**ACKNOWLEDGEMENT**

I would like to express my gratitude and appreciation to all those who gave me the possibility to complete this project successfully. First of all I would like to thank our Principal **Dr. Janhavi Inamdar** for her encouragement.

It is my sincere obligation to thank **Dr. Vikas D. Thombre**, Head of Computer Department, who has extended positive support and precious suggestions to make the project work a success.

A special thanks to my guide, **Prof. Dipali Khatri**, whose help, stimulating suggestions and encouragement, helped me to complete my project. I would also like to acknowledge with much appreciation the crucial role of the staff of Computer Department, who gave the permission to use all required resource and the necessary material to complete this project. Special thanks go to my department teachers and my friends, who help me to assemble the required information and gave suggestion about the control systems.

**LIST OF FIGURES**

|  |  |  |
| --- | --- | --- |
| **Figure. No.** | **Name of Figures** | **Page No.** |
| 1. | Abstract View of Software | 9 |
| 2. | Level 0 DFD | 10 |
| 3. | Level 1 DFD | 11 |
| 4. | Package Diagram | 12 |
| 5. | Class Diagram | 13 |
| 6. | Use Case Diagram | 14 |
| 7. | State-chart Diagram | 15 |
| 8. | Sequence Diagram | 16 |
| 9. | Communication Diagram | 17 |
| 10. | Activity Diagram | 18 |
| 11. | Component Diagram | 19 |
| 12. | Key-Block-Round-Combinations | 20 |
| 13. | Sub-Bytes Step | 22 |
| 14. | Shift-Row Step | 23 |
| 15. | Mix-Columns Step | 24 |
| 16. | Algorithm Flowchart | 25 |

**ABBREVIATION**

|  |  |  |
| --- | --- | --- |
| **Sr. No.** | **Abbreviation** | **Long Form** |
| 1. | AES | Advance Encryption Standard |
| 2. | MAC | Media Access Control |
| 3. | DES | Data Encryption Standard |
| 4. | SRS | Software Requirement Specification |
| 5. | NIST | National Institute of Standard and Technology |

**ABSTRACT**

This project is aimed at developing a Three Layer Encryption and Decryption Software using New Key Management and Bluetooth MAC Address. A system based on non-traditional idea that applies symmetric key encryption algorithm to keep your data secure against unauthorized access and undetected mutilation. In order to keep this symmetric key secret the proposed system encrypts this confidential symmetric key with the public cryptographic function. This system also uses the Bluetooth technology as the main technique to personalize communication between elements of the system and key keeper.

Now-a-days security challenges are still among the biggest concerns when considering the privacy of user’s data. This triggered a lot of research activities, resulting in a number of security softwares and proposed softwares targeting the various methods to achieve privacy of the user’s data. Alongside with these security issues, the security paradigm comes with a new set of unique features, which opens the path toward novel security approaches, techniques, and architectures. AES Rijndael Algorithm is one such approach.

This project provides an insight of a proposed software which provides a way for the user’s to protect their valuable data from unauthorized access in any scenario. The aim of the system is to ensure data integrity and confidentiality to the authorized parties only. Various distinct encryption standards are introduced and discussed according to their security and privacy capabilities and prospects.

**CONTENTS**

|  |  |  |
| --- | --- | --- |
| **Chapter No.** | **Chapter Name** | **Page No.** |
|  | Acknowledgement | i |
|  | List of Figures | ii |
|  | Abbreviations | iii |
|  | Abstract | iv |
|  | Contents | v |
| 1. | Introduction | 1 |
| 2. | Motivational Survey | 2 |
| 3. | Problem Definition And Scope | 3 |
|  | 3.1 Problem Statement | 3 |
|  | 3.2 Statement of Scope | 3 |
|  | 3.3 Goals and Objectives | 3 |
| 4. | Software Requirement Specification | 4 |
|  | 4.1 Introduction | 4 |
|  | 4.1.1 Scope for development of the project | 4 |
|  | 4.1.2 Overview of responsibility of developer | 4 |
|  | 4.2 General Description | 5 |
|  | 4.2.1 User Characteristics | 5 |
|  | 4.2.2 Product Perspective | 5 |
|  | 4.2.3 Overview of Functional Requirements | 5 |
|  | 4.2.4 Non Functional Requirements | 6 |
|  | 4.3 User View of Product Use | 6 |
|  | 4.4 Specific Requirements | 7 |
|  | 4.4.1 External Interface Requirements | 7 |
|  | 4.4.2 Quality Attributes | 7 |
| 5. | System Design Document | 8 |
|  | 5.1 Introduction | 8 |
|  | 5.1.1 Purpose and Scope | 8 |
|  | 5.2 Target Audience | 8 |
|  | 5.3 Pre - Requisites | 9 |
|  | 5.4 Architectural Strategies | 9 |
|  | 5.5 Logical Views | 9 |
|  | 5.6 Data Flow Diagrams | 10 |
|  | 5.7 UML Diagrams | 12 |
| 6. | Algorithmic Strategies | 20 |
|  | 6.1 Introduction | 20 |
|  | 6.2 Algorithm Specification | 21 |
|  | 6.2.1 The SubBytes Step | 22 |
|  | 6.2.2 The ShiftRows Step | 23 |
|  | 6.2.3 The MixColumns Step | 23 |
|  | 6.2.4 The AddRoundKey Step | 25 |
| 7. | Test Specification | 26 |
|  | 7.1 Introduction | 26 |
|  | 7.2 Purpose of the Document | 26 |
|  | Advantages | 27 |
|  | Limitations | 27 |
|  | Conclusion | 28 |
|  | Future Enhancement | 29 |
|  | Annexure |  |
|  | Annex A: Laboratory assignments on project analysis of algorithmic design |  |
|  | Annex B: Laboratory assignments on project quality and reliability testing of project design |  |
|  | Annex C: Project planner and progress report. |  |
|  | Annex D: Paper published |  |
|  | References(IEEE Format) | 30 |