
The Cryptoclub

Using Mathematics to Make and Break Secret Codes



Janet Beissinger
Vera Pless

Daria Tsoupikova, Artist



A K Peters
Wellesley, Massachusetts

Contents

Foreword	ix
Preface	xi
Acknowledgments	xiv

Unit 1 Introduction to Cryptography

Chapter 1 Caesar Ciphers	2
DO YOU KNOW? Little Orphan Annie and Captain Midnight	7
Chapter 2 Sending Messages with Numbers	8
DO YOU KNOW? Beale Ciphers and a Buried Treasure	18
Chapter 3 Breaking Caesar Ciphers	20
DO YOU KNOW? Navajo Code Talkers	26

Unit 2 Substitution Ciphers

Chapter 4 Keyword Ciphers	28
DO YOU KNOW? Dancing Men	33
Chapter 5 Letter Frequencies	34
DO YOU KNOW? Edgar Allen Poe Challenges	39

Chapter 6	Breaking Substitution Ciphers	40
	DO YOU KNOW? Poor Mary	50

Unit 3 Vigenère Ciphers

Chapter 7	Combining Caesar Ciphers	52
	DO YOU KNOW? The Civil War	61
Chapter 8	Cracking Vigenère Ciphers When You Know the Key Length	62
	DO YOU KNOW? Lewis and Clark	73
Chapter 9	Factoring	74
	DO YOU KNOW? Cicadas	83
Chapter 10	Using Common Factors to Crack Vigenère Ciphers	84
	DO YOU KNOW? The One-Time-Pad and Atomic Spies	98

Unit 4 Modular (Clock) Arithmetic

Chapter 11	Introduction to Modular Arithmetic	102
	DO YOU KNOW? How the United States Entered World War I	112
Chapter 12	Applications of Modular Arithmetic	114
	DO YOU KNOW? Non-Secret Codes	121

Unit 5 Multiplicative and Affine Ciphers

Chapter 13	Multiplicative Ciphers	124
	DO YOU KNOW? Passwords	131
Chapter 14	Using Inverses to Decrypt	132
	DO YOU KNOW? The German Enigma Cipher	142
Chapter 15	Affine Ciphers	144
	DO YOU KNOW? Atbash	152

Unit 6 Math for Modern Cryptography

Chapter 16	Finding Prime Numbers	154
	DO YOU KNOW? The Great Internet Mersenne Prime Search	165
Chapter 17	Raising to Powers	166
	DO YOU KNOW? Dead Men Can't Tell Passwords	172

Unit 7 Public Key Cryptography

Chapter 18	The RSA Cryptosystem	174
	DO YOU KNOW? Modern Uses of Cryptography	181
Chapter 19	Revisiting Inverses in Modular Arithmetic	182
	DO YOU KNOW? Jefferson and Madison: But Where Is the Key?	187
Chapter 20	Sending RSA Messages	188
	DO YOU KNOW? The British Public Key Ciphers	193
	Index	195
	Make Your Own Cipher Wheel	199