

Contents

Chapter 1: Introduction

Topics	Page no.
1.1 Introduction	3
1.2 Cryptosystems	4
1.2.1 Defining cryptosystems	4
1.2.2 Secret key cryptosystem	5
1.2.2.1 Requirements for secret key system	6
1.2.2.2 Evaluating a cryptographic system	7
1.2.2.3 Attacking a conventional encryption scheme	8
1.2.2.4 The condition for an encryption scheme to be unconditionally secure	9
1.2.2.5 The condition for an encryption scheme to be computationally secure	9
1.2.2.6 Basic building blocks in classical encryption techniques	10
1.2.2.6.1 Principals of substitution techniques	11
1.2.2.6.1.1 Ceaser cipher	11
1.2.2.6.1.2 Monoalphabetic substitution cipher	12
1.2.2.6.1.3 Homophonic substitution cipher	12
1.2.2.6.1.4 Play fair cipher	12
1.2.2.6.1.5 Polyalphabetic cipher	14
1.2.2.6.1.6 Vigenere cipher	14
1.2.2.6.2 Some other substitution ciphers	15
1.2.2.7 Principles of transposition technique	15
1.2.2.7.1 The rail fence technique	15
1.2.2.7.2 A cascaded approach	16
1.2.3 Public key cryptosystem	17
1.2.3.1 The Algorithm	17
1.2.3.2 Characteristics of public key cryptography	20

1.3 Evolution in the field of cryptography	21
1.4 Some of the existing techniques	23
1.4.1 The data encryption standard (DES)	24
1.4.1.1 Basic principals of DES	24
1.4.1.2 The basic algorithm	24
1.4.1.2.1 The function f	25
1.4.1.3 Application	26
1.4.1.3.1 Mode of operations	26
1.4.1.4 The DES controversy	27
1.4.2 The TDES technique	27
1.4.3 The RSA technique	27
1.4.3.1 The RSA algorithm	27
1.4.3.2 The Security of RSA	30
1.5 An overview of proposed technique	30
1.5.1 An overview of RCA technique	32
1.5.2 An overview of RKR technique	33
1.5.3 An overview of RSKA technique	34
1.5.4 An overview of CAOPB technique	34
1.5.5 An overview of RMOPB technique	35
1.5.6 An overview of CRKRTAB technique	36
1.5.7 A proposal on key structure for proposed techniques	38
1.5.7.1 Proposed key structure for block cipher with direct block-to-block conversion	39
1.5.7.2 Proposed key structure for block cipher with non contiguous bit allocation	39
1.5.7.3 Proposed key structure for block cipher with repeated block-to-block conversion	39
1.5.8 Factors considered for evaluating proposed techniques	40
1.5.8.1 Frequency distribution test	40
1.5.8.2 Chi square test	40
1.5.8.3 Analysis on the key space	41

1.5.8.4 Computation of encryption/decryption time	41
1.5.8.5 Comparison of performance with RSA/TDES techniques	42
1.6 A note on merits of proposed techniques	42

Chapter 2: RCA technique

2.1 Introduction	46
2.2 The scheme	47
2.3 Implementation	48
2.4 Results	56
2.4.1 Results of encryption/decryption time, and Chi square value	56
2.4.1.1 Result for .EXE files	56
2.4.1.2 Result for DOC files	58
2.4.1.3 Result for .DLL files	60
2.4.1.4 Result for .SYS files	62
2.4.1.5 Result for .CPP files	64
2.4.1.6 Discussion on Chi square test	66
2.4.2 Results of frequency distribution tests	68
2.4.3 Comparison with RSA and TDES system	71
2.4.3.1 Comparison of RCA with RSA, and TDES in terms of Chi square value	71
2.4.3.1.1 Comparison of RCA with RSA and TDES for .EXE files	71
2.4.3.1.2 Comparison of RCA with RSA and TDES for .DOC files	73
2.4.3.1.3 Comparison of RCA with RSA and TDES for .DLL files	75
2.4.3.1.4 Comparison of RCA with RSA and TDES for .SYS files	77
2.4.3.1.5 Comparison of RCA with RSA and TDES for .CPP files	79

2.4.3.2 Comparison of RCA with RSA and TDES in terms of frequency distribution	81
2.4.3.2.1 Comparison of RCA with RSA and TDES for .EXE files	82
2.4.3.2.2 Comparison of RCA with RSA and TDES for .DOC files	83
2.4.3.2.3 Comparison of RCA with RSA and TDES for .DLL files	84
2.4.3.2.4 Comparison of RCA with RSA and TDES for .SYS files	85
2.4.3.2.5 Comparison of RCA with RSA and TDES for .CPP files	86
2.5 Analysis	87
2.5.1 Analysis on block size	87
2.5.2 Analysis on factors considered for evaluation purpose	88
2.6 Conclusion	92

