# CONTENTS

<table>
<thead>
<tr>
<th>Title</th>
<th>Page No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>List of Tables</td>
<td>I-II</td>
</tr>
<tr>
<td>List of Figures</td>
<td>III-VII</td>
</tr>
<tr>
<td>List of Abbreviations</td>
<td>VIII-X</td>
</tr>
</tbody>
</table>

## Chapter 1: Introduction

1.1 Cryptography                                1
1.2 Plaintext and Ciphertext                    2
1.3 Encryption                                  3
1.4 Decryption                                  3
1.5 Encryption Key                              4
1.6 Stream Cipher and Block Cipher              4
1.7 Cryptographic Algorithms                   6
1.8 Operations Used by the Cryptographic Algorithms 7
1.9 Strength of Cryptographic Algorithms       8
1.10 Conventional Encryption Techniques        10
   1.10.1 Caesar Cipher Technique                11
   1.10.2 Monoalphabetic Technique               12
   1.10.3 Polyalphabetic Technique               13
   1.10.4 Hill Cipher Technique                 15
   1.10.5 Transposition Technique               18
1.11 Key Based Algorithms                      21
   1.11.1 Symmetric Key Algorithms               22
   1.11.2 Public Key Algorithms                  23
1.12 One Time Pads                              24
1.13 Steganography                             24
1.14 Cryptanalysis                             25
1.15 Security of Cryptographic Algorithms      26
1.16 Modern Cryptography                       27
   1.16.1 DES                                    27
   1.16.2 Triple DES                             31
   1.16.3 AES                                    32
   1.16.4 IDEA                                   37
   1.16.5 RSA                                    40
1.16.6 Hybrid Cryptographic System 42
   1.16.6.1 Digital Signing 42
   1.16.6.2 One-way Hash Function 42
   1.16.6.3 PGP: An Example of Hybrid Cryptographic System 44
1.16.7 ECC 45

Chapter 2: Literature Survey 48-68
   2.1 Introduction of Multiple Encryption 48
   2.2 The Importance of Multiple Encryption 50
   2.3 Comparison of Latest Multiple Encryption Techniques 53
   2.4 Categorization of Cryptographic Algorithms using Multiple Encryption 56
   2.5 Related Research Works and Results 62
   2.6 Recommendations for Cryptographic Algorithms 66

Chapter 3: Multiple Encryption: A New Framework 69-85
   3.1 General Approach of Multiple Encryption 69
   3.2 Working Criteria of Multiple Encryption 70
   3.3 Implementation of Multiple Encryption 71
   3.4 An Example of Multiple Encryption 78
   3.5 A Proposed Model of Multiple Encryption 79
      3.5.1 Basic Principle of Proposed Model of Multiple Encryption 79
      3.5.2 An Algorithm for Proposed Model of Multiple Encryption 82
      3.5.3 Experimental Results and Analysis 83

Chapter 4: Multiple Encryption in Information Security 86-106
   4.1 Multiple Encryption in Secure Electronic Transactions (SET) 86
      4.1.1 Needs of Encryption in SET 86
      4.1.2 Working Principle of SET 87
      4.1.3 Overview of the Proposed Multiple Encryption Technique in SET 90
   4.2 Multiple Encryption in Secure Voice Communication 91
      4.2.1 Description of Digital Secure Voice Communication 92
      4.2.2 SecureGSM: An Implementation of Secure Voice Communication 95
   4.3 Multiple Encryption in Secure Virtual Private Network 97
      4.3.1 Functionality of Virtual Private Network 97
      4.3.2 Multiple Encryption in Virtual Private Network 98
   4.4 Multiple Encryption for Secure Access to XML Documents 100
4.4.1 Overview of XML Encryption 100
4.4.2 Working Principle of Multiple Encryption in XML Document 101
4.4.3 A Program for Multiple Encryption of XML Document 102
4.5 Results and Conclusion 107

Chapter 5: Multiphase Encryption: An Extension of Multiple Encryption 108-130

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1 Multiphase Encryption</td>
<td>108</td>
</tr>
<tr>
<td>5.2 Working Principle of Multiphase Encryption</td>
<td>108</td>
</tr>
<tr>
<td>5.3 An Algorithm for Proposed Technique of Multiphase Encryption</td>
<td>111</td>
</tr>
<tr>
<td>5.4 Internal Architecture of Multiphase Encryption</td>
<td>111</td>
</tr>
<tr>
<td>5.5 An Encryption Tool used for proposed Multiple and Multiphase Encryption Technique</td>
<td>117</td>
</tr>
<tr>
<td>5.6 The implementation of Multiphase Encryption using Encryption Tool</td>
<td>120</td>
</tr>
<tr>
<td>5.7 Experimental Results and Analysis</td>
<td>128</td>
</tr>
<tr>
<td>5.8 Benefits and Limitations of Multiphase Encryption</td>
<td>129</td>
</tr>
</tbody>
</table>

Chapter 6: Conclusion and Scope for Future Work 131-133

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1 Conclusion</td>
<td>131</td>
</tr>
<tr>
<td>6.2 Future Work</td>
<td>132</td>
</tr>
</tbody>
</table>

- References 134-146
- Research Publications 147-148
- Appendices 149-156

Appendix-A: Some Tools for Multiple Encryption 149-153

Appendix-B: GINGER-A Software Tool for Grammar Checking used in Ph. D. Thesis 154-156