**ACKNOWLEDGEMENT**

We dedicate this page to acknowledge and thank those responsible for the shaping of the project. Without their guidance and help, the experience while constructing the dissertation would not have been so smooth and efficient.

We are extremely thankful to our **Principal Dr. Shantharama Rai C.** for his support and encouragement.

We owe our profound gratitude to **Dr. Antony P J, Head of the Department**, Computer Science and Engineering, whose kind consent and guidance helped us to complete this work successfully.

We sincerely thank **Mrs. Saranya Babu, Mr. Pradeep Kumar, Assistant Professor**, Computer Science and Engineering, for their guidance and valuable suggestions which helped us to fulfill the experiments prescribed by the university.

We would like to thank all our Computer Science and Engineering staff members who have always been with us extending their support, precious suggestions, guidance and encouragement through the project.

We also like to extend thanks to our friends and family members for their continuous support.

**ABSTRACT**

The main objective of this project is to graphically illustrate the visualization of Diffie-Hellman key exchange algorithm. It is used to secure a variety of Internet services. This algorithm allows two parties who have not previously met to securely establish a key in which they can use to secure their communication. The method was followed shortly by RSA, an implementation of public-key cryptography using asymmetric algorithms.

The Diffie-Hellman key exchange was one of the most important developments in public-key cryptography and it is still frequently implemented in a range of today’s different security protocols. Diffie-Hellman key exchange is frequently implemented in security protocols such as TLS, IPsec, SSH, PGP, and many others. This makes it an integral part of our secure communications. As part of these protocols, the Diffie-Hellman key exchange is often used to help secure your connection to a website, to remotely access another computer, and for sending encrypted emails. Technically, the Diffie-Hellman key exchange can be used to establish public and private keys. These keys can then be used with symmetric-key algorithms to transmit information in a protected manner. Symmetric algorithms tend to be used to encrypt the bulk of the data because they are more efficient than public key algorithms.

**CONTENTS**

**Sl.No Title**  **Pg.No**

**Acknowledgement…………………………………………………………………………i**

**Abstract……………………………………………………………………………………ii**

**1. Introduction…………………………………………………………………………….1**

1.1 Computer Graphics……………………………………………………………… 1

1.2 OpenGL………………….………………………………………….………….....2

1.3 Problem Statement………………………………………………………………..2

1.4 Overview of the Project…………………………………………………………...3

1.5 Applications of Diffie Hellman key exchange……………………………………3

**2. Software Requirement Specification…………………………………………….........4**

2.1 Functional Requirements………………………………………………...............4

2.2 Non Functional Requirements…………………………………………………...4

2.3 Hardware Requirements………………………………………………................4

2.4 Software Requirements……………………………………………………….....4

**3. System Design.……...……………………………………………………….................5**

3.1 Flowchart……………………………………………………………………......5

**4. Implementation………………………………………………………………….........7**

4.1 Description of Implementation Modules..……………………………………....7

4.2 Implementation of OpenGL built in functions………………………………….7

4.3 Implementation of OpenGL User defined functions……………………………9

4.4 Code Snippet……………………………………………………………………10

**5. Testing………………………………………………………………………………...13**

5.1 Testing………..…………………………………………………………………13

5.2 User Interface Testing……………………………………………………..........13

5.3 System Testing………………………………………………………………….13

5.4 Performance…………………………………………………………………….13

**6. Results………………………..………………………………………………………. 14**

**7. Conclusion and Future Enhancement……………...………………………………. 19**

**References………………………………………………………………………………..20**

**LIST OF FIGURES**

**Figure No. Title Pg.No**

Figure 3.1 Flowchart………………………………………...………..........................5

Figure 6.1 Project Title……………………………………………………………….14

Figure 6.2 Menus……………………………………………………………………..14

Figure 6.3 Parties before communication…………………………………………….15

Figure 6.4 Exchange of public keys…………………………………………………..15

Figure 6.5 Selection of private key…………………………………………………...16

Figure 6.6 Mixing of two different keys……………………………………………...16

Figure 6.7 Exchange of private keys………………………………………………….17

Figure 6.8 Adding private keys……………………………………………………….17

Figure 6.9 Connection establishment…………………………………………………18

Figure 6.10 Quit option…………………………………………………………………18

**LIST OF TABLES**

**Table No. Title Pg. No.**

Table 5.1 Test Cases…….………..……………………………..................................13