Chapter 3: RKR technique

3.1 Introduction	95
3.2 The scheme	96
3.2.1 Example	97
3.3 Implementation	99
3.4 Results	106
3.4.1 Results of encryption/decryption time, and Chi square value	106
3.4.1.1 Result for .EXE files	106
3.4.1.2 Result for .DOC files	108
3.4.1.3 Result for .DLL files	110
3.4.1.4 Result for .SYS files	112
3.4.1.5 Result for .CPP files	114
3.4.2 Results of frequency distribution tests	116

3.4.3 Comparison with RSA and TDES system	119
3.4.3.1 Comparison of RKR with RSA, and TDES in terms of Chi square value	119
3.4.3.1.1 Comparison of RKR with RSA and TDES for .EXE files	119
3.4.3.1.2 Comparison of RKR with RSA and TDES for .DOC files	121
3.4.3.1.3 Comparison of RKR with RSA and TDES for .DLL files	123
3.4.3.1.4 Comparison of RKR with RSA and TDES for .SYS files	125
3.4.3.1.5 Comparison of RKR with RSA and TDES for .CPP files	127
3.4.3.2 Comparison of RKR with RSA and TDES in terms of frequency distribution	129
3.4.3.2.1 Comparison of RKR with RSA and TDES for .EXE files	130
3.4.3.2.2 Comparison of RKR with RSA and TDES for .DOC files	131
3.4.3.2.3 Comparison of RKR with RSA and TDES for .DLL files	132
3.4.3.2.4 Comparison of RKR with RSA and TDES for .SYS files	133
3.4.3.2.5 Comparison of RKR with RSA and TDES for .CPP files	134
3.5 Analysis and conclusion	135
3.5.1 Comparative study of RKR with RCA techniques	135
3.5.1.1 Comparative study for .EXE files	135
3.5.1.2 Comparative study for .DOC files	136
3.5.1.3 Comparative study for .DLL files	137

3.5.1.4 Comparative study for .SYS files	137
3.5.1.5 Comparative study for .CPP files	138
3.5.2 A conclusive analysis of different results obtained	139

Chapter 4: RSKA technique

4.1 Introduction	144
4.2 The scheme	145
4.2.1 The encryption and decryption	145
4.3 Implementation	148
4.3.1 The process of encryption and decryption	149
4.4 Results	155
4.4.1 Computing encryption/decryption time and Chi square value	156
4.4.1.1 Result for .EXE files	156
4.4.1.2 Result for .DOC files	158
4.4.1.3 Result for .DLL files	160
4.4.1.4 Result for .SYS files	162
4.4.1.4 Result for .CPP files	165
4.4.2 Results on frequency distribution test	166
4.4.3 Comparison with RSA and TDES technique	169
4.4.3.1 Comparison of RSKA with RSA and TDES in terms of Chi square value	169
4.4.3.1.1 Comparison of RSKA with RSA and TDES for .EXE files	169
4.4.3.1.2 Comparison of RSKA with RSA and TDES for .DOC files	171
4.4.3.1.3 Comparison of RSKA with RSA and TDES for .DLL files	173
4.4.3.1.4 Comparison of RSKA with RSA and TDES for .SYS files	175
4.4.3.1.5 Comparison of RSKA with RSA and TDES for	

.CPP files	177
4.4.3.2 Comparison of RSKA with RSA and TDES in terms of frequency distribution	180
4.4.3.2.1 Comparison of RSKA and TDES for .EXE files	181
4.4.3.2.2 Comparison of RSKA and TDES for .DOC files	182
4.4.3.2.3 Comparison of RSKA and TDES for .DLL files	183
4.4.3.2.4 Comparison of RSKA and TDES for .SYS files	184
4.4.3.2.5 Comparison of RSKA and TDES for .CPP files	185
4.5 Analysis and conclusion	186
4.5.1 Comparative study of RSKA with RCA, and RKR techniques	186
4.5.1.1 Comparative study for .EXE files	186
4.5.1.2 Comparative study for .DOC files	187
4.5.1.3 Comparative study for .DLL files	188
4.5.1.4 Comparative study for .SYS files	188
4.5.1.5 Comparative study for .CPP files	189
4.5.2 A conclusive analysis of different results obtained	190

Chapter 5: CAOPB technique

5.1 Introduction	195
5.2 The scheme	196
5.2.1 The encryption/decryption technique	196
5.3 Implementation	198
5.3.1 Implementation of encryption/decryption of CAOPB technique	198
5.4 Results	205
5.4.1 Result of encryption/decryption time, Chi square value and file size alteration	206
5.4.1.1 Result for .EXE files	206
5.4.1.2 Result for .DOC files	208
5.4.1.3 Result for .DLL files	211
5.4.1.4 Result for .SYS files	213

