**Abstract**

Cryptography is knowledge of sending information securely over the network. RSA is a well-known cryptic algorithm used worldwide. For providing confidentiality in the network and to improve the security of RSA algorithm, development and implementation of Modified RSA (MREA) algorithm was done. The project aims at providing a better counterpart of the above two algorithms on the basis of the time complexity and security. It is the most advantageous solution for the security of information in computer network.

The proposed method tries to decrease the time taken by the MREA for encryption and decryption. This is done with the help of Offline Storage and Big Integer library. Offline storage basically means generation of keys prior to the commencement of the encryption process and stores it in a database.

Use of Big Integer library aims at using pre-defined functions so as to decrease the time taken by the MREA algorithm. The proposed system will be using these two techniqes so as to get better result. MREA is one of the strongest algorithm when it comes to security but the time taken by it make the algorithm impractical for general usage. So the basic focus of this system will be to decrease the time taken in the entire process taking the help of above mentioned techniques in creating a better cryptic algorithm.

**ACKNOWLEDGEMENT**

We are grateful to our guide Mr. Sankusu Sharma Sir and Head of Department of Computer Engineering, Mrs. Neeta Patil Madam who has extended all valuable guidance, help and constant encouragement through various difficult stages for the development of the project.

We would like to thank Mr. Gunashekar Sir and Mrs. Anita Sunderajan Madam for their valuable suggestions and guidance.

We express our sincere gratitude to our respected Principal Dr. Satish Takalikar Sir for encouragement and facilities provided to us.

We would also like to acknowledge the patience that our ever beloved parents have shown during our efforts and the encouragement we have received from them.

Thus we are fully obliged and convey our thanks to the all the teaching as well as the non-teaching staff of the department. Special thanks to all the lab assistants for their constant support to solve any technical issues.

Last but not the least we would like to thank all direct and indirect identities of the college with whom we took the strides for this successful project.

**Joel Akshay Ulahanna**

**Neil Periera**

**Sneha Susan Varghese**

**TABLE OF CONTENTS**

|  |  |  |
| --- | --- | --- |
| **Ch No** | **Contents** | **Pg No** |
| **1.0** | **Introduction**  1.1 Motivation  1.2 Problem statement  1.3 Scope of the project | **1**  1  2  2 |
| **2.0** | **Literature Survey**  2.1 Existing System  2.2 RSA  2.3 MREA | **3**  3  4  5 |
| **3.0** | **Software Requirement Specification**  3.1 Introduction  3.1.1 Purpose  3.1.2 Scope  3.1.3 Overview  3.2 Definitions, Acronyms And Abbreviations  3.3 Overall Description  3.3.1 Product Perspective  3.3.1.1 System Interfaces  3.3.1.2 User Interfaces  3.3.2 Product Functions  3.3.3 General Constraints  3.4 Specific Requirements    3.4.1 External Interface Requirements  3.4.1.1 User Interfaces  3.4.1.2 Encryption Algorithm  3.4.2 Functional Requirements  3.4.2.1 View Messages  3.4.2.2 View Console  3.4.3 Non-Functional Requirements  3.4.3.1 User Interface  3.4.3.2 Deployment Platform  3.4.4 Software System Attributes | **6**  6  6  6  6  7  13  13  13  13  14  14  14  14  14  14  15  15  15  15  15  15  16 |
| **4.0** | **Requirements Gathering And Analysis**  4.1 Requirement Elicitation  4.2 Feasibility study  4.2.1 Technical feasibility  4.2.2 Economical feasibility  4.3 Requirement Analysis | **18**  18  19  19  19  20 |
| **5.0** | **Design**  5.1 UML diagrams | **21**  21 |
| **6.0** | **Proposed System**  6.1 Architectural diagram | **26**  26 |
| **7.0** | **Implementation**  7.1 Algorithm  7.2 Technology used  7.3 Project WBS chart | **27**  27  28  30 |
| **8.0** | **Result and Discussions** | **31** |
| **9.0** | **Conclusion and Further Work** | **37** |
| **10.0** | **References** | **38** |
| **11.0** | **Appendix** | **39** |

**LIST OF FIGURES**

|  |  |  |
| --- | --- | --- |
| **Fig. No** | **Name of Figure** | **Page No** |
| **1** | **Use Case diagram** | **17** |
| **2** | **Block diagram** | **19** |
| **3** | **Activity diagram** | **21** |
| **4** | **Sequence diagram** | **22** |
| **5** | **State Chat diagram** | **23** |
| **6** | **Class diagram** | **24** |
| **7** | **Data Flow diagram** | **25** |
| **8** | **Architecture diagram** | **26** |
| **9** | **WBS Chart** | **30** |
| **10** | **Static Encryption Comparison Graph** | **31** |
| **11** | **Static Decryption Comparison Graph** | **32** |
| **12** | **Home page** | **34** |
| **13** | **RSA Output** | **34** |
| **14** | **MREA Output** | **35** |
| **15** | **JNS Output** | **35** |
| **16** | **Encryption Graph** | **36** |
| **17** | **Decryption Graph** | **36** |

**LIST OF TABLES**

|  |  |  |
| --- | --- | --- |
| **Table No.** | **Table Name** | **Page No.** |
| **1** | **Use Case Description** | **18** |
| **2** | **Abbreviations** | **39** |