**Project Report Format & Guidelines**

**Department of CSE, BUBT**

This guide is designed to provide graduate students with the formatting requirements for all theses and project reports. It covers structure, layout, form, and style. Departments may use additional requirements that do not conflict with the guidelines provided in this document.

**1. Project Report Arrangement**

Assemble the thesis/project report in this order:

1. Cover page: includes the title, author, degree ("Thesis/Project submitted in partial fulfilment of the requirements for the Degree of Master of ... in ..."), and date.

2. Abstract; a concise summary of the essential information of the work being presented, namely of the study's scope, purpose and results. The reference-free single-spaced abstract should not exceed two pages.

3. Acknowledgments page: Should acknowledge all the people from whom you got support for this thesis or project.

4. Plagiarism policy compliance statement.

5. Copyright page that grants BUBT/ Students the right to use and reproduce fully or partially the work being presented.

6. Dedication page: You may dedicate your thesis/project to someone.

7. Certification

8. Thesis/Project Approval Form.

9. Abbreviations page: lists all the abbreviations used in the text alongside their fully written unabbreviated form.

10. Table of Contents: includes all the subsections of each chapter and the list of appendices (if applicable) and page numbers.

11. List of Figures: includes figure number, caption, and the page number.

12. List of Tables: includes table number, caption, and the page number.

13. Thesis/Project text; the layout is described in the next section

**2. Layout**

The following presents a framework for a thesis. The information is offered as a general guideline. Students should always consult their advisor for additional guidelines. In particular, the layout of project reports can be different depending on the type and scope of the project. Note that each chapter should start on a new page.

1**-** *Introduction:* background; statement of the problem; definition of terms; purpose of the study; theoretical basis; contributions of the study; organization of the remainder of the study (Site references from where you collect the information).

2- *Existing System and Literature Review*: chronological, categorical or related theoretical view points related to topic.

3- *Proposed Solution/Methodology:* Requirement Analysis, DFD design, E-R design, Database design, Implementations, Results Analysis, Social/National impact, Conclusions.

4*- User Manual:* Software/Hardware requirements, explain each and every screen shots, conclusions.

5- *Conclusions and Future works*: the entire research effort; addresses the initial purpose of the study (stated in the introduction); stresses the importance of the work accomplished; leaves a final impression on the reader. It can also include suggestions for further work (At most two pages).

6- *Bibliography/References:* references should acknowledge any work done by someone other than the author. The reference should also include work performed by the author if presented or published at an earlier date.  References should adopt the Harvard styles and citation is recommended. For more information, contact the supervisor/Chairman of the department.

7- *Appendices:* material too detailed or lengthy for inclusion in the body of the study (e.g. questionnaires, maps). Appendices may also contain information that might clarify the thesis but is routine in nature or indirectly related to the thesis. Raw data and examples of calculation could be incorporated.

**3. Style and Form**

**3.1   Paper:**Use high-quality acid-free A4-size paper, with only one side of the paper.

**Printing:**A high-quality laser printer should be used for the final copy**.**

**Headings:**

In disciplines where section numbering is normally used, the following guidelines apply:

Chapter title: 18 – 24 pt size, bold.

Main Section Headings: can be numbered as chapter-number.section-number (e.g., 3.2 for chapter 3, section 2) in 14 pt size, bold.

Second Headings:  can be numbered as x.y.z (e.g., 3.2.4 for chapter 3, section 2, subsection 4) in 12 pt size, bold.

First Subheadings: can be numbered as w.x.y.z (e.g., 3.2.4.1 for chapter 3, section 2, subsection 4, sub-subsection 1) in 12 pt size, regular.

Second Subheadings: preferably unnumbered, 12 pt, italics.

**Text Font:** Acceptable fonts generated by word processing programs include, but are not restricted to: Times Roman 12, Helvetica 12, Letter Gothic 12. The font provided through LaTeX is acceptable. Bold and italics should not be used excessively in the text. Furthermore, colored text should not be used.

**Spacing:** Double or one and a half spacing is required for the text.  Only footnotes, long quotations, bibliography entries (double space between entries), table captions, and similar special material may be single spaced.

**Margins:** Left, 4 cm; top, bottom, and right, 2.5 cm. These are necessary to allow for binding and trimming.

**Page Numbering:** Preliminary pages of the thesis, that is, those preceding the text are to be numbered in Roman numerals. The first page must not show its page number. Pages of the text itself and of all items following the text should be numbered consecutively throughout in Arabic numbers, beginning with number 1 on the first page of the first chapter. Page numbers should be placed in the lower right corner or center of the page. Only the number should appear, not page 9.

