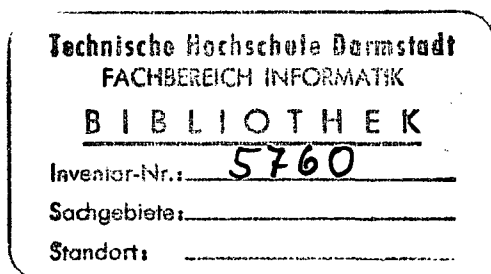


# Cryptography

## A Primer

ALAN G. KONHEIM  
*Mathematical Sciences Department*  
*IBM Thomas J. Watson Research Center*



A Wiley-Interscience Publication

JOHN WILEY & SONS

New York • Chichester • Brisbane • Toronto • Singapore

# Contents

## Part I Foundations of Cryptography

### CHAPTER

1	INTRODUCTION	3
1.1	The Problem	4
1.2	Nomenclature	6
1.3	The Ground Rules of Cryptanalysis	7
1.4	Side Information	9
1.5	The Tools of Cryptanalysis	10

### CHAPTER

2	SECRECY SYSTEMS	11
2.1	Introduction	11
2.2	Alphabets	11
2.3	The Plaintext Source	14
2.4	Cryptographic Systems	27
2.5	Cryptanalysis by the Bayesian Opponent	31
2.6	The Bayesian Decision as $n \rightarrow \infty$	38
2.7	Perfect Secrecy	42
2.8	Entropy	44
2.9	The Plaintext Source Entropy	51
2.10	The Variation of Equivocation with the Length of Intercepted Ciphertext	53
2.11	Random Cryptographic Systems	55
2.12	The Unicity Distance	61
	Problems	62

## CHAPTER

3	MONALPHABETIC SUBSTITUTION	64
3.1	Permutations of $n$ -Grams	64
3.2	Letter Substitutions	65
3.3	Substitution Systems	66
3.4	Examples of Plaintext	67
3.5	Caesar Substitution	69
3.6	Analysis of Caesar Substitution—I	72
3.7	The Operational Procedure	76
3.8	Analysis of Caesar Substitution—II	79
3.9	Mixed Standard Alphabets	83
3.10	Affine Caesar Substitution	90
3.11	General Monalphabetic Substitution	91
3.12	Two-Gram Substitutions: Playfair Encipherment	95
3.13	Cryptanalysis of <i>CIPHER(2.2)</i>	101
3.14	$N$ -Gram Substitution: Linear Algebra Over $\mathbf{Z}_m$	110
3.15	$N$ -Gram Substitution: Hill Encipherment	115
3.16	Cryptanalysis of Hill Encipherment with Chosen Plaintext	116
3.17	Cryptanalysis of Hill Substitution with Corresponding Plaintext and Ciphertext	116
	Problems	120

## CHAPTER

4	POLYALPHABETIC SYSTEMS	135
4.1	The One-Time System	135
4.2	Vigenère Encipherment	137
4.3	Analysis of the Vigenère System if the Period $r$ Is Known	139
4.4	Generalized Vigenère Encipherment	141
4.5	The Phi Test	143
4.6	The Phi Reference Value for Monalphabetic Substitution	146
4.7	The Phi Reference Value for Polyalphabetic Substitution	150
4.8	Using $\phi$ to Estimate the Period $r$	154
4.9	The Incidence of Coincidence	158
4.10	Using $\kappa$ to Estimate the Period of a Polyalphabetic Substitution	161
4.11	Key Expansion	163
4.12	Key Differencing	165
4.13	The Cryptanalysis of <i>CIPHER(1.4)</i>	170
4.14	Differences of Differenced Keys	172

4.15	The Cryptanalysis of Multiloop Vigenère with Unknown Periods .....	182
4.16	Coda .....	183
	Problems .....	184

## CHAPTER

5	ROTOR SYSTEMS .....	190
5.1	Rotors .....	190
5.2	Rotational Equivalence .....	194
5.3	Cryptanalysis with Corresponding Plaintext and Ciphertext .....	199
5.4	Cryptanalysis with Ciphertext Only: $N = 1$ .....	205
5.5	Cryptanalysis with Ciphertext Only: $N = 2$ .....	211
5.6	The Enigma Machine .....	212
5.7	Properties of Enigma Encipherment .....	214
5.8	Cryptanalysis of the Enigma with Corresponding Plaintext and Ciphertext .....	215
5.9	The Plugboard .....	222
	Problems .....	223

