# LIST OF FIGURES

<table>
<thead>
<tr>
<th>Fig. 2.1</th>
<th>Symmetric Key Encryption</th>
<th>15</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fig. 2.2</td>
<td>Asymmetric Key Encryption</td>
<td>16</td>
</tr>
<tr>
<td>Fig. 2.3</td>
<td>Generic Representation of a Cryptographic Hash Function</td>
<td>18</td>
</tr>
<tr>
<td>Fig. 2.4</td>
<td>Example of One-Way Function</td>
<td>20</td>
</tr>
<tr>
<td>Fig. 2.5</td>
<td>Data Security Digital Signature Process</td>
<td>26</td>
</tr>
<tr>
<td>Fig. 2.6</td>
<td>e-Sign Architecture</td>
<td>28</td>
</tr>
<tr>
<td>Fig. 2.7</td>
<td>A Simple Representation of Image Steganography</td>
<td>29</td>
</tr>
<tr>
<td>Fig. 2.8</td>
<td>Few of The Common Biometric Types</td>
<td>32</td>
</tr>
<tr>
<td>Fig. 2.9</td>
<td>Biometric Based Key Release Method</td>
<td>33</td>
</tr>
<tr>
<td>Fig. 2.10</td>
<td>Biometrics-Based Key Generation Crypto -Biometric Matcher</td>
<td>33</td>
</tr>
<tr>
<td>Fig. 2.11</td>
<td>Comparison of Various Biometric Technologies</td>
<td>34</td>
</tr>
<tr>
<td>Fig. 2.12</td>
<td>Features of Biological Information Used in Biometric Techniques</td>
<td>36</td>
</tr>
<tr>
<td>Fig. 2.13</td>
<td>Pictorial Depiction of Diffie-Hellman Key Exchange</td>
<td>38</td>
</tr>
<tr>
<td>Fig. 2.14</td>
<td>Working of The DHKE Protocol</td>
<td>39</td>
</tr>
<tr>
<td>Fig. 2.15</td>
<td>MITM in The Classic DHKE Protocol</td>
<td>40</td>
</tr>
<tr>
<td>Fig. 2.16</td>
<td>Drug Counterfeit Incidents Reported Worldwide</td>
<td>49</td>
</tr>
<tr>
<td>Fig. 2.17</td>
<td>A Nucleotide</td>
<td>51</td>
</tr>
</tbody>
</table>
Fig. 2.18 Helical Structure of DNA 51
Fig. 2.19 DNA Strand 52
Fig. 2.20 Structure of DNA Base Pairs 52
Fig. 2.21 The Central Dogma of Molecular Biology 54
Fig. 2.22 The Stages in PCR 55
Fig. 2.23 Structure Coding Region in a Segment of Chromosomal DNA 56
Fig. 2.24 Represents DNA Fingerprinting 57
Fig. 2.25 Expanding the Genetic Alphabet 70
Fig. 3.1 Major Phases of Introns and Exons Based Data Encryption 80
Fig. 3.2 Represents Architecture of Proposed Scheme 84
Fig. 3.3 Verification Parameters Selected for the Analysis 91
Fig. 3.4 Scyther Analysis of Proposed Protocol 92
Fig. 3.5 Major Phases of Proposed PCR based Encryption Algorithm 97
Fig. 3.6 The Architecture of PCR based Data Encryption Algorithm 104
Fig. 3.7 Verification Parameters Selected for PCR Protocol Analysis 113
Fig. 3.8 Formal Analysis of the Proposed PCR based Protocol 114
Fig. 3.9 Major Phases of DNA-DHKE Protocol 121
Fig. 3.10 Message Sequence Chart of DNA-DHKE Protocol 128
Fig. 3.11 The Architecture of proposed DNA-DHKE of Protocol 129
Fig. 3.12 Verification Parameters for Analysis 136
Fig. 3.13 Formal Analysis of DNA-DHKE Using Scyther 137
Fig. 3.14 Registration Phase of DNA based User Authentication 144
Fig. 3.15 Authentication Phase of DNA based User Authentication 145
Fig. 3.16 DNA based User Authentication Architecture 147
Fig. 3.17 Screenshot of Canis Lupus Familiaris Whole Genome Sequence 149
Fig. 3.18 Screenshot of DNA Fragment Selected for Data Hiding 150
Fig. 3.19 Cover Image Selected for Steganography 150
Fig. 3.20 Stego Image Generated 152
Fig. 3.21 The Parameters Selected for Protocol Verification 155
Fig. 3.22 Formal Analysis of DNA based Authentication Protocol 156
Fig. 3.23 The Proposed Architecture for Health Care System in India 162
Fig. 3.24 Registration Phase for Healthcare User 164
Fig. 3.25 Authentication Phase for Health Care User 166
Fig. 3.26 The Architecture of Genome Steganography and Aadhaar based User Authentication 168
Fig. 3.27 The Parameters Selected for Protocol Verification Using Scyther 173
Fig. 3.28 Scyther Analysis of Proposed DNA based Authentication for the Health Care 174
Fig. 3.29 The Proposed Product Authentication Scheme 181
Fig. 3.30 Random Sequence Imported to Sequence Tool in MATLAB 183
Fig. 3.31 Complement DNA Sequence Generated Using Sequence Tool 184
Fig. 3.32 The QR Code Generated for Product Authentication 186
Fig. 3.33 Mobile based Product Authentication 187
Fig. 3.34 The Verification Parameters Selected for Scyther Analysis 188
Fig. 3.35 Formal Analysis of Product Authentication Method 189
Fig. 3.36 Process Flow of Generating Bio-Hash Algorithm 197
Fig. 3.37 Process Flow of Generating Bio-Sign for the e-Document 199
Fig. 3.38 Process Flow Diagram of Verification Bio-Sign and e-Document 201
Fig. 3.39 The Architecture for e-Sign based on DNA-Hash 202
Fig. 3.40 QR Code with Bio-Sign and a Link to the e-Sign Service Provider 204
Fig. 3.41 The Verification Parameters for Scyther Analysis 208
Fig. 3.42 Formal Analysis of Proposed Protocol Using Scyther 209
Fig. 4.1 The Integrated Architecture 213
Fig. A1 The Sequence Manipulation Suite 245
Fig. A2 The NCBI Home 247
Fig. A3 Selecting Taxonomy 248
Fig. A4 The Selected Taxonomy 248
Fig. A5 The Details of Organism Selected 249

Fig. A6 The Sequence Selected 249

Fig. A7 Selecting Sequence Using Accession Number 250

Fig. A8 The Salmonella Enterica Sequence 251