
FUNDAMENTALS OF CRYPTOLOGY

*A Professional Reference
and Interactive Tutorial*

by

Henk C.A. van Tilborg
*Eindhoven University of Technology
The Netherlands*



KLUWER ACADEMIC PUBLISHERS
Boston/Dordrecht/London

Contents

	Preface	xiii
1	Introduction	1
1.1	Introduction and Terminology	1
1.2	Shannon's Description of a Conventional Cryptosystem	2
1.3	Statistical Description of a Plaintext Source	4
1.4	Problems	7
2	Classical Cryptosystems	9
2.1	Caesar, Simple Substitution, Vigenère	9
2.1.1	Caesar Cipher	9
2.1.2	Simple Substitution	10
	The System and its Main Weakness	10
	Cryptanalysis by The Method of a Probable Word	11
2.1.3	Vigenère Cryptosystem	13
2.2	The Incidence of Coincidences, Kasiski's Method	16
2.2.1	The Incidence of Coincidences	16
2.2.2	Kasiski's Method	19
2.3	Vernam, Playfair, Transpositions, Hagelin, Enigma	20
2.3.1	The One-Time Pad	20
2.3.2	The Playfair Cipher	20
2.3.3	Transposition Ciphers	21
2.3.4	Hagelin	22
2.3.5	Enigma	24
2.4	Problems	25
3	Shift Register Sequences	27
3.1	Pseudo-Random Sequences	27
3.2	Linear Feedback Shift Registers	31
3.2.1	(Linear) Feedback Shift Registers	31
3.2.2	PN-Sequences	35
3.2.3	Which Characteristic Polynomials give PN-Sequences?	38
3.2.4	An Alternative Description of $\Omega(f)$ for Irreducible f	44
3.2.5	Cryptographic Properties of PN Sequences	46
3.3	Non-Linear Algorithms	49
3.3.1	Minimal Characteristic Polynomial	49
3.3.2	The Berlekamp-Massey Algorithm	52
3.3.3	A Few Observations about Non-Linear Algorithms	58

3.4	Problems	60
4	Block Ciphers	63
4.1	Some General Principles	63
4.1.1	Some Block Cipher Modes	63
	Codebook Mode	63
	Cipher Block Chaining	64
	Cipher Feedback Mode	65
4.1.2	An Identity Verification Protocol	66
4.2	DES	67
	DES	67
	Triple DES	69
4.3	IDEA	70
4.4	Further Remarks	72
4.5	Problems	73
5	Shannon Theory	75
5.1	Entropy, Redundancy, and Unicity Distance	75
5.2	Mutual Information and Unconditionally Secure Systems	80
5.3	Problems	85
6	Data Compression Techniques	87
6.1	Basic Concepts of Source Coding for Stationary Sources	87
6.2	Huffman Codes	92
6.3	Universal Data Compression - The Lempel-Ziv Algorithms	97
	Initialization	98
	Encoding	99
	Decoding	101
6.4	Problems	103
7	Public-Key Cryptography	105
7.1	The Theoretical Model	105
7.1.1	Motivation and Set-up	105
7.1.2	Confidentiality	106
7.1.3	Digital Signature	107
7.1.4	Confidentiality and Digital Signature	108
7.2	Problems	109
8	Discrete Logarithm Based Systems	111
8.1	The Discrete Logarithm System	111
8.1.1	The Discrete Logarithm Problem	111
8.1.2	The Diffie-Hellman Key Exchange System	114
8.2	Other Discrete Logarithm Based Systems	116
8.2.1	ElGamal's Public-Key Cryptosystems	116

	Setting It Up	116
	ElGamal's Secrecy System	116
	ElGamal's Signature Scheme	117
8.2.2	Further Variations	119
	Digital Signature Standard	119
	Schnorr's Signature Scheme	120
	The Nyberg-Rueppel Signature Scheme	120
8.3	How to Take Discrete Logarithms	120
8.3.1	The Pohlig-Hellman Algorithm	121
	Special Case: $q - 1 = 2^n$	121
	General Case: $q - 1$ has only small prime factors	123
	An Example of the Pohlig-Hellman Algorithm	124
8.3.2	The Baby-Step Giant-Step Method	127
8.3.3	The Pollard- ρ Method	130
8.3.4	The Index-Calculus Method	135
	General Discussion	135
	\mathbb{Z}_p^* , i.e. the Multiplicative Group of $\text{GF}(p)$	136
	$\text{GF}(2^n)$	141
8.4	Problems	145
9	RSA Based Systems	147
9.1	The RSA System	147
9.1.1	Some Mathematics	147
9.1.2	Setting Up the System	148
	Step 1 Computing the Modulus n_U	148
	Step 2 Computing the Exponents e_U and d_U	149
	Step 3 Making Public: e_U and n_U	150
9.1.3	RSA for Privacy	150
9.1.4	RSA for Signatures	153
9.1.5	RSA for Privacy and Signing	154
9.2	The Security of RSA: Some Factorization Algorithms	156
9.2.1	What the Cryptanalyst Can Do	156
9.2.2	A Factorization Algorithm for a Special Class of Integers	158
	Pollard's $p - 1$ Method	158
9.2.3	General Factorization Algorithms	161
	The Pollard- ρ Method	161
	Random Square Factoring Methods	162
	Quadratic Sieve	167
9.3	Some Unsafe Modes for RSA	169
9.3.1	A Small Public Exponent	169
	Sending the Same Message to More Receivers ...	169
	Sending Related Messages to a Receiver with Small Public Exponent	171

[Click here to download full PDF material](#)