

q t g x a n w c j o i v z p h y b
f s w z m v b i n h u y o g x a c
i p y l u a h m g t x n f w z b v
u x k t z g l f s w m e v y a o h
w j s y f k e r v l d u x z n g q
i r x e j d q u k c t w y m f p n
q s COMPUTER v x l b d i f
v c h b o s i a r u w k d n l e x
f z m SECURITY l j AND w
b g a n r h z q t v j c m k d w e
x u CRYPTOGRAPHY l v f
k o e w n q s g z j h a t b u f i
n d v m p r f y i g z s a t e h u
c u l o q e x h f y r z s d g t k
t k n p d w g e x q y r c f s j m
j c ALAN d G. p KONHEIM y
l n b u e c v o w p a d q h k x g

CONTENTS

<i>FOREWORD</i>	ix	3.4 The χ^2 -Test of a Hypothesis	67
<i>PREFACE</i>	xi	3.5 Pruning from the Table of Isomorphs	68
<i>ABOUT THE AUTHOR</i>	xvii	3.6 Partial Maximum Likelihood Estimation of a Monoalphabetic Substitution	73
		3.7 The Hidden Markov Model (HMM)	78
		3.8 Hill Encipherment of ASCII <i>N</i> -Grams	90
		3.9 Gaussian Elimination	102
		3.10 Monoalphabetic Substitution Problems	111
CHAPTER 1 <i>APERITIFS</i>		CHAPTER 4 <i>POLYALPHABETIC SUBSTITUTION</i>	
1.1 The Lexicon of Cryptography	1	4.1 Running Keys	116
1.2 Cryptographic Systems	4	4.2 Blaise de Vigenère	117
1.3 Cryptanalysis	4	4.3 Gilbert S. Vernam	117
1.4 Side Information	6	4.4 The One-Time Pad	119
1.5 Thomas Jefferson and the M-94	6	4.5 Finding the Key of Vernam–Vigenère Ciphertext with Known Period by Correlation	120
1.6 Cryptography and History	7	4.6 Coincidence	124
1.7 Cryptography and Computers	8	4.7 Venona	127
1.8 The National Security Agency	9	4.8 Polyalphabetic Substitution Problems	132
1.9 The Giants	10		
1.10 No Sex, Money, Crime or . . . Love	12	CHAPTER 5 <i>STATISTICAL TESTS</i>	
1.11 An Example of the Inference Process in Cryptanalysis	13	5.1 Weaknesses in a Cryptosystem	136
1.12 Warning!	15	5.2 The Kolmogorov–Smirnov Test	136
		5.3 NIST's Proposed Statistical Tests	138
		5.4 Diagnosis	139
		5.5 Statistical Tests Problems	143
CHAPTER 2 <i>COLUMNAR TRANSPOSITION</i>		CHAPTER 6 <i>THE EMERGENCE OF CIPHER MACHINES</i>	
2.1 Shannon's Classification of Secrecy Transformations	18	6.1 The Rotor	150
2.2 The Rules of Columnar Transposition Encipherment	18	6.2 Rotor Systems	152
2.3 Cribbing	21	6.3 Rotor Patents	153
2.4 Examples of Cribbing	25	6.4 A Characteristic Property of Conjugacy	155
2.5 Plaintext Language Models	30	6.5 Analysis of a 1-Rotor System: Ciphertext Only	156
2.6 Counting <i>k</i> -Grams	33	6.6 The Displacement Sequence of a Permutation	158
2.7 Deriving the Parameters of a Markov Model from Sliding Window Counts	34	6.7 Arthur Scherbius	160
2.8 Markov Scoring	34		
2.9 The ADFGVX Transposition System	47		
2.10 CODA	49		
2.11 Columnar Transposition Problems	50		
CHAPTER 3 <i>MONOALPHABETIC SUBSTITUTION</i>			
3.1 Monoalphabetic Substitution	63		
3.2 Caesar's Cipher	65		
3.3 Cribbing Using Isomorphs	66		

