

Chapter 1: Prime Position Orientations of Bits (PPO)	1
1.1 Introduction	1
1.2 Cryptanalysis	4
1.3 Security of algorithms	6
1.4 Classical cryptosystems	7
1.4.1 Substitution ciphers	8
1.4.2 Transposition ciphers	9
1.4.3 Product ciphers	9
1.5 Few popular algorithms	9
1.5.1 Caesar cipher	10
1.5.2 Rail Fence cipher	10
1.5.3 Vigenère cipher	11
1.5.4 One-Time Pad	12
1.5.5 Rotor Machines	13
1.5.6 Data Encryption Standard (DES)	13
1.5.7 RSA	14
1.6 Confusion and diffusion	15
1.7 Block cipher modes of operation	16
1.7.1 Electronic Code Book (ECB) mode	17
1.7.2 Cipher Block Chaining (CBC) mode	17
1.7.3 Cipher Feed-back (CFB) mode	19
1.7.4 Output Feed-back (OFB) mode	20
1.8 Proposal of the thesis	21
1.8.1 Embedded systems	22
1.8.2 Proposed algorithms	24
1.8.2.1 Prime Position Orientations (PPO)	26
1.8.2.2 Block Exchange Technique (BET)	26
1.8.2.3 Selective Positional Orientation of Bits (SPOB)	27
1.8.2.4 Modulo-Arithmetic Technique (MAT)	27
1.8.2.5 Overlapped Modulo-Arithmetic Technique (OMAT)	27
1.8.2.6 Modified Modulo-Arithmetic Technique (MMAT)	28
1.8.2.7 Bit-pair Operation and Separation (BOS)	28
1.8.2.8 Decimal Equivalent Positional Substitution (DEPS)	28
1.8.3 Methods of evaluation	29
1.8.3.1 Character frequency distribution	29
1.8.3.2 Heterogeneity of the source and encrypted files	29
1.8.3.3 Avalanche test	30
1.8.3.4 Runs test	30
1.8.4 Microprocessor-based implementation	30
1.9 Structure of the thesis	31
Chapter 2: Prime Position Orientations (PPO)	32
2.1 Introduction	32
2.2 The PPO scheme	32
2.3 Example	34
2.4 Discussion	35
2.5 Microprocessor-based implementation	40
2.5.1 Routines for 8-bit block-size	40
2.5.1.1 Routines for 8-bit RSPB	41
2.5.1.2 Routine for 8-bit LSPB	42
2.5.1.3 Routine for 8-bit DSPB	42
2.5.2 Routine for 16-bit (and higher) block-sizes	43
2.5.2.1 Routines for 16-bit (and higher) RSPB	44
2.5.2.2 Routine for 16-bit (and higher) LSPB	46
2.5.2.3 Routine for 16-bit (and higher) DSPB	46

2.6	Results and comparisons	46
2.6.1	Character frequency	47
2.6.2	Chi-Square test and encryption time	52
2.6.3	Avalanche and runs	56
2.7	Conclusion	59

Chapter 3: Block Exchange Technique (BET) 60

3.1	Introduction	60
3.2	The BET scheme	60
3.2.1	Algorithm for BET	60
3.3	Example of BET	61
3.3.1	A discussion	62
3.4	Microprocessor-based implementation	63
3.4.1	Routines for block-size 8 bits	63
3.4.1.1	Routines for 8-bit BET	64
3.4.2	Routine for block-size 16 bits (and higher)	65
3.4.2.1	Routines for 16-bit (and higher) BET	65
3.5	Results and comparisons	67
3.5.1	Character frequency	67
3.5.2	Chi-Square test and encryption time	70
3.5.3	Avalanche and runs	73
3.6	Conclusion	74

Chapter 4: Selective Positional Orientation of Bits (SPOB) 75

4.1	Introduction	75
4.2	The SPOB scheme	75
4.2.1	The rounds of SPOB	75
4.3	Example and discussion	76
4.4	Microprocessor-based implementation	78
4.4.1	Look-up tables for 8-bit SPOB	78
4.4.2	Look-up tables for 16-bit (and higher) SPOB	79
4.5	Results and comparisons	79
4.5.1	Character frequency	79
4.5.2	Chi-Square test and encryption time	82
4.5.3	Avalanche and runs	85
4.6	Conclusion	86

