

## Contents

Preface	vii
Chapter 1. Introduction	1
Chapter 2. Caesar Cipher	3
Chapter 3. Terminology and Results from Number Theory	9
Chapter 4. Modular Arithmetic	17
Chapter 5. Describing the Caesar Cipher Mathematically	27
Chapter 6. Cryptanalysis for the Caesar Cipher	31
Chapter 7. Multiplication Cipher	37
Chapter 8. Cryptanalysis for the Multiplication Cipher	47
Chapter 9. Multiplication-Shift Cipher	51
Chapter 10. Cryptanalysis for the Multiplication-Shift Cipher	59
Chapter 11. Non-Mathematical Substitution Ciphers	69
Chapter 12. Preparing to Generalize	75
Chapter 13. Finding Inverses Modulo $n$	81
Chapter 14. General Multiplication-Shift Cipher	89
Chapter 15. Security of the General Multiplication-Shift Cipher	93
Chapter 16. Introduction to the Exponential Cipher	103
Chapter 17. Deciphering the Exponential Cipher	111
Chapter 18. Cryptanalysis for the Exponential Cipher	119
Chapter 19. Mathematical Basis for the Exponential Cipher	123
Chapter 20. Public Key Ciphers	127
Chapter 21. RSA Cipher	131

Chapter 22. Signatures	133
Chapter 23. Security and Implementation of the RSA Cipher	143
Chapter 24. Computer Programs	149
Chapter 25. Further Reading	151
Chapter 26. Answers to Selected Exercises	153
Index	157