5.4.1.5 Result for .CPP files	216
5.4.2 Result for frequency distribution test	218
5.4.3 Comparison with RSA and TDES technique	222
5.4.3.1 Comparison of CAOPB with RSA and TDES in terms of Chi square value	222
5.4.3.1.1 Comparison of CAOPB with RSA and TDES for .EXE files	222
5.4.3.1.2 Comparison of CAOPB with RSA and TDES for .DOC files	224
5.4.3.1.3 Comparison of CAOPB with RSA and TDES for .DLL files	226
5.4.3.1.4 Comparison of CAOPB with RSA and TDES for .SYS files	228
5.4.3.1.5 Comparison of CAOPB with RSA and TDES for .CPP files	231
5.4.3.2 Comparison of CAOPB with RSA and TDES in terms of frequency distribution	233
5.4.3.2.1 Comparison of CAOPB with RSA and TDES for .EXE files	234
5.4.3.2.2 Comparison of CAOPB with RSA and TDES for DOC files	235
5.4.3.2.3 Comparison of CAOPB with RSA and TDES for .DLL files	236
5.4.3.2.4 Comparison of CAOPB with RSA and TDES for .SYS files	237
5.4.3.2.5 Comparison of CAOPB with RSA and TDES for .CPP files	238
5.5 Analysis and conclusion	239
5.5.1 Comparative study of CAOPB with RSKA, RCA, and RKR technique	239
5.5.1.1 Comparative study for .EXE files	239

5.5.1.2 Comparative study for .DOC files	240
5.5.1.3 Comparative study for .DLL files	241
5.5.1.4 Comparative study for .SYS files	242
5.5.1.5 Comparative study for .CPP files	243
5.5.2 A conclusive analysis of different results obtained	244

Chapter 6: RMOPB technique

6.1 Introduction	250
6.2 The scheme	251
6.2.1 The encryption and decryption technique	251
6.2.1.1 Example	252
6.3 Implementation	254
6.4 Results	260
6.4.1 Results of encryption/decryption time and Chi square value	260
6.4.1.1 Result for .EXE files	260
6.4.1.2 Result for .DOC files	262
6.4.1.3 Result for .DLL files	264
6.4.1.4 Result for .SYS files	266
6.4.1.5 Result for .CPP files	268
6.4.2 Result of frequency distribution tests	270
6.4.3 Comparison with RSA and TDES technique	273
6.4.3.1 Comparison of RMOPB with RSA and TDES in terms Chi square value	273
6.4.3.1.1 Comparison of RMOPB with RSA and TDES for .EXE files	273
6.4.3.1.2 Comparison of RMOPB with RSA and TDES for .DOC files	276
6.4.3.1.3 Comparison of RMOPB with RSA and TDES for .DLL files	278
6.4.3.1.4 Comparison of RMOPB with RSA and TDES for	

.SYS files	281
6.4.3.1.5 Comparison of RMOPB with RSA and TDES for .CPP files	283
6.4.3.2 Comparison of RMOPB with RSA and TDES in terms of frequency distribution	286
6.4.3.2.1 Comparison of RMOPB with RSA and TDES for .EXE files	287
6.4.3.2.2 Comparison of RMOPB with RSA and TDES for .DOC files	288
6.4.3.2.3 Comparison of RMOPB with RSA and TDES for .DLL files	289
6.4.3.2.4 Comparison of RMOPB with RSA and TDES for .SYS .EXE files	290
6.4.3.2.5 Comparison of RMOPB with RSA and TDES for .CPP files	291
6.5 Analysis and conclusion	292
6.5.1 Comparative study of RMOPB with RCA, RKR, RSKA and CAOPB technique	292
6.5.1.1 Comparative study for .EXE files	292
6.5.1.2 Comparative study for .DOC files	293
6.5.1.3 Comparative study for .DLL files	294
6.5.1.4 Comparative study for .SYS files	295
6.5.1.5 Comparative study for .CPP files	296
6.5.2 A conclusive analysis of different results obtained	297

