

ST. XAVIER'S COLLEGE
MAITIGHAR, KATHMANDU

**GUIDELINES FOR PREPARATION OF PROJECT REPORT
(MINOR AND MAJOR PROJECT)**

Introduction

Project report in this manual refers to a documented report of the process followed and the results of minor and major project conducted by a student in fulfillment of the requirements in bachelor degree. This report will outline the report format for both Major and Minor Project. These rules must be adhered strictly.

Contents of Project report

The Project Report should contain the items as outlined below and is to be presented in the order as listed. Details and specimens are shown in the appendices.

Number of Copies to be submitted to the Department

Two hard copies of the report are to be submitted to the Department after corrections done as suggested by guide/Department at any time when report submission is called by guide/Department. Students are suggested to bind the report with hard cover and print the cover in golden. A soft copy (pdf format) should also be submitted to Department in CD along with report.

Requirements for Report Writing:

Your report should meet following standards:

Font Name: Times New Roman

Left Margin: 1 inch

Right Margin: 1 inch

Top Margin: 1.25 inch

Bottom Margin: 1.25 inch

Gutter Margin: 0.5 inch

Header and Footer: 0.5 inch

Line Spacing: 1.5

Paragraph Spacing: 18 pt
Font Size: 12 pt (for normal text)
Follow following standard for headings

1. Heading1 (16 pt, Bold)
1.1 Heading2 (14 pt, Bold)
1.1.1 Heading3 (13 pt, Bold)
1.1.1.1 Heading4 (12 pt, Bold)

1. ARRANGEMENT OF CONTENTS:

The sequence in which the project report material should be arranged and bound should be as follows:

- | | |
|------------------------------|-------------------|
| 1. Cover Page | (Specimen copy-1) |
| 2. Title Page | (Specimen copy-2) |
| 3. Certificate of Approval | (Specimen copy-3) |
| 4. Corporate Certificate | (If Available) |
| 5. Acknowledgment | (Specimen copy-4) |
| 6. Abstract | (Specimen copy-5) |
| 7. Table of Contents | (Appendix 1) |
| 8. List of Figures (if any) | (Appendix 2) |
| 9. List of Tables (if any) | (Appendix 3) |
| 10. List of Symbols (if any) | (Appendix 4) |
| 11. Abbreviations (if any) | (Appendix 5) |
| 12. Chapters | (Appendix 6) |
| 13. Appendices (if any) | |
| 14. References | (Appendix 7) |

** Students can add their own topics or sub-topics as per necessity.*

** Justify the report for clean look at both left and right side of page.*

**The level of English writing must be appropriate to the level of the Bachelor's degree. Normally, there should be no first person references (e.g., I, we, us) in the report. If self-reference is required, reference may be made to "the author" or "this study".*

2. BINDING SPECIFICATIONS:

Students have to submit tape or spiral binding of the report to the department at the time of report submission for correction purpose. Students are suggested to bind the final draft of the report with hard cover and print the cover in golden.

3. PREPARATION FORMAT:

Cover Page - A specimen copy of the Title page of the project report is given in **Specimen copy-1.**

Title Page – A specimen copy of the Title page of the project report is given in **Specimen copy-2.**

Certificate – A specimen copy of the Certificate of the project report is given **Specimen copy-3.**

Acknowledgment- A specimen copy of the Acknowledgment of the project report is given **Specimen copy-4.**

Abstract – It is a heart of the report. Abstract should be one-page synopsis of the project report and it must clearly give the overview of the project (Avoid unnecessary things in abstract) (**Specimen copy-5**).

Table of Contents – The table of contents should list all material following it as well as any material which precedes it. The title page and Certificate of approval will not find a place among the items listed in the Table of Contents but the page numbers of which are in lower case Roman letters. One and a half spacing should be adopted for typing the matter under this head. A specimen copy of the Table of Contents of the project report is given in **Appendix 1.**

List of Figures – The list should use exactly the same captions as they appear below the figures in the text. One and a half spacing should be adopted for typing the matter under this head (**Appendix 2**).