**Tables and Figures:** Figures and tables should be inserted at the appropriate place in the text. Figures must have numbers and captions under the figures. Tables have their titles and numbers above. Table and Figure numbers must include Chapter number and must be bold i.e., figure 1 of Chapter 2 should be numbered as **Figure 2.1**: Image Processing.

**Drawings**:  Any material which cannot be typed or computer generated should be drawn with permanent black ink in neat and heavy lines.  Photographs of drawings are acceptable.  Xerox reproductions of drawings are acceptable if they are of high contrast.

**Photographs:**Mount small photographs with glue. Do not use rubber cement or tape. High-clarity Xerox copies of photographs are also acceptable. However, high-quality scanned e-images can also be inserted into the thesis text.

**Footnotes:** In disciplines where footnotes are normally used, they should appear at the bottom of the same page as their reference. Footnotes should be numbered in Arabic numerals. The footnote reference is superscripted and the explanation at the bottom of the page begins with the footnote reference number. Footnotes should have a smaller font size than the text (e.g. 10 pt).

**CDs and DVDs:** identify with title, name of student, and date.

**Computer Software:** Describe in separate section in prefatory pages (e.g., list of figures and tables). If applicable, state requirements for the use of the software (e.g., hardware, screen resolution type) and any other information necessary for proper viewing of the software.

**Oversized Material:** Oversize foldout pages may be included, though ample margins for binding must be included. Leave oversize page unfolded. The bindery will fold and insert them. All pages must appropriately numbered if found in the text.

**Binding:** Binding will be arranged by the library, for a fee, in order to ensure consistency. At least two copies of the thesis should be submitted to the library of the campus concerned.

1. **Sample Table of Contents**

The following table of contents is appended to show how these guidelines can be implemented.

**Table of Contents**

**Page No**

|  |  |
| --- | --- |
| Abstract | ii |
| Declaration | iii |
| Certification  Dedication | iv |
| Acknowledgement | v |
| Approval  Copyright  Abbreviations | Vi  Vii  Viii |
|  |  |

1. **Introduction** 
   1. Introduction
   2. Existing Theory (with Problem Statement in a short form)
   3. Motivation
   4. Objectives
   5. Contributions
   6. Organization of Project Report
   7. Conclusions
2. **Existing System**

**2.1** Introduction

**2.2** Existing System

**2.3** Existing/supporting Literature

**2.4** Analysis of Existing System

**2.5** Conclusion

1. **Proposed model**

**3.1** Introduction

**3.2** Feasibility Study

3.3 Requirement Analysis

3.4 System Design

3.4.1 ERD

3.4.2 DFD

3.4.3 Database Design

3.4.4 Forms Design

3.4.5 Report Design

3.5 Implementation

3.6 Conclusions

**4. Experimental Results**

4.1 Introduction

4.2 Result Analysis

4.3 Applications

4.4 Conclusions

**5. User Manual**

5.1 Introduction

5.2 System Requirements

5.2.1 H/W Requirements

5.2.2 S/W Requirements

5.3 User Interface

5.3.1 Put all the screenshots with explanations how user can work and corresponding output. Each in one subsection

5.4 Conclusions

**6. Conclusions**

6.1. Conclusions (What you did; Why you did; How you did; Application)

6.2. Future Works extensions

|  |  |
| --- | --- |
| **List of Tables** | **ix** |
| **List of Figures** | **x** |
| **References** | **73** |
| **Appendix A** | **76** |
|  |  |

**List of Figures**

|  |  |
| --- | --- |
|  | **Page no** |
| **Figure-1.1**:Secret Key | 2 |
| **Figure-1.2**:Public Key | 2 |
| **Figure-1.3**:Hash Function | 3 |
| **Figure-2.1**:Cryptosystem | 10 |
| **Figure-2.2**:Symmetric Key Encryption and Decryption | 13 |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**List of Tables**

|  |  |
| --- | --- |
|  | **Page no** |
| **Table-2.1**: Cryptography Primitive table | 10 |
| **Table-2.2**: Generation of ElGamal Key Pair | 19 |
| **Table-2.3**:Cryptosystem | 37 |
| **Table-4.1**: Examples of Known Plain Test System | 68 |
| **Table-4.2**: Examples of Frequency Analysis | 70 |
| **Table-4.3**: Comparison | 71 |

**Thesis Report Format & Guidelines**

**Department of CSE, BUBT**

This guide is designed to provide graduate students with the formatting requirements for all theses and project reports. It covers structure, layout, form, and style. Departments may use additional requirements that do not conflict with the guidelines provided in this document.