## CHAPTER

6	BLOCK CIPHERS AND THE DATA ENCRYPTION STANDARD .....	228
6.1	Block Ciphers .....	228
6.2	Building Blocks of Block Ciphers .....	229
6.3	What Does Corresponding Plaintext and Ciphertext Reveal About $\pi$ ? .....	230
6.4	Block Cipher Systems .....	231
6.5	Generating $\text{SYM}(\mathbb{Z}_{2,N})$ .....	233
6.6	Involutions .....	236
6.7	DES .....	240
6.8	Preliminary Assessment of DES .....	248
6.9	The Criticism of DES .....	248
6.10	The S- and P-Box Design Criteria .....	248
6.11	The Number of Iterations .....	249
6.12	The Key Length .....	249
6.13	Cryptanalysis of DES: The Ground Rules .....	250
6.14	Cycle Length .....	250
6.15	Correlation Between Output and Input Subblocks .....	251
6.16	The $\chi^2$ -Test .....	251
6.17	The Kolmogorov-Smirnov Test .....	254

6.18	Applying the $\chi^2$ -Test to Detect Dependence Between Output and Input	256
6.19	The Avalanche Effect	262
6.20	Dependence of Output on Input	262
6.21	Boolean Representation of DES	263
6.22	Power Systems	266
6.23	Time-Memory Trade-off	267
6.24	Chaining	269
6.25	Step Encipherment	276
6.26	Stream Encipherment	278
	Problems	279

## Part II Applications of Cryptography

### CHAPTER

7	KEY MANAGEMENT	285
7.1	Communications Security/File Security	285
7.2	Current Applications of Cryptography	285
7.3	Key Management in an Information Processing System	288
7.4	Session Keys	288
7.5	Discussion and Critique	292
7.6	The Midnight Attack	293
	Problems	293

### CHAPTER

8	PUBLIC KEY SYSTEMS	294
8.1	Why Public Key Systems?	294
8.2	Complexity Theory	294
8.3	Trap Door and One-Way Functions	296
8.4	A Public Key System Based on the Logarithm Problem	298
8.5	Adelman's Analysis of the Logarithm Problem	300
8.6	A Public Key System Based on the Knapsack Problem	303
8.7	Critique of the Knapsack Problem as the Basis for a Public Key System	307
8.8	Best Rational Approximations to $\vartheta$	308
8.9	Review of Some Number Theory	315
8.10	The Rivest-Shamir-Adelman Encipherment System [R11]	319

8.11	Critique and Discussion of the Rivest-Shamir-Adelman Public Key System . . . . .	320
8.12	Berlekamp's Solution of $y^2 = \alpha$ (modulo $p$ ) . . . . .	322
8.13	Solution of $y^2 - \alpha = 0$ (modulo $m$ ), where $m = pq$ with $p, q$ Known Primes . . . . .	324
8.14	Rabin's Equivalence Theorem . . . . .	324
8.15	The Pitfalls of Complexity Theory in Cryptography . . . . .	326
	Problems . . . . .	329

## CHAPTER

9	DIGITAL SIGNATURES AND AUTHENTICATIONS . . . . .	331
9.1	The Problem . . . . .	331
9.2	The Threats . . . . .	332
9.3	What Does Transaction Verification Require? . . . . .	332
9.4	Authentication . . . . .	333
9.5	Examples of Signatures . . . . .	334
9.6	Handshaking . . . . .	334
9.7	The Transaction . . . . .	334
9.8	Assumptions . . . . .	336
9.9	Disputes . . . . .	336
9.10	Settling a Dispute . . . . .	337
9.11	The Rivest-Shamir-Adelman Signature System [RI1] . . . . .	338
9.12	The Quadratic Residue Signature Scheme . . . . .	338
9.13	The Trusted Authority . . . . .	339
9.14	Hardware Assumptions . . . . .	341
9.15	The Transaction . . . . .	341
9.16	Threat Analysis . . . . .	344
9.17	Cryptography Without Secrecy . . . . .	345
	Problems . . . . .	346

## CHAPTER

10	FILE SECURITY . . . . .	348
10.1	The Problem . . . . .	348
10.2	The Design Philosophy of IPS . . . . .	349
10.3	Augmentation of DES by Chaining/Key Crunching . . . . .	351
10.4	Key Selection and Key Crunching . . . . .	352
10.5	Components of IPS . . . . .	353
10.6	IPS and the IBM Cryptographic Products . . . . .	360
10.7	Summary . . . . .	362

REFERENCES	365
APPENDIX	
P    PROBABILITY THEORY	371
P.1    Chance Experiments and Their Sample Spaces	372
P.2    Probability Distributions	373
P.3    Events	374
P.4    Random Variables	375
P.5    Distribution Functions	376
P.6    Moments	377
P.7    Examples of Probability Distributions	378
P.8    Independence	379
P.9    Conditional Probability and Dependence	381
P.10   Chebyshev's Inequality	382
P.11   Limit Theorems: The Laws of Large Numbers	382
P.12   Limit Theorems: The Poisson Approximation to the Binomial Distribution	383
P.13   Limit Theorems: The Central Limit Theorem	383
P.14   Generating Functions	383
APPENDIX	
V    THE VARIANCE OF $\Phi$	385
SOLUTIONS TO SELECTED PROBLEMS	395
INDEX	427