

# Contents

## Chapter 1: Introduction

<b>Topic</b>	<b>Page No.</b>
<b>1.1 Introduction</b>	<b>3</b>
<b>1.2 Cryptosystems</b>	<b>4</b>
<b>1.2.1 Definition of Cryptosystem</b>	<b>4</b>
<b>1.2.2 Secret Key Cryptosystem</b>	<b>5</b>
<b>1.2.2.1 Requirements for Secret Key Cryptosystem</b>	<b>6</b>
<b>1.2.2.2 Evaluating a Cryptographic System</b>	<b>8</b>
<b>1.2.2.3 Attacking a Conventional Encryption Scheme</b>	<b>9</b>
<b>1.2.2.4 The Condition for an Encryption Scheme to be Unconditionally Secure</b>	<b>9</b>
<b>1.2.2.5 The Condition for an Encryption Scheme to be Computationally Secure</b>	<b>10</b>
<b>1.2.2.6 Basic Building Blocks in Classical Encryption Techniques</b>	<b>11</b>
<b>1.2.2.6.1 Principles of Substitution Techniques</b>	<b>11</b>
<b>1.2.2.6.1.1 Caesar Cipher</b>	<b>12</b>
<b>1.2.2.6.1.2 Monoalphabetic Substitution Cipher</b>	<b>13</b>
<b>1.2.2.6.1.3 Homophonic Substitution Cipher</b>	<b>13</b>
<b>1.2.2.6.1.4 Playfair Cipher</b>	<b>13</b>
<b>1.2.2.6.1.5 Polyalphabetic Cipher</b>	<b>14</b>
<b>1.2.2.6.1.6 Vigenere Cipher</b>	<b>15</b>
<b>1.2.2.6.1.7 Enhancement from Vigenere Cipher</b>	<b>17</b>
<b>1.2.2.6.1.8 Some Other Substitution Ciphers</b>	<b>18</b>
<b>1.2.2.6.2 Principles of Transposition Techniques</b>	<b>18</b>

<b>Topic</b>	<b>Page No.</b>
<b>1.2.2.6.2.1 The Rail Fence Technique</b>	<b>18</b>
<b>1.2.2.6.2.1.1 A Cascaded Approach</b>	<b>19</b>
<b>1.2.2.6.3 Rotor Machines – Composite Substitution and Transposition Cipher</b>	<b>20</b>
<b>1.2.3 Public Key Cryptosystem</b>	<b>21</b>
<b>1.2.3.1 The Algorithm</b>	<b>22</b>
<b>1.2.3.2 Characteristics of Public Key Cryptography</b>	<b>25</b>
<b>1.3 Evolution in the Field of Cryptography</b>	<b>25</b>
<b>1.4 Some of the Existing Techniques</b>	<b>28</b>
<b>1.4.1 The Data Encryption Standard (DES)</b>	<b>28</b>
<b>1.4.1.1 Basic Principles of DES</b>	<b>28</b>
<b>1.4.1.2 The Basic Algorithm</b>	<b>29</b>
<b>1.4.1.2.1 The Function f</b>	<b>30</b>
<b>1.4.1.3 Applications</b>	<b>30</b>
<b>1.4.1.3.1 Modes of Operations</b>	<b>31</b>
<b>1.4.1.4 The DES Controversy</b>	<b>31</b>
<b>1.4.2 The RSA Technique – The Special Characteristics</b>	<b>31</b>
<b>1.4.2.1 The RSA Algorithm</b>	<b>31</b>
<b>1.4.2.2 The Security of RSA</b>	<b>34</b>
<b>1.5 An Overview of Proposed Techniques</b>	<b>34</b>
<b>1.5.1 An Overview of the RPSM Technique</b>	<b>37</b>
<b>1.5.2 An Overview of the TE Technique</b>	<b>38</b>
<b>1.5.3 An Overview of the RPPO Technique</b>	<b>40</b>
<b>1.5.4 An Overview of the RPMS Technique</b>	<b>41</b>
<b>1.5.5 An Overview of the RSBP Technique</b>	<b>42</b>
<b>1.5.6 An Overview of the RSBM Technique</b>	<b>43</b>
<b>1.5.7 A Proposal on Key Structures for Proposed Techniques</b>	<b>44</b>