List of Tables – The list should use exactly the same captions as they appear above the tables in the text. One and a half spacing should be adopted for typing the matter under this head (**Appendix 3**).

List of Symbols - The list should provide the detail of the symbols used in the report. One and a half spacing should be adopted for typing the matter under this head (**Appendix 4**).

Abbreviations – Abbreviation list should provide the details of the abbreviations used in the report in alphabetical order. One and a half spacing should be adopted or typing the matter under this head (**Appendix 5**).

Page numbering - The preliminary parts (Acknowledgement, Abstract, Table of Contents, List of symbols, List of figure, List of Tables) are numbered in roman numerals (i, ii, etc). The first page of the first chapter (Introduction) onwards will be numbered in Arabic numerals 1 2 3 etc at the bottom, centered.

Numbering sections, subsections, equations, figures etc. - A word on numbering scheme used in the project is in order. It is common practice to use decimal numbering in the project. If the chapter number is 2, the section numbers will be 2.1,2.2, 2.3 etc. The subsections in section 2.2 will be numbered as 2.2.1, 2.2.2 etc. Unless essential, it is not necessary to use numbers to lower levels than three stages.

Similarly, it is useful and convenient to number the figures also chapter-wise. The figures in chapter 4 will be numbered as Figure 4.1: Figure Name, Figure 4.2: Figure Name etc. This helps you in assembling the figures and putting it in proper order. Similarly, the tables are also numbered as Table 4.1: Table Name, Table 4.2: Table

Name etc. All figures and tables should have proper captions. Usually the figure captions are written below the figure and table captions on top of the table. All figures should have proper description by legends, title of the axes and any other information to make the figures self-explanatory.

The same numbering scheme can be used for equations also. Only thing to be remembered is that references to the figures are made like Figure 4.2: Figure Name, and equations as Eqn (5.8).

Chapters – The main text will be divided into several chapters and each chapter may be further divided into several divisions and sub-divisions.

Chapter 1: Introduction

- Problem Statement
- Objectives and Scope
- Project Features
- Requirement Analysis and Feasibility
- System Requirement – Hardware and Software Platforms

Chapter 2: Literature Review (Use IEEE Citation and Referencing guidelines)

Chapter 3: System Development

- Project Management Strategy and Tools
- System Analysis
- System Design (Algorithm, Flowchart, Context Diagram, DFD upto Level 2 for major processes, ER Diagram, Use Case Diagrams, Class Diagrams, System Sequence Diagram, DB and its Schema) **[explain every diagram used]**
- Project Schedule (GANTT Chart, Time Schedule)
- System Testing [Include various testing strategies with relevant test case, test scenario and testing screen shots]
- Implementation Methods

Chapter 4: Result Analysis

- Results with relevant screen shots **[function prototype, screenshot and explanation of the screen]**
- Critical Analysis
- Application of the system
- Limitations and Future Enhancements
- Conclusion

Chapter 5: Bibliography (Optional)

Chapter 6: References

Chapter 7: Appendix (If Any)

List of References –The reference material should include the author name, title, year in details as shown in **Appendix 7**.

Appendices – Appendices are provided to give supplementary information, which is included in the main text may serve as a distraction and cloud the central theme. Appendices should be numbered using Arabic numerals, e.g. Appendix 1, Appendix 2, etc. Tables and References appearing in appendices should be numbered and referred to at appropriate places just as in the case of chapters.