1. **Thesis and Project Report Arrangement**

Assemble the thesis/project report in this order:

* 1. Cover page: includes the title, author, degree (“Thesis/Project submitted in partial fulfillment of the requirements for the Degree of Master of … in …”), and date.
  2. Abstract: a concise summary of the essential information of the work being presented, namely of the study’s scope, purpose and results. The reference-free single spaced abstract should not exceed two pages.
  3. Acknowledgments page (optional).
  4. Plagiarism policy compliance statement.
  5. Copyright page that grants BUBT/ Students the right to use and reproduce fully or partially the work being presented.
  6. Dedication page (optional).
  7. Certification
  8. Thesis/Project Approval Form.
  9. Abbreviations page: lists all the abbreviations used in the text alongside their fully written unabbreviated form.
  10. Table of Contents: includes all the subsections of each chapter and the list of appendices (if applicable) and page numbers.
  11. List of Figures: includes figure number, caption, and the page number.
  12. List of Tables: includes table number, caption, and the page number.
  13. Thesis/Project text; the layout is described in the next section.

**2. Layout**

The following presents a framework for a thesis. The information is offered as a general guideline. Students should always consult their advisor for additional guidelines. In particular, the layout of project reports can be different depending on the type and scope of the project. Note that each chapter should start on a new page.

1**-** *Introduction:* background; statement of the problem; definition of terms; purpose of the study; theoretical basis; contributions of the study; organization of the remainder of the study (Site references from where you collect the information).

2- *Literature Review*: chronological, categorical or related theoretical view points related to topic.

3- *Proposed Solution/Methodology:* research design or approach (quantitative, qualitative or algorithmic); population and / or sample; collection and tabulation of data; and data analysis procedures.

4- *Solution Validation, Analysis of the Data, Results, and Discussion:* presentation and discussion of the findings, including limitations.

5- *Conclusions, Recommendations:* What you did; Why you did; How you did; Application, summarizes the entire research effort; addresses the initial purpose of the study (stated in the introduction); stresses the importance of the work accomplished; leaves a final impression on the reader. It can also include suggestions for further work (At most two pages).

6- *Bibliography/References:* references should acknowledge any work done by someone other than the author. The reference should also include work performed by the author if presented or published at an earlier date.  References should adopt the Harvard styles and citation is recommended. For more information, contact the supervisor/Chairman of the department.

7- *Appendices:* material too detailed or lengthy for inclusion in the body of the study (e.g. questionnaires, maps). Appendices may also contain information that might clarify the thesis but is routine in nature or indirectly related to the thesis. Raw data and examples of calculation could be incorporated.

**3. Style and Form**

**3.1   Paper:**Use high-quality acid-free A4-size paper, with only one side of the paper.

**Printing:**A high-quality laser printer should be used for the final copy**.**

**Headings:**

In disciplines where section numbering is normally used, the following guidelines apply:

Chapter title: 18 – 24 pt size, bold.

Main Section Headings: can be numbered as chapter-number.section-number (e.g., 3.2 for chapter 3, section 2) in 14 pt size, bold.

Second Headings:  can be numbered as x.y.z (e.g., 3.2.4 for chapter 3, section 2, subsection 4) in 12 pt size, bold.

First Subheadings: can be numbered as w.x.y.z (e.g., 3.2.4.1 for chapter 3, section 2, subsection 4, sub-subsection 1) in 12 pt size, regular.

Second Subheadings: preferably unnumbered, 12 pt, italics.

**Text Font:** Acceptable fonts generated by word processing programs include, but are not restricted to: Times Roman 12, Helvetica 12, Letter Gothic 12. The font provided through LaTeX is acceptable. Bold and italics should not be used excessively in the text. Furthermore, colored text should not be used.

**Spacing:** Double or one and a half spacing is required for the text.  Only footnotes, long quotations, bibliography entries (double space between entries), table captions, and similar special material may be single spaced.

**Margins:** Left, 4 cm; top, bottom, and right, 2.5 cm. These are necessary to allow for binding and trimming.

**Page Numbering:** Preliminary pages of the thesis, that is, those preceding the text are to be numbered in Roman numerals. The first page must not show its page number. Pages of the text itself and of all items following the text should be numbered consecutively throughout in Arabic numbers, beginning with number 1 on the first page of the first chapter. Page numbers should be placed in the lower right corner or center of the page. Only the number should appear, not page 9.