<b>Topic</b>	<b>Page No.</b>
1.5.7.1 Proposed Key Structure for Block Ciphers with Direct Block-to-Block Conversion	45
1.5.7.2 Proposed Key Structure for Block Ciphers with Option-based Block-to-Block Conversion	45
1.5.7.3 Proposed Key Structure for Block Ciphers with Non-Contiguous Bit Allocation	46
1.5.7.4 Proposed Key Structure for Block Ciphers with Repeated Block-to-Block Conversion	46
1.5.8 Factors Considered for Evaluating Proposed Techniques	46
1.5.8.1 Frequency Distribution Test	46
1.5.8.2 Chi Square Test	47
1.5.8.3 Analysis of the Key Space	47
1.5.8.4 Computation of Encryption/Decryption Time	48
1.5.8.5 Comparison of Performance with RSA Technique	48
1.6 A Note on Merits of Proposed Techniques	48

## **Chapter 2: Encryption Through Recursive Positional Substitution based on Prime-Nonprime (RPSP) of Cluster**

<b>Topic</b>	<b>Page No.</b>
2.1 Introduction	53
2.2 The Scheme	54
2.2.1 Example	56
2.2.1.1 Example of Encryption	59
2.2.1.2 Example of Decryption	59
2.3 Implementation	59
2.4 Results	66

Topic	Page No.
2.4.1 Result for Encryption/Decryption Time and Chi Square Value	66
2.4.1.1 Result for <i>EXE</i> Files	67
2.4.1.2 Result for <i>COM</i> Files	68
2.4.1.3 Result for <i>DLL</i> Files	69
2.4.1.4 Result for <i>SYS</i> Files	70
2.4.1.5 Result for <i>CPP</i> Files	72
2.4.1.6 Report on Variation of Encryption Time with Varying Block Sizes	73
2.4.2 Results for Frequency Distribution Tests	75
2.4.3 Comparison with RSA Technique	78
2.5 Analysis	80
2.5.1 Proof of Cycle Formation	80
2.5.2 Analysis on Block Size	81
2.5.3 Analysis on Factors Considered for Evaluation Purpose	84
2.6 Conclusion	87

### Chapter 3: Encryption Through Triangular Encryption (TE) Technique

Topic	Page No.
3.1 Introduction	90
3.2 The Scheme	91
3.2.1 Formation of Triangle	91
3.2.2 Options for Forming Target Blocks from Triangle	93
3.2.3 Generating Source Block from a Target Block	94
3.2.3.1 Generating Source Block from Target Block $s^{n-1}_0$ $s^{n-2}_0 s^{n-3}_0 s^{n-4}_0 s^{n-5}_0 \dots s^1_0 s^0_0$ (With Option Serial No. 010)	94

Topic	Page No.
<b>3.2.3.2 Generating Source Block from Target Block</b> $S^0_{n-1} S^1_{n-2} S^2_{n-3} S^3_{n-4} S^4_{n-5} \dots S^{n-2}_1 S^{n-1}_0$ (With Option Serial No. 011)	95
<b>3.2.4 A Sample Example to Illustrate the Scheme</b>	96
<b>3.3 Implementation</b>	98
<b>3.4 Results</b>	116
<b>3.4.1 Result for Encryption/Decryption Time and Chi Square  Value</b>	116
<b>3.4.1.1 Result for EXE Files</b>	117
<b>3.4.1.2 Result for COM Files</b>	118
<b>3.4.1.3 Result for DLL Files</b>	120
<b>3.4.1.4 Result for SYS Files</b>	121
<b>3.4.1.5 Result for CPP Files</b>	123
<b>3.4.2 Results for Frequency Distribution Tests</b>	124
<b>3.4.3 Comparison of TE with RSA Technique</b>	127
<b>3.5 Analysis and Conclusion including Comparison with RPSP</b>	129

