**DEVELOPMENT ENCRYPTION -SECURE COMMUNICATION USING PUBLIC KEY AND SYMMETRICKEY**

A Dissertation submitted to the Bharathidasan University

In Partial fulfillment of the requirements for the

Award of the degree of

**Master of Science**

**Information Technology**

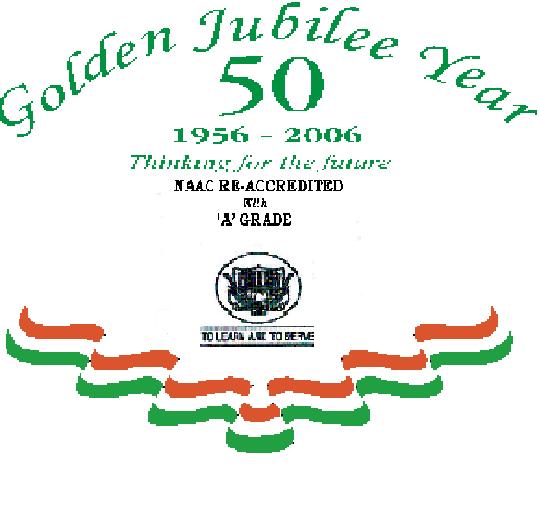
Submitted By,

**G.TAMILKODI**

**Reg.No.09IT455**

Guided By

**Miss.M.LOGESHWARI M.Sc., M.Phil,**



**DEPARTMENT OF COMPUTER SCIENCE**

**A.V.V.M SRI PUSHPAM COLLEGE (AUTONOMOUS)**

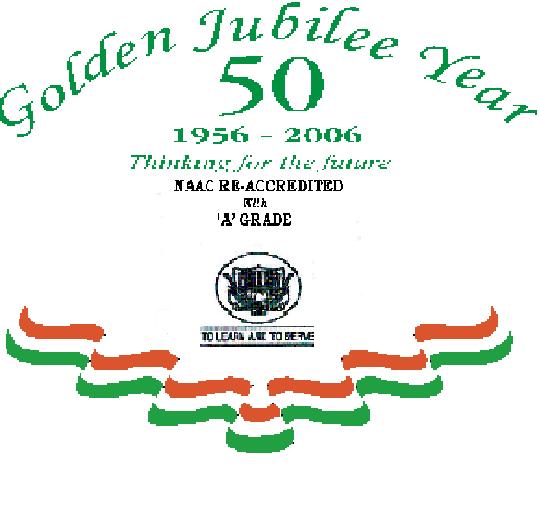
**(NAAC RE- ACCREDITED WITH “A” GRADE)**

**POONDI-THANJAVUR-613 503**

**A.V.V.M SRI PUSHPAM COLLEGE**

**(AUTONOMOUS)**

**(NAAC RE- ACCREDITED WITH “A” GRADE)**



**DEPARTMENT OF COMPUTER SCIENCE**

**BONAFIDE CERTIFICATE**

This is to certified that this project report work done under my guidance, and dissertation entitled “**ENCRYPTION - SECURE COMMUNICATION USING PUBLICKEYAND SYMMETRICKEY ” submitted** by **G.TAMILKODI (REGNO: 09IT455)** In partial fulfillment of the require for the M.SC (IT), Degree course for the academic year 2009-2011 in the subject information technology is the original work of the candidates.

Submitted for viva-vice examination held on \_\_\_\_\_\_\_\_\_\_\_\_ at A.V.V.M Sri Pushpam College, Poondi.

Signature of Guide, Signature of coordinator,

Miss.M. LOGESHWARI, M.Sc., M.Phil. Dr.R.SIVAKUMAR, Ph.D.,

Lecturer in computer science, Coordinator ofcomputer science

A.V.V.M Sri Pushpam College, A.V.V.M Sri Pushpam College,

Poondi. Poondi.

Examiners

Date: 1.\_\_\_\_\_\_\_\_\_\_\_\_

Place: Poondi 2.\_\_\_\_\_\_\_\_\_

**ACKNOWLEDGEMENT**

Words can never simply express the deep sense of gratitude. Have for my institutionpre-dominant by itself – A.V.V.M. Sri Pushpam College, kindest of all, which has provided me the opportunity to pursue my PG Level Education.