**Tables and Figures:** Figures and tables should be inserted at the appropriate place in the text. Figures must have numbers and captions under the figures. Tables have their titles and numbers above. Table and Figure numbers must include Chapter number and must be bold i.e., figure 1 of Chapter 2 should be numbered as **Figure 2.1**: Image Processing.

**Drawings**:  Any material which cannot be typed or computer generated should be drawn with permanent black ink in neat and heavy lines.  Photographs of drawings are acceptable.  Xerox reproductions of drawings are acceptable if they are of high contrast.

**Photographs:**Mount small photographs with glue. Do not use rubber cement or tape. High-clarity Xerox copies of photographs are also acceptable. However, high-quality scanned e-images can also be inserted into the thesis text.

**Footnotes:** In disciplines where footnotes are normally used, they should appear at the bottom of the same page as their reference. Footnotes should be numbered in Arabic numerals. The footnote reference is superscripted and the explanation at the bottom of the page begins with the footnote reference number. Footnotes should have a smaller font size than the text (e.g. 10 pt).

**CDs and DVDs:** identify with title, name of student, and date.

**Computer Software:** Describe in separate section in prefatory pages (e.g., list of figures and tables). If applicable, state requirements for the use of the software (e.g., hardware, screen resolution type) and any other information necessary for proper viewing of the software.

**Oversized Material:** Oversize foldout pages may be included, though ample margins for binding must be included. Leave oversize page unfolded. The bindery will fold and insert them. All pages must appropriately numbered if found in the text.

**Binding:** Binding will be arranged by the library, for a fee, in order to ensure consistency. At least two copies of the thesis should be submitted to the library of the campus concerned.

1. **Sample Table of Contents**

The following table of contents is appended to show how these guidelines can be implemented.

**Table of Content**

|  |  |
| --- | --- |
|  | **Page no** |
| Abstract | ii |
| Declaration | iii |
| Certification | iv |
| Acknowledgement | v |
| Dedication | vi |
| Approval  Copyright  Abbreviations | vii |
| **Chapter 01**: **Introduction** | **1-5** |
| * 1. Introduction   2. Existing Model | 1 |
| 1.3 Aims and Objectives | 3 |
| 1.4 Contribution | 3 |
| 1.5 Organization of Thesis | 4 |
| 1.6 Conclusion | 5 |
| **Chapter 02** : **Data Encryption Basics** | **6-44** |
| 2.1 Introduction | 6 |
| 2.2 Cryptosystem | 7 |
| 2.3 Attacks on Cryptosystem | 38 |
| 2.4 Conclusion | 44 |
| **Chapter 3** : **BMR Encryption System** | **45-63** |
| 3.1 Introduction | 45 |
| 3.2 Procedure | 45 |
| 3.3 Flowchart | 58 |
| 3.4 Algorithm | 59 |
| 3.5 Example | 59 |
| 3.6 Advantage | 63 |
| 3.7 Conclusion | 64 |
| **Chapter 4** : **Experimental Result** | **64-71** |
| 4.1 Introduction | 64 |
| 4.2 Man in the Middle Attack | 64 |
| 4.3 Brute Force Attack | 65 |
| 4.4 Known Plain Text Attack | 66 |
| 4.5 Frequency Analysis | 69 |
| 4.6 Comparison | 71 |
| 4.7 Conclusion | 71 |
| **Chapter 5** : **Conclusions** | **72** |
| 5.1 Conclusion | 72 |
| 5.2 Future Works | 72 |
| **List of Tables** | **ix** |
| **List of Figures** | **x** |
| **References** | **73** |
| **Appendix A** | **76** |
|  |  |

**List of Figures**

|  |  |
| --- | --- |
|  | **Page no** |
| **Figure-1.1**:Secret Key | 2 |
| **Figure-1.2**:Public Key | 2 |
| **Figure-1.3**:Hash Function | 3 |
| **Figure-2.1**:Cryptosystem | 10 |
| **Figure-2.2**:Symmetric Key Encryption and Decryption | 13 |
| **Figure-2.3**:Diffie-Hellam | 22 |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**List of Tables**

|  |  |
| --- | --- |
|  | **Page no** |
| **Table-2.1**: Cryptography Primitive table | 10 |
| **Table-2.2**: Generation of ElGamal Key Pair | 19 |
| **Table-2.3**:Cryptosystem | 37 |
| **Table-4.1**: Examples of Known Plain Test System | 68 |
| **Table-4.2**: Examples of Frequency Analysis | 70 |
| **Table-4.3**: Comparison | 71 |