6.8	Enigma Key Distribution Protocol	163	9.7	Is DES a Random Mapping?	297
6.9	Cryptanalysis of the Enigma	166	9.8	DES in the Output-Feedback Mode (OFB)	299
6.10	Cribbing Enigma Ciphertext	167	9.9	Cryptanalysis of DES	300
6.11	The Lorenz Schlüsselzusatz	170	9.10	Differential Cryptanalysis	302
6.12	The SZ40 Pin Wheels	171	9.11	The EFS DES-Cracker	308
6.13	SZ40 Cryptanalysis Problems	175	9.12	What Now?	311
6.14	Cribbing SZ40 Ciphertext	176	9.13	The Future Advanced Data Encryption Standard	312
CHAPTER 7 THE JAPANESE CIPHER MACHINES			9.14	And the Winner Is!	312
7.1	Japanese Signaling Conventions	191	9.15	The Rijndael Operations	314
7.2	Half-Rotors	191	9.16	The Rijndael Cipher	323
7.3	Components of the RED Machine	193	9.17	Rijndael's Strength: Propagation of Patterns	323
7.4	Cribbing RED Ciphertext	200	9.18	When is a Product Block-Cipher Secure?	326
7.5	Generalized Vowels and Consonants	209	9.19	Generating the Symmetric Group	327
7.6	"Climb Mount Itaka" – War!	210	9.20	A Class of Block Ciphers	329
7.7	Components of the PURPLE Machine	211	9.21	The IDEA Block Cipher	332
7.8	The PURPLE Keys	217	CHAPTER 10 THE PARADIGM OF PUBLIC KEY CRYPTOGRAPHY		
7.9	Cribbing PURPLE: Finding the V-Stepper	219	10.1	In the Beginning. . .	334
7.10	Cribbing PURPLE: Finding the C-Steppers	238	10.2	Key Distribution	335
CHAPTER 8 STREAM CIPHERS			10.3	E-Commerce	336
8.1	Stream Ciphers	244	10.4	Public-Key Cryptosystems: Easy and Hard Computational Problems	337
8.2	Feedback Shift Registers	244	10.5	Do PKCs Solve the Problem of Key Distribution?	341
8.3	The Algebra of Polynomials over $\mathbb{Z}_2$	247	10.6	P.S.	342
8.4	The Characteristic Polynomial of a Linear Feedback Shift Register	251	CHAPTER 11 THE KNAPSACK CRYPTOSYSTEM		
8.5	Properties of Maximal Length LFSR Sequences	254	11.1	Subset Sum and Knapsack Problems	344
8.6	Linear Equivalence	258	11.2	Modular Arithmetic and the Euclidean Algorithm	346
8.7	Combining Multiple Linear Feedback Shift Registers	259	11.3	A Modular Arithmetic Knapsack Problem	350
8.8	Matrix Representation of the LFSR	260	11.4	Trap-Door Knapsacks	350
8.9	Cribbing of Stream Enciphered ASCII Plaintext	261	11.5	Knapsack Encipherment and Decipherment of ASCII-Plaintext	355
8.10	Nonlinear Feedback Shift Registers	271	11.6	Cryptanalysis of the Merkle–Hellman Knapsack System (Modular Mapping)	358
8.11	Nonlinear Key Stream Generation	273	11.7	Diophantine Approximation	364
8.12	Irregular Clocking	275	11.8	Short Vectors in a Lattice	368
8.13	RC4	278	11.9	Knapsack-Like Cryptosystems	37
8.14	Stream Encipherment Problems	281	11.10	Knapsack Cryptosystem Problems	37
CHAPTER 9 BLOCK-CIPHERS: LUCIFER, DES, AND AES			CHAPTER 12 THE RSA CRYPTOSYSTEM		
9.1	LUCIFER	283	12.1	A Short Number-Theoretic Digression	376
9.2	DES	288	12.2	RSA	378
9.3	The DES S-Boxes, P-Box, and Initial Permutation (IP)	289	12.3	The RSA Encipherment and Decipherment of ASCII-Plaintext	379
9.4	DES Key Schedule	292			
9.5	Sample DES Encipherment	294			
9.6	Chaining	295			