Chapter 7: CRKRTAB technique

7.1 Introduction	303
7.2 The scheme	304
7.2.1 Example	309
7.3 Implementation	312

7.4 Results	315
7.4.1 Results of encryption/decryption time and Chi square value	315
7.4.1.1 Result for .EXE files	316
7.4.1.2 Result for .DOC files	318
7.4.1.3 Result for .DLL files	320
7.4.1.4 Result for .SYS files	322
7.4.1.5 Result for .CPP files	324
7.4.2 Result of frequency distribution tests	326
7.4.3 Comparison with RSA and TDES technique	329
7.4.3.1 Comparison of CRKRTAB with RSA and TDES in terms Chi square value	329
7.4.3.1.1 Comparison of CRKRTAB with RSA and TDES for .EXE files	329
7.4.3.1.2 Comparison of CRKRTAB with RSA and TDES for .DOC files	331
7.4.3.1.3 Comparison of CRKRTAB with RSA and TDES for .DLL files	333
7.4.3.1.4 Comparison of CRKRTAB with RSA and TDES for .SYS files	335
7.4.3.1.5 Comparison of CRKRTAB with RSA and TDES for .CPP files	337
7.4.3.2 Comparison of CRKRTAB with RSA and TDES in terms of frequency distribution	339
7.4.3.2.1 Comparison of CRKRTAB with RSA and TDES for .EXE files	340
7.4.3.2.2 Comparison of CRKRTAB with RSA and TDES for .DOC files	341
7.4.3.2.3 Comparison of CRKRTAB with RSA and TDES for .DLL files	342
7.4.3.2.4 Comparison of CRKRTAB with RSA and TDES for .SYS files	343

7.4.3.2.5 Comparison of CRKRTAB with RSA and TDES for .CPP files	344
7.5 Analysis and conclusion	345
7.5.1 Comparative study of CRKRTAB with RCA, RKR, RSKA, CAOPB and RMOPB technique	345
7.5.1.1 Comparative study for .EXE files	345
7.5.1.2 Comparative study for .DOC files	346
7.5.1.3 Comparative study for .DLL files	347
7.5.1.4 Comparative study for .SYS files	348
7.5.1.5 Comparative study for .CPP files	349
7.5.2 A conclusive analysis of different results obtained	350

Chapter 8: Formation of secret key

8.1 Introduction	355
8.2 Proposed key structure	355
8.2.1 Proposed key structure for RCA technique	355
8.2.1.1 Example of key generation	357
8.2.1.2 Example of key generation for the given file size	359
8.2.2 Proposed key structure for RKR and CAOPB technique	360
8.2.2.1 Example of key generation	363
8.2.2.2 Example of key generation for the given file size	364
8.2.3 Proposed key structure for RMOPB and CRKRTAB technique	366
8.2.3.1 Example of key generation	368
8.2.3.2 Example of key generation for the given file size	370
8.2.4 Proposed key structure for RSKA technique	372
8.2.4.1 Example of key generation	374
8.2.4.2 Example of key generation for the given file size	375
8.3 Vulnerability	377
8.4 Conclusion	378

Chapter 9: Encryption through cascaded implementation of the proposed technique

9.1 Introduction	382
9.1.1 Basic principal of cascading	382
9.1.2 Strength of cascading approach	383
9.2 Implementation	383
9.2.1 Encrypting source file using proposed technique in cascaded manner	384
9.2.2 Decrypting encrypted file, encrypted using 9.1.2	386
9.2.3 Analysis and implementation	398
9.3 Result	390
9.4 Analysis	396
9.5 Proposal of an integrated encryption system	396
9.5.1 Principals of proposed integrated system	397
9.5.2 Schematic characteristics of the proposed integrated system	397
9.5.3 Operational Characteristics of the proposed integrated system	398
9.5.4 Structure of the secret key	398
9.5.4.1 Criteria for an efficient key generation	399
9.5.4.2 Formation of different segments in the 192-bit key	399
9.5.4.3 The 192-bit secret key	401
9.6 Conclusion	401

Chapter 10: A Conclusive discussion

10.1 Introduction	404
10.2 A comparative study	404
10.2.1 Comparison among different implementations	405
10.2.1.1 Comparison among different implementation for .EXE files	405
10.2.1.2 Comparison among different implementation for .DOC files	407
10.2.1.3 Comparison among different implementation for .DLL	

files	410
10.2.1.4 Comparison among different implementation for .SYS files	413
10.2.1.5 Comparison among different implementation for .CPP files	416
10.2.2 A comparison among different implementations, RSA and TDES technique	419
10.2.2.1 A comparison among different implementations, RSA and TDES technique for .EXE file	419
10.2.2.2 A comparison among different implementations, RSA and TDES technique for .DOC file	420
10.2.2.3 A comparison among different implementations, RSA and TDES technique for .DLL file	422
10.2.2.4 A comparison among different implementations, RSA and TDES technique for .SYS file	423
10.2.2.5 A comparison among different implementations, RSA and TDES technique for .CPP file	425
10.3 Conclusion	430

Appendix	Topic	Page no.
A	References	i-x
B	List of publications	xi-xv
C	List of source code	xvi-lvi
D	List of tables	lvii-lxv
E	List of figures	lxvi-lxix
F	List of graphs	lxx-lxxxiii