## Chapter 4: Encryption Through Recursive Paired Parity Operation (RPPO)

Topic	Page No.
<b>4.1 Introduction</b>	132
<b>4.2 The Scheme</b>	133
<b>4.2.1 Example</b>	134
<b>4.3 Implementation</b>	136
<b>4.4 Results</b>	143
<b>4.4.1 Result of Encryption/Decryption Time, Total Number of  Operations, Chi Square Value</b>	143

<b>Topic</b>	<b>Page No.</b>
4.4.1.1 Result for <i>EXE</i> Files	144
4.4.1.2 Result for <i>COM</i> Files	145
4.4.1.3 Result for <i>DLL</i> Files	146
4.4.1.4 Result for <i>SYS</i> Files	148
4.4.1.5 Result for <i>CPP</i> Files	150
4.4.2 Results of Frequency Distribution Tests	151
4.4.3 Comparison with RSA Technique	154
4.5 Analysis and Conclusion including Comparison with RPSP, TE	156
4.5.1 Comparative Analysis with RPSP and TE Techniques	156
4.5.2 Formation of Cycle	156
4.5.3 Proof of the Finiteness in Re-generating Source Block	159
4.5.3.1 Proof for Block Size of 2 Bits	159
4.5.3.2 Proof for Block Size of 3 Bits	159
4.5.3.3 Proof for Block Size of 4 Bits	159
4.5.4 A Conclusive Analysis of Different results Obtained	160

## **Chapter 5: Encryption Through Recursive Positional Modulo-2 Substitution (RPMS) Technique**

<b>Topic</b>	<b>Page No.</b>
5.1 Introduction	166
5.2 The Scheme	167
5.2.1 The Encryption	167
5.2.2 The Decryption	171
5.3 Implementation	174
5.3.1 The Process of Encryption	174
5.3.2 The Process of Decryption	177
5.4 Results	178
5.4.1 Computing Encryption/Decryption Time	179

<b>Topic</b>	<b>Page No.</b>
5.4.1.1 Result for <i>EXE</i> Files	179
5.4.1.2 Result for <i>COM</i> Files	180
5.4.1.3 Result for <i>DLL</i> Files	182
5.4.1.4 Result for <i>SYS</i> Files	183
5.4.1.5 Result for <i>CPP</i> Files	185
5.4.1.6 Discussion on Chi Square Tests	186
5.4.2 Result on Frequency Distribution Tests	188
5.4.3 Comparison with RSA Technique	191
5.5 Analysis and Conclusion including Comparison with RPSP, TE, RPPO	193

## **Chapter 6: Encryption Through Recursive Substitution of Bits Through Prime-Nonprime (RSBP) Detection of Sub-stream**

<b>Topic</b>	<b>Page No.</b>
6.1 Introduction	197
6.2 The Scheme	198
6.2.1 The Encryption Technique	198
6.2.2 The Decryption Technique	202
6.3 Implementation	206
6.3.1 Implementation of Encryption Technique of RSBP	207
6.3.2 Implementation of Decryption Technique of RSBP	210
6.4 Results	217
6.4.1 Result of Encryption/Decryption Time, Chi Square value and File Size Alteration	218
6.4.1.1 Result for <i>EXE</i> Files	218
6.4.1.2 Result for <i>COM</i> Files	219
6.4.1.3 Result for <i>DLL</i> Files	221

<b>Topic</b>	<b>Page No.</b>
6.4.1.4 Result for <i>SYS</i> Files	223
6.4.1.5 Result for <i>CPP</i> Files	225
6.4.2 Result for Frequency Distribution Tests	226
6.4.3 Comparison with RSA Technique	229
6.5 Analysis and Conclusion including Comparison with RPSP, TE, RPPO, RPMS	231