I owe my thanks to the Principal **Dr. S. Chinnaiyan Ph.D.,** A.V.V.M. Sri Pushpam College, Poondi for allowing me to do this project work in partial fulfillment of the Degree of Master of Computer Science.

I express my hearty thanks to **Dr R. Sivakumar Ph.D.,** and Coordinator of Computer Science Department.

I express my gratitude to **Miss.M.Logeshwari M.Sc., M.Phil.** Lecturer in Computer Science Department for his timely suggestion, able guidance and painstaking interest at every stage of this project.

I sincerely, thank all the Staff members of Computer Science Department. A.V.V.M. Sri Pushpam College, Poondi. My hearty thanks to one and all those who stood by me to mould this Project properly.

**SYNOPSIS**

**Encryption -Secure Communication Using Public Key and**

**Symmetric key**

The project “**Encryption -Secure Communication Using Public Key and Symmetric key** is designed using Active Server Pages .NET with Microsoft Visual Studio.Net 2008 as front end which works in.Net framework version 2.0. The coding language used is C# .Net

Cryptography is one of the most important security technologies which used to secure the data transmission and the data itself. As the time and challenge growth, the cryptography also grows up with variety of encryption techniques and algorithms. Among the algorithms, one of the most popular is the RSA. This thesis concentrates on the study of the PKI concept generally and the RSA algorithm specifically. Furthermore, through this thesis we developed the prototype of chat using Java Programming Language. The development process follows the seven systematic phases of system development life cycle. At the end of the development, the prototype of the application is come out readily to be tested. The prototype only covers the transmitting and receiving chat messages between two parties (client and server).Each message, it should be able to decrypt the cipher text back to the original plaintext. This thesis actually is just a beginning step to discover the PKI system. The PKI system is very complex and complicated. More resource, energy and time are needed to develop a complete PKI system. Hopefully this thesis can be a stepping stone to go further and deeper in the world of information security, focusing on encryption within PKI environment.

The prototype only covers the transmitting and receiving chat messages between two parties (client and server).Each message, it should be able to decrypt the cipher text back to the original plaintext. This thesis actually is just a beginning step to discover the PKI system. The PKI system is very complex and complicated. More resource, energy and time are needed to develop a complete PKI system. Hopefully this thesis can be a stepping stone to go further and deeper in the world of information security, focusing on encryption within PKI environment.

**Contents**

|  |  |  |
| --- | --- | --- |
| **CHAPTER** | **INDEX** | **PAGE NO** |
| **1.** | **introduction** |  |
| **2.** | **SOFTWARE PROJECT PLAN** |  |
| **3.** | **CUSTOMER REQUIREMENTSDETERMINATION**  **3.1 Existing Proposed System**  **3.2 Proposed System** |  |
| **4.** | **Software requirements SPECIFICATION**  **4.1 Functional Requirements**  **4.2 Performance Requirements**  **4.3 Interface Requirements**  **4.4 Operational Requirements**  **4.5 Resource Requirements**  **4.6 Security Requirements**  **4.7 Design Requirements**  **4.8 Quality and reliability Requirements** |  |
| **5.** | **System Analysis**  **5.1 Data Flow Diagram**  **5.2 ER Diagram**  **5.3 Use Case Diagram**  **5.4 Software development lifecycle** |  |
| **6.** | **System design**  **6.1 Input Design**  **6.2 Output Design**  **6.3 Interface Design**  **6.4 Table And Database Design**  **6.5 Front-end Design**  **6.6 Back-end Design**  **6.7 Algorithm** |  |
| **7.** | **CODING** |  |
| **8.** | **System testing**  **8.1 Unit Testing**  **8.2 Integration Testing**  **8.3 Validation Testing**  **8.4 Verification Testing**  **8.5 User Acceptance Testing** |  |
| **9.** | **PrOBLEMS FACED** |  |
| **10.** | **FUTURE PLANS** |  |
|  | **Conclusion** |  |
|  | **appendix** |  |
|  | **REFERENCES** |  |
|  | **BIBLIOGRAPHY** |  |