Chapter 5: Modulo-Arithmetic Technique (MAT) 87

5.1	Introduction	87
5.2	The Modulo-Arithmetic Technique	87
5.2.1	Algorithm for MAT	88
5.2.2	The modulo-addition operation	88
5.3	Example of MAT	89
5.4	Microprocessor-based implementation	90
5.4.1	Routine for 8-bit MAT encryption	90
5.4.2	Routine for 8-bit MAT decryption	91
5.4.3	Routine for 16-bit (and higher) MAT encryption	92
5.4.4	Routine for 16-bit (and higher) MAT decryption	92
5.5	Results and comparisons	93
5.5.1	Character frequency	93
5.5.2	Chi-Square test and encryption time	96
5.5.3	Avalanche and runs	99
5.6	Conclusion	100

Chapter 6: Overlapped Modulo-Arithmetic Technique (OMAT)	101
6.1 Introduction	101
6.2 The Overlapped Modulo-Arithmetic Technique	101
6.3 Example of OMAT	102
6.4 Microprocessor-based implementation	103
6.4.1 Routine for 8-bit OMAT encryption	103
6.4.2 Routine for 8-bit OMAT decryption	104
6.4.3 Routine for 16-bit (and higher) OMAT encryption	104
6.4.4 Routine for 16-bit (and higher) OMAT decryption	105
6.5 Results and comparisons	105
6.5.1 Character frequency	105
6.5.2 Chi-Square test and encryption time	108
6.5.3 Avalanche and runs	111
6.6 Conclusion	112
Chapter 7: Modified Modulo-Arithmetic Technique (MMAT)	113
7.1 Introduction	113
7.2 The Modified Modulo-arithmetic Technique	113
7.3 Example of MMAT	114
7.4 Microprocessor-based implementation	115
7.4.1 Routine for 8-bit MMAT encryption	115
7.4.2 Routine for 8-bit MMAT decryption	116
7.4.3 Routine for 16-bit (and higher) MMAT encryption	117
7.4.4 Routine for 16-bit (and higher) MMAT decryption	117
7.5 Results and comparisons	118
7.5.1 Character frequency	118
7.5.2 Chi-Square test and encryption time	121
7.5.3 Avalanche and runs	124
7.6 Conclusion	125
Chapter 8: Bit-pair Operation and Separation (BOS)	126
8.1 Introduction	126
8.2 The BOS technique	126
8.2.1 The algorithm for BOS	126
8.2.2 The bit-pair operations	127
8.3 Example of BOS	128
8.4 Microprocessor-based implementation	129
8.4.1 Routine for 8-bit BOS encryption/decryption	130
8.4.2 Routine for 16-bit BOS (and higher) encryption/decryption	131
8.5 Results and comparisons	132
8.5.1 Character frequency	132
8.5.2 Chi-Square test and encryption time	135
8.5.3 Avalanche and runs	138
8.6 Conclusion	139
Chapter 9: Decimal Equivalent Positional Substitution (DEPS)	140
9.1 Introduction	140
9.2 The DEPS scheme	140
9.2.1 Algorithm for DEPS encryption	141
9.2.2 Algorithm for DEPS decryption	142
9.3 Example of DEPS	143
9.3.1 The process of encryption	143
9.3.2 The process of decryption	144

9.4	Microprocessor-based implementation	145
9.4.1	Routine for 8-bit DEPS encryption	146
9.4.2	Routine for 8-bit DEPS decryption	146
9.5	Results and comparisons	147
9.5.1	Character frequency	147
9.5.2	Chi-Square test and encryption time	150
9.5.3	Avalanche and runs	153
9.6	Conclusion	155
Chapter 10: Cascaded Techniques: Product Ciphers		156
10.1	Introduction	156
10.2	OMAT and BET	156
10.2.1	Character frequency	156
10.2.2	Chi-Square test and encryption time	159
10.2.3	Avalanche and runs	162
10.3	MMAT and DSPB	163
10.3.1	Character frequency	163
10.3.2	Chi-Square test and encryption time	163
10.3.3	Avalanche and runs	168
10.4	Conclusion	169
Chapter 11: Proposed Key Formats		170
11.1	Introduction	170
11.2	Format 1	171
11.3	Format 2	172
11.4	Format 3	174
11.5	Format 4	176
11.6	Conclusion	177
Chapter 12: Concluding Discussions		179
12.1	Introduction	179
12.2	Comparison of character frequencies	185
12.3	Comparison of χ^2 values	186
12.4	Comparison of encryption times	186
12.5	Conclusions	186
Appendix A: C Source Codes		188
Appendix B: 8085 Assembly Language Programs		268
Appendix C: Figures and Tables		306
References		
<i>List of Publications by the Author</i>		