

CERTIFICATE



DELHI TECHNOLOGICAL UNIVERSITY
BAWANA ROAD, DELHI – 110042

Date: _____

This is to certify that dissertation entitled “**A Remote Authentication Methodology for Secure Communication in Distributed Network**” has been completed by **Himanshu Mittal, University Roll No. 06/SWE/2010** in partial fulfillment of the requirement for the award of **Master of Technology in Software Engineering** at **Delhi Technological University, Delhi**.

This thesis is a record of his own work carried out by him under my supervision and support during the academic session 2011-2012. The matter embodied in this thesis is original and has not been submitted for the award of any other degree.

(Dr. DAYA GUPTA)
HOD & PROJECT GUIDE
DEPT. OF COMPUTER ENGINEERING
DELHI TECHNOLOGICAL UNIVERSITY
BAWANA ROAD, DELHI – 110042

ACKNOWLEDGEMENT

It is a great pleasure to have the opportunity to extend my heartiest felt gratitude to everybody who helped me throughout the course of this project.

It is distinct pleasure to express my deep sense of gratitude and indebtedness to my project guide **Dr. Daya Gupta, Professor, Head of Department, Department of Computer Engineering, Delhi Technological University**, for her invaluable guidance, encouragement and patient reviews. With her continuous inspiration only, it becomes possible to complete the project.

I would also like to take the opportunity to present my sincere regards to **Mrs. KAKALI CHATTERJEE, Research Scholar, Department of Computer Engineering, Delhi Technological University**, for their technical support and encouragement throughout the program.

I would also like present my sincere regards to all the faculty members of the Department for their constant support and encouragement.

I am grateful to my parents for their moral support all the time. They have been always around to support me in all the way. I am also thankful to my classmates for their unconditional support and motivation during this work.

HIMANSHU MITTAL

M.Tech (Software Engineering)

Roll No. 06/S.W.E./2010

Department of Computer Engineering

Delhi Technical University, Delhi

(Formerly Delhi College of Engineering)

ABSTRACT

With the fast development of network technologies, increasing number of services are provided through internet instead of traditional ways. Owing to the openness of the internet, method of guarding valuable resources from unauthorized access is as essential the data/services itself.

To facilitate a legal user, to access a distant server in distributed environment for utilizing various information resources and services available on the multi-server network, we propose “A Remote Authentication Methodology for Secure Communication in Distributed Network”.

This scheme is based on one-way hash function, XOR function and Diffie-Hellman. It provide more security, reduce the computational and communication cost and is less complex. It uses an authentication center, that consists of multiple servers registered on it and allow the remote users to securely and efficiently get authenticated and generate session key with the desired server. The User registers only once with the authentication center and can obtain the services from multiple servers without repeating registration process on every individual server.

The proposed scheme has many advantages such as no encryption, signature, verification tables, timestamps and public keys directory are needed to be maintained. Also the proposed scheme is invulnerable to the security attacks such as insider attack, man-in-the-middle attack, forward security, impersonation attack, replay attack and safe guard from many possible attacks effectively.

TABLE OF CONTENTS

Certificate.....	ii
Acknowledgement.....	iii
Abstract.....	iv
Table of Content.....	v
List of Figures.....	ix
List of Tables.....	xi
Chapter 1 Introduction	1
1.1 Motivation	2
1.2 Related Work	3
1.3 Problem Statement	4
1.4 Scope of Work	5
1.5 Organization	6
Chapter 2 Literature Survey	9
2.1 Objective	9
2.2 State of Art	9
2.3 Related Work of Cryptography	10
2.3.1 Cryptography	10

2.3.1.1 Two Kinds of Cryptography Systems	10
2.3.1.2 Symmetric Key Cryptography–An Overview	11
2.3.1.3 Asymmetric Key Cryptography–An Overview	12
2.3.2 Diffie-Hellman Key Exchange Protocol	13
2.4 Mathematical Overview	14
2.4.1 Groups	14
2.4.2 Modular Arithmetic	14
2.4.3 Additive Inverse	15
2.4.4 Multiplicative Inverse	15
2.4.5 Generator ‘g’	15
2.4.6 Cyclic Group	15
2.4.7 Euler’s Totient function ‘ $\phi(n)$ ’	16
2.4.8 Order of the Group	16
2.4.9 Order of the Element	16
2.4.10 Primitive Root	16
2.4.11 Diffie-Hellman Key Exchange Protocol	17
2.5 Various Authentication Schemes for Distributed Network	18
Chapter 3 Methodology	24
3.1 System Framework	24
3.2 Proposed Methodology	26
3.2.1 Server Registration Phase	27
3.2.2 User Registration Phase	28

3.2.3 Authentication of Remote User and Server	29
3.2.4 Mutual Authentication and Session Key Generation	34
Chapter 4 Analysis	41
4.1 Security Analysis	41
4.2 Performance Analysis	46
Chapter 5 Implementation of Proposed Methodology	47
5.1 Development Environment	47
5.1.1 .Net Framework	47
5.1.2 Visual Studio	48
5.1.3 C#	48
5.2 Procedure for Implementation of Proposed Methodology	49
5.2.1 Procedure for Group Generator	50
5.2.2 Procedure for Hash and XORing Operation	50
5.2.3 Procedure for Power operation using Square and Multiply	50
5.2.4 Procedure for Sending Data	51
5.2.5 Procedure for Receiving Data	52
5.2.6 Procedure for Mutual Key	52
5.2.7 Procedure for Session key	53
5.2.8 Procedure for Encrypting Data	53
5.2.9 Procedure for Decrypting Data	53
5.2.10 Procedure for Diffie-Hellman Key Exchange	54

5.3 Results	54
5.1.1 Server Registration	54
5.1.2 User Registration	56
5.1.3 Authentication of Remote User and Server and Mutual Authentication and Session Key Generation	58
Chapter 6 Conclusion and Future Work	63
6.1 Conclusion of the Thesis	63
6.2 Future Work	64
Chapter 7 References and Bibliography	65
Appendix A	70

LIST OF FIGURES

Figure 2.1: Symmetric Key Cryptography - Encryption Process.....	11
Figure 2.2: Symmetric Key Cryptography - Decryption Process.....	11
Figure 2.3: Asymmetric Key Cryptography - Encryption Process.....	12
Figure 2.4: Asymmetric Key Cryptography - Decryption Process.....	12
Figure 3.1: System Framework.....	25
Figure 3.2: Server Registration Phase.....	27
Figure 3.3: User Registration Phase.....	28
Figure 3.4: Authentication Phase.....	40
Figure 5.1: Authentication Center(Server Registration).....	56
Figure 5.2: Server 'asd' Registration.....	56
Figure 5.3: Server 'abc' Registration.....	57
Figure 5.4: Authentication Center(User Registration).....	58
Figure 5.5: User Registration.....	58
Figure 5.6: Authentication Center.....	59
Figure 5.7: Target Server Session Key.....	60
Figure 5.8: User Session Key.....	61
Figure 5.9: Session Key Generated.....	62
Figure 5.10: User encrypting data using session key.....	62

Figure 5.11: Server decrypting data using session key.....63

LIST OF TABLES

Table 3.1: Notations.....	26
Table 4.1: Security Properties.....	46