## **Chapter 7: Encryption Through Recursive Substitution of Bits Through Modulo-2 (RSBM) Detection of Substream**

<b>Topic</b>	<b>Page No.</b>
7.1 Introduction	235
7.2 The Scheme	236
7.2.1 The Encryption Technique	236
7.2.2 The Decryption Technique	240
7.3 Implementation	244
7.4 Results	252
7.4.1 Result of Encryption/Decryption Time and Chi Square Value	253
7.4.1.1 Result for <i>EXE</i> Files	253
7.4.1.2 Result for <i>COM</i> Files	254
7.4.1.3 Result for <i>DLL</i> Files	256
7.4.1.4 Result for <i>SYS</i> Files	257
7.4.1.5 Result for <i>CPP</i> Files	258
7.4.2 Result of Frequency Distribution Tests	259
7.4.3 Comparison with RSA Technique	262
7.5 Analysis and Conclusion including Comparison with RPSP, TE, RPPO, RPMS, RSBP	264



## **Chapter 8: Formation of Secret Key**

<b>Topic</b>	<b>Page No.</b>
<b>8.1 Introduction</b>	<b>268</b>
<b>8.2 Proposed Key Structures</b>	<b>268</b>
<b>8.2.1 Proposed Key Structure for RPSP and RPPO Techniques</b>	<b>269</b>
<b>8.2.2 Proposed Key Structure for TE Technique</b>	<b>270</b>
<b>8.2.3 Proposed Key Structure for RSBP Technique</b>	<b>272</b>
<b>8.2.4 Proposed Key Structure for RPMS and RSBM Techniques</b>	<b>274</b>
<b>8.3 Conclusion</b>	<b>276</b>

## **Chapter 9: Encryption Through Cascaded Implementation of Proposed Techniques**

<b>Topic</b>	<b>Page No.</b>
<b>9.1 Introduction</b>	<b>280</b>
<b>9.1.1 Basic Principle of Cascading</b>	<b>280</b>
<b>9.1.2 Strength of the Cascaded Approach</b>	<b>281</b>
<b>9.2 Implementation</b>	<b>282</b>
<b>9.2.1 Encrypting Source File using Proposed Techniques in Cascaded Manner</b>	<b>282</b>
<b>9.2.2 Decrypting Encrypted File, Encrypted in Section 9.2.1</b>	<b>284</b>
<b>9.2.3 Analysis of Implementation</b>	<b>286</b>
<b>9.3 Results</b>	<b>288</b>
<b>9.4 Analysis</b>	<b>293</b>
<b>9.5 Proposal of An Integrated Encryption System</b>	<b>293</b>
<b>9.5.1 Principles of the Proposed Integrated System</b>	<b>294</b>
<b>9.5.2 Schematic Characteristics of the Proposed Integrated System</b>	<b>294</b>

<b>Topic</b>	<b>Page No.</b>
<b>9.5.3 Operational Characteristics of the Proposed Integrated System</b>	<b>295</b>
<b>9.5.4 Structure of the Secret Key for the Integrated System</b>	<b>296</b>
<b>9.5.4.1 Criteria for an Efficient Key Generation</b>	<b>296</b>
<b>9.5.4.2 Formation of Different Segments in the 252-bit Key</b>	<b>296</b>
<b>9.5.4.3 The 252-bit Secret Key</b>	<b>299</b>
<b>9.6 Conclusion</b>	<b>300</b>

## **Chapter 10: A Conclusive Discussion**

<b>Topic</b>	<b>Page No.</b>
<b>10.1 Introduction</b>	<b>303</b>
<b>10.2 A Comparison among Different Implementations</b>	<b>303</b>
<b>10.3 Conclusion on Different Model Implementations</b>	<b>310</b>

<b>Appendix</b>	<b>Topic</b>	<b>Page No.</b>
<b>A</b>	<b>References</b>	<b>i</b>
<b>B</b>	<b>List of Publications</b>	<b>vii</b>
<b>C</b>	<b>Listing of Source Codes</b>	<b>x</b>
<b>D</b>	<b>Bibliography</b>	<b>lxxiv</b>