**BMR Encryption System**

**(BMRES)**



**Department of Computer Science and Engineering**

**Bangladesh University of Business and Technology**

**Dhaka-1216**

**July 2017**

**BMR Encryption System**

**(BMRES)**

*A Thesis*

*submitted to the department of Computer Science and Engineering*

*in partial fulfillment of the requirements*

*for the degree of*

**Bachelor of Science in Computer Science and Engineering**

**By**

**Mohammad Mehadi Hasan (ID: 12132103018)**

**Nusrat Jahan Rakhi (ID: 12132103001)**

**G.M Shoaibuzzaman (ID: 12132103029)**

**Supervised by**

**Samsuddin Ahmed**

Assistant Professor

Department of Computer Science and Engineering (CSE)

Bangladesh University of Business and Technology (BUBT)

Mirpur-2, Dhaka-1216, Bangladesh

# **ABSTRACT**

In this paper, we propose a new encryption system. There are some encryption and decryption algorithms like AES, DES, 3DES and Blowfish which have been put forward to satisfy the security of the information. These algorithms are still very successful. But these algorithms are very complicated. We wanted to develop an algorithm that is simple, less complex but highly secure. Our main goal is to provide better security for communication. The algorithm will provide only one variable length key and variable length block size (vary from 128 to 512 bit). To develop this algorithm, we have used some basic logical operations and shuffling technics. Here we have used our own character table for encryption and decryption. We extract the key from the data. The minimum length of the key is 128 bit. This is an End-To-End encryption system. In further it can also be used for transferring image, audio and video files from one end to another end.

We designed such an algorithm that is both simple and efficient. Though it is simple and the key length is variable it is impossible to break. Our study will show that this algorithm will be very helpful for secure communication.

# **DECLARATION**

We declare that this thesis and the work presented in it are our own and has been generated by us as the result of our own original research

We confirm that:

* This Work is done wholly or mainly while in candidature for a research degree at this University;
* This thesis work has not been previously submitted for any degree at this university or any other educational institutes;
* We have quoted from the work of others; the source is always given. With the exception of such quotations, this thesis is entire our own work;

-------------- -------------- --------------

Md. Mehadi Hasan Nusrat Jahan Rakhi G.M Shoaibuzzaman

ID: 12132103018 ID: 12132103001 ID: 12132103029

# CERTIFICATE

This is to certify that Md. Mehadi Hasan, Nusrat Jahan Rakhi and G. M. Shoaibuzzaman students of B.Sc. in CSE have completed their thesis work titled “BMR Encryption System” satisfactorily in partial fulfillment for the requirement of B.Sc.in CSE. Bangladesh University of Business and Technology in the year 2017.

-------------- -------------- --------------

Md. Mehadi Hasan Nusrat Jahan Rakhi G.M Shoaibuzzaman

ID: 12132103018 ID: 12132103001 ID: 12132103029

**--------------------------------**

Thesis Supervisor

**(Samsuddin Ahmed)**

Assistant Professor

Department of Computer Science and Engineering (CSE)

Bangladesh University of Business and Technology (BUBT)

# **DEDICATION**

Dedicated to our parents for all their love and inspiration.

# **ACKNOWLEDGEMENTS**

First of all, we are thankful and expressing our gratefulness to Almighty Allah who offers us His divine blessing, patient, mental and physical strength to complete this project work.

We are deeply indebted to our project supervisor Samsuddin Ahmed, Assistant Professor, Department of Computer Science and Engineering (CSE), Bangladesh University of Business and Technology (BUBT). His scholarly guidance, important suggestions, work for going through our drafts and correcting them, and generating courage from the beginning to the end of the research work has made the completion of this thesis possible.

We would like to express our deep gratitude to our Teacher Md. Mahbubur Rahman, Assistant Professor, Department of Computer Science and Engineering (CSE), Bangladesh University of Business and Technology (BUBT). It was fantastic to get help from him and without his support it will be tough for us to reach the accurate goal.

A very special gratitude goes out to all our friends for their support and help to implement our works. The discussions with them on various topics of our works have been very helpful for us to enrich our knowledge and conception regarding the work.