12.4	Attack on RSA	382	15.10	The Elliptic Curve Digital Signature Algorithm	444
12.5	Williams Variation of RSA	383	15.11	The Certicom Challenge	445
12.6	Multiprecision Modular Arithmetic	387	15.12	NSA and Elliptic Curve Cryptography	445
CHAPTER 13 PRIME NUMBERS AND FACTORIZATION			CHAPTER 16 KEY EXCHANGE IN A NETWORK		
13.1	Number Theory and Cryptography	390	16.1	Key Distribution in a Network	447
13.2	Prime Numbers and the Sieve of Eratosthenes	390	16.2	U.S. Patent '770	448
13.3	Pollard's $p - 1$ Method	391	16.3	Spoofing	448
13.4	Pollard's ρ -Algorithm	394	16.4	El Gamal's Extension of Diffie-Hellman	450
13.5	Quadratic Residues	396	16.5	Shamir's Autonomous Key Exchange	451
13.6	Random Factorization	401	16.6	X9.17 Key Exchange Architecture	453
13.7	The Quadratic Sieve (QS)	403	16.7	The Needham-Schroeder Key Distribution Protocol	456
13.8	Testing if an Integer is a Prime	405			
13.9	The RSA Challenge	407			
13.10	Perfect Numbers and the Mersenne Primes	408	CHAPTER 17 DIGITAL SIGNATURES AND AUTHENTICATION		
13.11	Multiprecision Arithmetic	409	17.1	The Need for Signatures	464
13.12	Prime Number Testing and Factorization Problems	410	17.2	Threats to Network Transactions	465
CHAPTER 14 THE DISCRETE LOGARITHM PROBLEM			17.3	Secrecy, Digital Signatures, and Authentication	465
14.1	The Discrete Logarithm Problem Modulo p	414	17.4	The Desiderata of a Digital Signature	466
14.2	Solution of the DLP Modulo p Given a Factorization of $p - 1$	415	17.5	Public-Key Cryptography and Signature Systems	467
14.3	Adelman's Subexponential Algorithm for the Discrete Logarithm Problem	419	17.6	Rabin's Quadratic Residue Signature Protocol	468
14.4	The Baby-Step, Giant-Step Algorithm	420	17.7	Hash Functions	470
14.5	The Index-Calculus Method	420	17.8	MD5	471
14.6	Pollard's ρ -Algorithm	424	17.9	The Secure Hash Algorithm	473
14.7	Extension Fields	426	17.10	NIST's Digital Signature Algorithm	474
14.8	The Current State of Discrete Logarithm Research	428	17.11	El Gamal's Signature Protocol	475
			17.12	The Fiat-Shamir Identification and Signature Schema	476
			17.13	The Oblivious Transfer	478
CHAPTER 15 ELLIPTIC CURVE CRYPTOGRAPHY			CHAPTER 18 APPLICATIONS OF CRYPTOGRAPHY		
15.1	Elliptic Curves	429	18.1	UNIX Password Encipherment	480
15.2	The Elliptic Group over the Reals	431	18.2	Magnetic Stripe Technology	482
15.3	Lenstra's Factorization Algorithm	432	18.3	Protecting ATM Transactions	484
15.4	The Elliptic Group over $\mathbb{Z}_p$ ($p > 3$)	434	18.4	Keyed-Access Cards	491
15.5	Elliptic Groups over the Field $\mathbb{Z}_{m,2}$	436	18.5	Smart Cards	491
15.6	Computations in the Elliptic Group $\mathcal{E}_{\mathbb{Z}_{m,2}}(a, b)$	438	18.6	Who Can You Trust?: Kohnfelder's Certificates	495
15.7	Supersingular Elliptic Curves	441	18.7	X.509 Certificates	495
15.8	Diffie-Hellman Key Exchange Using an Elliptic Curve	442	18.8	The Secure Socket Layer (SSL)	497
15.9	The Menezes-Vanstone Elliptic Curve Cryptosystem	443	18.9	Making a Secure Credit Card Payment on the Web	502

CHAPTER 19 *CRYPTOGRAPHIC
PATENTS*

19.1	What is a Patent?	506	19.7	U.S. Patent 3,543,904	509
19.2	Patentability of Ideas	507	19.8	U.S. Patent 4,200,770	511
19.3	The Format of a Patent	507	19.9	U.S. Patent 4,218,582	512
19.4	Patentable versus Nonpatentable Subjects	508	19.10	U.S. Patent 4,405,829	512
19.5	Infringement	509	19.11	PKS/RSADSI Litigation	514
19.6	The Role of Patents in Cryptography	509	19.12	Leon Stambler	514
			<i>INDEX</i>		516