SPECIMEN -1 (Cover Page)
ST. XAVIER'S COLLEGE
(Affiliated to Tribhuvan University)
Maitighar, Kathmandu



Final Year Project Report
on
“Project Title” - (Course Code)

A Final Year Project Report submitted in the partial fulfillment of the requirements for the degree of Bachelor of Science in Computer Science and Information Technology awarded by Tribhuvan University

Under the supervision of
“Supervisor Name”
“Designation”

Submitted by
Full Name (T.U. Exam Roll No. 494/066)
Full Name (T.U.Exam Roll No. 506/066)

Submitted to
ST. XAVIER'S COLLEGE
Department of Computer Science
Maitighar, Kathmandu, Nepal
October ____, 2016

SPECIMEN-2 (Title Page for Project)

Project Title

[Course Code:]

A final year project report submitted in partial fulfillment of the requirements for the degree of Bachelor of Science in Computer Science and Information Technology awarded by Tribhuvan University

Submitted by

Full Name (T.U. Exam Roll No. 494/066)

Full Name (T.U.Exam Roll No. 506/066)

Submitted to

ST. XAVIER'S COLLEGE

Department of Computer Science

Maitighar, Kathmandu, Nepal

October ____, 2016

SPECIMEN-3 (Certificate of Approval for Major Project)



ST. XAVIER'S COLLEGE
MAITIGHAR, KATHMANDU, NEPAL
Post Box :7437
Contact: 4221365,4244636
Email: ktm@xsc.edu.np

सेन्ट जेभियर्स कलेज
माईतीघर, काठमाडौं, नेपाल
पो.ब.नं. : ७४३७
फोन : ४२२१३६५, ४२४४६३६
ईमेल : ktm@xsc.edu.np



CERTIFICATE OF APPROVAL

The undersigned certify that they have read and recommended to the Department of Computer Science for acceptance, a project report entitled “.....” submitted by (students name) in partial fulfillment of the requirements for the degree of Bachelor of Science in Computer Science and Information Technology awarded by Tribhuvan University.

.....
(Supervisor Name)
Supervisor/Lecturer

.....
External Examiner
Tribhuvan University

.....
Mr. Vishnu Kumar Rana
Head of Department
St. Xavier's College

SPECIMEN-4 (Acknowledgement Sample)

ACKNOWLEDGEMENT

It gives us immense pleasure to express our deepest sense of gratitude and sincere thanks to our highly respected and esteemed guide Er./Mr.(Supervisor name with full designation if any), for his/ her valuable guidance, encouragement and help for completing this work. His/ her useful suggestions for this whole work and co-operative behavior are sincerely acknowledged.

We would like to express our sincere thank to Er./Mr(with full designation and department), for giving us this opportunity to undertake this project. We would also like to thank Er./Mr.(Head of Department name with full designation) for whole hearted support.

We are also grateful to our teachers (teachers name with full designation) for their constant support and guidance.

At the end we would like to express our sincere thanks to all our friends and others who helped us directly or indirectly during this project work.

Student(s) Name with Exam Roll No.

Full Name (T.U. Exam Roll No. 494/066)

Full Name (T.U.Exam Roll No. 506/066)

SPECIMEN-5 (Abstract Sample)

ABSTRACT

The protection of sensitive data that has to be transmitted on the computer network has been the most challenging issue in the field of computer. Cryptographic algorithms play a crucial role in the information society by providing protection from unauthorized access to sensitive data.

Although the security of encryption algorithm like Advanced Encryption Algorithm (AES) is beyond doubt, the limitations in computing power of a personal computer has caused the difficulties for encrypting the data file which is large in size. Hence this system allows encrypting the large files with the existing computational power of the personal computers by the use of grid based computation.

In this research work, a Grid-Based Cryptography application was studied and developed. It is an application that uses the computational resources and power of multiple personal computers in order to encrypt large files. The encryption standard Advanced Encryption Standard (AES) was used as the encryption. Grid nodes were generated for the computation. Grid manager splits the large text file into small file size and distributes them among the available grid nodes. Grid manager constantly checks for untreated file and failure of any grid node. After completing the task, the grid nodes return the cipher text back to the grid manager.