Last but not the least; we are highly grateful to our parents and family members for supporting us spiritually throughout writing this thesis and our life in general.

# **APPROVAL**

This Thesis “**BMR Encryption System**” Submitted by **Md. Mehadi Hasan, G.M. Shoaibuzzaman** and  **Nusrat Jahan Rakhi** ID NO: **12132103018**, **12132103029** and **12132103001** Department of Computer Science and Engineering (CSE), Bangladesh University of Business and Technology (BUBT) under the supervision of Samsuddin Ahmed, Assistant Professor and, Department of Computer Science and Engineering has been accepted as satisfactory for the partial fulfillment of the requirement for the degree of Bachelor of Science (B.Sc. Eng.) in Computer Science and Engineering and approved as to its style and contents.

**--------------------------------**

**Supervisor:**

**Samsuddin Ahmed**

Assistant Professor

Department of Computer Science and Engineering (CSE)

Bangladesh University of Business and Technology (BUBT)

Mirpur-2, Dhaka-1216, Bangladesh

**--------------------------------**

**Chairman:**

|  |  |
| --- | --- |
| |  | | --- | | **Prof. M. Ameer Ali** | |

Professor and Chairman

Department of Computer Science and Engineering (CSE)

Bangladesh University of Business and Technology (BUBT)

Mirpur-2, Dhaka-1216, Bangladesh

© Copyright by Md. Mehadi Hasan (12132103018), G.M. Shoaibuzzaman (12132103029), and Nusrat Jahan Rakhi (12132103001)

All Right Reserved

# **Abbreviations**

|  |  |
| --- | --- |
| **Synonyms and Acronyms** | **Descriptions** |
| RAM | **R**andon **A**ccess **M**emmory |

**Table of Content**

|  |  |
| --- | --- |
|  | **Page no** |
| Abstract | ii |
| Declaration | iii |
| Certification | iv |
| Acknowledgement | v |
| Dedication | vi |
| Approval  Copyright | vii |
| **Chapter 01**: **Introduction** | **1-5** |
| * 1. Introduction   2. Existing Model | 1 |
| 1.3 Aims and Objectives | 3 |
| 1.4 Contribution | 3 |
| 1.5 Organization of Thesis | 4 |
| 1.6 Conclusion | 5 |
| **Chapter 02** : **Data Encryption Basics** | **6-44** |
| 2.1 Introduction | 6 |
| 2.2 Cryptosystem | 7 |
| 2.3 Attacks on Cryptosystem | 38 |
| 2.4 Conclusion | 44 |
| **Chapter 3** : **BMR Encryption System** | **45-63** |
| 3.1 Introduction | 45 |
| 3.2 Procedure | 45 |
| 3.3 Flowchart | 58 |
| 3.4 Algorithm | 59 |
| 3.5 Example | 59 |
| 3.6 Advantage | 63 |
| 3.7 Conclusion | 64 |
| **Chapter 4** : **Experimental Result** | **64-71** |
| 4.1 Introduction | 64 |
| 4.2 Man in the Middle Attack | 64 |
| 4.3 Brute Force Attack | 65 |
| 4.4 Known Plain Text Attack | 66 |
| 4.5 Frequency Analysis | 69 |
| 4.6 Comparison | 71 |
| 4.7 Conclusion | 71 |
| **Chapter 5** : **Conclusions** | **72** |
| 5.1 Conclusion | 72 |
| 5.2 Future Works | 72 |
| **List of Tables** | **ix** |
| **List of Figures** | **x** |
| **References** | **73** |
| **Appendix A** | **76** |
|  |  |

**List of Figures**

|  |  |
| --- | --- |
|  | **Page no** |
| **Figure-1.1**:Secret Key | 2 |
| **Figure-1.2**:Public Key | 2 |
| **Figure-1.3**:Hash Function | 3 |
| **Figure-2.1**:Cryptosystem | 10 |
| **Figure-2.2**:Symmetric Key Encryption and Decryption | 13 |
| **Figure-2.3**:Diffie-Hellam | 22 |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**List of Tables**

|  |  |
| --- | --- |
|  | **Page no** |
| **Table-2.1**: Cryptography Primitive table | 10 |
| **Table-2.2**: Generation of ElGamal Key Pair | 19 |
| **Table-2.3**:Cryptosystem | 37 |
| **Table-4.1**: Examples of Known Plain Test System | 68 |
| **Table-4.2**: Examples of Frequency Analysis | 70 |
| **Table-4.3**: Comparison | 71 |