importance in stream ciphers. Their relations with other number-theoretic problems. The existence problem. A search for cryptographic Sophie Germain primes. Tchebychef primes and sequences. Their cryptographic significance. Existence and search problem. Other primes of form *k* x 2n + 1 and sequences. Primes of form (*an*- 1)/(*a* - 1) and sequences. Mersenne primes and sequences. Cryptographic primes of form ((4*u*)*n*- 1)/(4*u* - 1). Prime repunits and their cryptographic values. *n*! ± 1 and *p#* ± 1 Primes and sequences. Twin primes and sequences over *GF*(2). The significance of twins and their sexes. Cryptographic twins and the sex distribution. Twin primes and sequences over *GF*(3). Other special primes and sequences. Prime distribution and their significance. Primes for stream ciphers and for RSA.   
  
**Difference Sets and Cryptographic Functions.**   
Rudiments of difference sets. Difference sets and autocorrelation functions. Differece sets and nonlinearity. Difference sets and information stability. Difference sets and linear approximation. Almost difference sets. Almost difference sets and autocorrelation functions. Almost difference sets, nonlinearity and approximation. Summary.   
  
**Difference Sets and Sequences.**   
The NSG realization of sequences. Differential analysis of sequences. Linear complexity of DSC (ADSC) sequences. Barker sequences.   
  
**Binary Cyclotomic Generators.**   
Cyclotomic generator of order 2k. Two-prime generator of order 2. Two-prime generator of order 4. Prime-square generator. Implementation and performance. A summary of binary cyclotomic generators.   
  
**Analysis of Cyclotomic Generators of Order 2.**   
Crosscorrelation property. Decimation property. Linear complexity. Security against a decision tree attack. Sums of DSC sequences. Linear complexity analysis. Balance analysis. Correlation analysis. Differential analysis.   
  
**Nonbinary Cyclotomic Generators.**  
The *r*th-order cyclotomic generator. Linear complexity. Autocorrelation property. Decimation property. Ideas behind the cyclotomic generators.   
  
**Generators Based on Permutations.**   
The cryptographic idea. Permutations on finite fields. A generator based on inverse permutations. Binary generators and permutations of *GF*(2*n*). APN permutations and their properties. Quadratic permutations with controllable nonlinearity. Permutations of order 3. APN permutations of order *n* - 1. Permutations of order *n* - 2. Permutations *Xd*with *d* = 2*m*- 1. APN permutations via crosscorrelation function. Other power functions with good nonlinearity. Choosing the linear functions. Cyclic-key generators and their problems. Cyclic-key generators. Several specific forms: An overview. A generator based on permutations of *Zm*.   
  
**Quadratic Partitions and Cryptography.**   
Quadratic partition and cryptography. *p* = *x2*+ *y2*and *p* = *x2*+ 4*y2*. *p* = *x2*+ *2y2*and *p* = *x2*+ 3*y2*. *p* = *x2*+ *ny2*and quadratic reciprocity. *p* = *x2*+ *7y2*and quadratic forms. *p* = *x2*+ *15y2*and genus theory. *p* = *x2*+ *ny2*and class field theory. Other cryptographic quadratic partitions.   
  
**Group Characters and Cryptography.**   
Group characters. Field characters and cryptography. Field multiplicative characters: most used ones. Field additive characters: most used ones. The nonlinearity of characters. The nonlinearity of multiplicative characters. The nonlinearity of additive characters. Ring characters and cryptography. Group characters and cyclotomic numbers.   
  
***P*-Adic Numbers, Class Numbers and Sequences.**   
The 2-adic value and 2-adic expansion. A fast algorithm for the 2-adic expansion. The arithmetric of*Q* [2] and *Z* [2]. Feedback shift registers with carry. Analysis and synthesis of FCRSs. The 2-adic span and 2-RA algorithm. Some properties of FCSR sequences. Blum-Blum-Shub sequences & class numbers.   
  
**Prime Ciphering Algorithms.**   
Prime-32: a description. Theoretical results about prime-32. Security arguments. Performing of prime-32. Prime-32 with a 192-bit key. Prime-64.   
  
**Cryptographic Problems and Philisophies.**   
Nonlinearity and linearity. Stability and instability. Stability and diffusion. Stability and local nonlinearities and differences. Correlation stability and pattern stability. Mutual information stability. Localness and globalness. Goodness and badness. About good plus good. About good plus bad. About Bad plus good. Hardware and software model complexity.   
  
**A. More About Cyclotomic Numbers.**   
Cyclotomic numbers of order 7. Cyclotomic numbers of order 9, 28. Cyclotomic numbers of order eleven. On other cyclotomic numbers. Behind cyclotomic numbers.   
  
**B. Cyclotomic Formulae of Order 6, 8 and 10. C. Finding Practical Primes. D. List of Research Problems. E. Exercises. F. List of Mathematical Symbols. Bibliography. Index.**