

Contents

1	An Introduction to Classical and Modern Cryptography	1
1.1	Overview	1
1.2	Introduction to Cryptography	4
1.3	Cryptography Terminologies	5
1.4	Goals of Cryptography	8
1.4.1	Data Confidentiality	8
1.4.2	Data Integrity	12
1.4.3	Authentication	17
1.5	Analysis Criteria of Cryptography Algorithms	21
1.6	Classical Cryptography	23
1.6.1	Substitution Algorithms	25
1.6.2	Transposition Algorithms	36
1.7	Symmetric Key Algorithms	36
1.8	Asymmetric Key Algorithms	38
1.9	Common Attacks in Cryptography	40
1.10	The Basic Principles of Modern Cryptography	42
1.10.1	Principle 1 – Formulation of Exact Definitions	43
1.10.2	Principle 2 – Reliance on Precise Assumptions	44
1.10.3	Principle 3 – Rigorous Proofs of Security	45
	Bibliography	46
2	Security Standards for Classical and Modern Cryptography	47
2.1	Overview	47
2.2	Data Encryption Standard (DES)	47
2.2.1	Feistel Structure	48
2.2.2	How Does DES Work?	51
2.2.3	Triple DES	56
2.2.4	Simplified Data Encryption Standard (S-DES)	56
2.2.5	The Switch Function	61
2.3	Modes of Operation	61
2.3.1	Electronic Code Book Mode	62

2.3.2	Cipher Block Chaining Mode	64
2.3.3	Cipher Feedback Mode	65
2.3.4	Output Feedback Mode	67
2.3.5	Counter Mode	67
2.4	Stream Cipher	70
2.5	Advanced Encryption Standard (AES)	72
2.5.1	High-Level Description of the AES Encryption	73
2.5.2	Sub-Bytes	73
2.5.3	Shift Rows	74
2.5.4	Mix-Columns	74
2.5.5	Add Round Key	76
2.5.6	AES Key Schedule	76
2.5.7	AES Decryption	77
2.5.8	Cryptanalysis of AES	78
2.6	Pseudo Random Number Generator (PRNG)	80
2.7	LFRS Based Stream Cipher	81
	Bibliography	82
3	Mathematical Foundation for Classical and Modern	
	Cryptography	85
3.1	Overview	85
3.2	Modular Arithmetic	86
3.2.1	Quotient Remainder Theorem	86
3.2.2	Modular Addition	86
3.2.3	Modular Multiplication	87
3.2.4	Modular Division	87
3.2.5	Modular Inverse	88
3.2.6	Modular Exponentiation	88
3.2.7	Congruence	88
3.2.8	Application of Modular Arithmetic	90
3.2.9	Computational Complexity	92
3.3	Groups	92
3.3.1	Abelian Groups	93
3.3.2	Cyclic Groups	93
3.3.3	Rings	93
3.3.4	Fields	94
3.4	Finite Fields	95
3.4.1	Types of Finite Fields	96
3.4.2	Applications	98
3.5	Elliptic Curves	99
3.5.1	Elliptic Curve over the Real Numbers	101
3.5.2	Elliptic Curves over the Rational Numbers	101
3.5.3	Elliptic Curves over Finite Fields	101
3.5.4	Algorithms that Use Elliptic Curves	102
3.6	Elliptic Curve Cryptography	102

3.6.1	Elliptic Curve Cryptography Implementation	104
3.6.2	Elliptic Curve Cryptography Applications.	106
3.6.3	Security	106
	Bibliography	107
4	Asymmetric Key Cryptography	109
4.1	Overview	109
4.2	Introduction to Asymmetric Key Cryptography	110
4.3	Applications	112
4.4	Hybrid Cryptosystems	113
4.5	Public Key Infrastructure	113
4.6	Weaknesses of Asymmetric Key Cryptography.	116
4.6.1	Algorithms	117
4.6.2	Alteration of Public Keys.	117
4.6.3	Public Key Infrastructure	118
4.7	Asymmetric Key Techniques	119
4.7.1	RSA	119
4.7.2	RC4	126
4.7.3	ElGamal	128
4.7.4	Digital Signature Algorithm.	130
4.7.5	Diffie-Hellman Key Exchange Protocol	134
4.7.6	Password-Authenticated Key Agreement	141
4.8	Examples of Protocols Using Asymmetric Key Algorithms	
	Include	142
4.8.1	S/Mime.	142
4.8.2	PGP	145
4.8.3	IPSec	147
4.8.4	Secure Shell (SSH)	150
4.8.5	Transport Layer Security (TLS) and its Predecessor	
	Secure Socket Layer (SSL)	154
	Bibliography	165
5	Modern Cryptanalysis Methods, Advanced Network Attacks	
	and Cloud Security	167
5.1	Overview	167
5.1.1	Cryptanalysis	168
5.2	Types of Cryptanalysis Systems	169
5.2.1	Linear Cryptanalysis	169
5.2.2	Differential Cryptanalysis	171
5.3	Difference Between Linear and Differential Cryptanalysis.	172
5.4	Types of Cryptanalytic Attacks	173
5.5	Network Security: Common and Advanced Network Attacks.	178
5.5.1	Reconnaissance Attacks.	184
5.5.2	Access Attacks	184
5.5.3	Social Engineering Attack	186
5.5.4	DoS Attack and DDoS Attack	188

5.5.5	Common IPv4 and IPv6 Attacks	189
5.5.6	TCP and UDP Vulnerabilities	195
5.5.7	IP Services Vulnerabilities	200
5.5.8	DNS Attacks.	201
5.6	Cloud Security	206
5.7	Introduction to Blockchain and Bitcoin.	212
5.7.1	Blockchain	212
5.7.2	Bitcoin	213
	Bibliography	214