Appendix – 1: Table of Contents

TABLE OF CONTENTS

TITLE	PAGE NO.
Acknowledgement	i
Abstract	ii
List of figures	iii
List of tables	iv
List of symbols	v
Abbreviation	vi
Chapter 1: Introduction 1	
1.1	1
1.2	2
1.2.1	5
1.2.2	12
1.2.2.1	19
1.2.2.2	25
1.2.3	30
1.3	45
1.4	58
.....	60
(Make other chapters in the same format)	
References	100
Appendices	102

Appendix – 2: List of figures

LIST OF FIGURES

Figure Number	Figure	Page No.
Figure 1	State array, input and output	4
Figure 2	AES Encryption and Decryption Architecture	9
Figure 3	S – Box (substitution values for the byte xy, in hexadecimal format)	10
Figure 4	Sub byte transformation	12
Figure 5	Shift Rows Transformation	13
Figure 6	Mix column transformation	14
Figure 7	Add Round Key Operation	18
Figure 8	AES Key Expansion	19
Figure 9	The structure of GTPBE System	26
Figure 10	Architecture of cryptography using Grid Computing	32
Figure 11	Overview of Advance Encryption Standard	33
Figure 12	GridManager is listening the GridNode	34
Figure 13	GridManager is responding a GridNode	34
Figure 14	Architecture of GridManager	34
Figure 15	Chart showing the difference between time using Grid Computing and without it	36

Appendix – 3: List of tables

LIST OF TABLES

Table Number	Table	Page No.
Table 1	AES parameters	4
Table 2	Key Block Round combination	8
Table 3	Data Preparation	31
Table 4	Table showing the encrypted time taken in single machine	35
Table 5	Table showing the encrypted time taken using Grid Computing in 5 machines	36

Appendix – 4: List of symbols

LIST OF SYMBOLS

m	Number of transmit antennas
n	Number of receive antennas
$h_{i,j}$	Channel matrix element
\mathbf{H}	Channel matrix
\mathbf{y}	Received signal
\mathbf{x}	Transmit signal vector
P	Total transmit power
Det	Determinant
N	Diversity order
M	Order of QAM modulation
\mathbf{I}	Identity matrix

Appendix – 5: Abbreviations

ABBREVIATIONS

AES	Advance Encryption Standard
DES	Data Encryption Standard
GF	Galois Field
QoS	Quality of Service
RMI	Remote Method Invocation
S – Box	Substitution Box
GTPBE	Grid and Thread Pool Based Cryptography

Appendix – 6: Format of Body Text

CHAPTER 1: INTRODUCTION

1. 1 Background

The protection of sensitive data that has to be transmitted on the computer network has been the most challenging issue in the field of computer. Cryptographic algorithms play a crucial role in the information society by providing protection from unauthorized access to sensitive data.

Although the security of encryption algorithm like Advanced Encryption Algorithm (AES) is beyond doubt, the limitations in computing power of a personal computer has caused the difficulties for encrypting the data file which is large in size. Hence this system allows encrypting the large files with the existing computational power of the personal computers by the use of grid based computation.

In this research work, a Grid-Based Cryptography application was studied and developed. It is an application that uses the computational resources and power of multiple personal computers in order to encrypt large files. The encryption standard Advanced Encryption Standard (AES) was used as the encryption. Grid nodes were generated for the computation. Grid manager splits the large text file into small file size and distributes them among the available grid nodes. Grid manager constantly checks for untreated file and failure of any grid node. After completing the task, the grid nodes return the cipher text back to the grid manager.

Appendix – 7: Format of References Page

References

- [1] Gaines, Helen Fouché – Cryptanalysis 1939 ISBN 0-486-20097-3.
- [2] Patterson, Wayne. Mathematical Cryptology for Computer Scientists and Mathematicians, Rowman & Littlefield ,1987
- [3] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone – Handbook of Applied Cryptography ISBN 0-8493-8523-7
- [4] Christof Paar and Jan Pelzl – Understanding Cryptography: A Textbook for Students and Practitioners, Springer, 2009, ISBN 978-3-642-04100-6