**Declaration**

Title of Project Report – Security System for DNS using Cryptography

I understand what plagiarism is and am aware of the University’s policy in this regard.

I declare that

1. The work submitted by me in partial fulfilment of the requirement for the award of degree Bachelor of Technology assessment in this Minor Project is my own; it has not previously been presented for another assessment.
2. I declare that this Minor Project is my original work. Wherever work from other source has been used, all debts (for words, data, arguments and ideas) have been appropriately acknowledged and referenced in accordance with the requirements of NTCC Regulations and Guidelines.
3. I have not used work previously produced by another student or any other person to submit it as my own.
4. I have not permitted, and will not permit, anybody to copy my work with the purpose of passing it off as his or her own work.
5. The work confirms to the guidelines for layout, content and style as set out in the Regulations and Guidelines.

Date: 19/12/15 Ujjwal Pengoria

A7605212020

B.Tech CSE

**Certificate**

I hereby certify that

1. Ujjwal Pengoria, A7605212020 student of B.Tech CSE batch 2012-2016 at ASET, Amity University Uttar Pradesh has completed the Project Report on “Security System for DNS using Cryptography”, under my supervision.
2. The presented work embodies original research work carried out by the student as per the guidelines given in University Regulations.
3. The research and writing embodied in the thesis are those of the candidate except where due reference is made in the text.
4. I am satisfied that the above candidate’s, prima facie, is worthy of examination both in terms of its content and its technical presentations relative to the standards recognized by the university as appropriate for examination.
5. I certify that in accordance with NTCC guidelines, the report does not exceed the prescribed maximum word limit; or Prior approval has been sought to go beyond the word limit.
6. Wherever work from other source has been used, all debts (for words, data, arguments and ideas) have been appropriately acknowledged and referenced in accordance with the requirements of NTCC Regulations and Guidelines.

--------------------------------------

Mr. Shashwat Shukla

Assistant Professor

Department of CSE, AUUP, Lucknow

**Acknowledgment**

Before I proceed further, I would like to spent some time in expressing my gratitude to all those who have been involved in guiding me out during the entire curriculum.

I wish to express my most sincere and profound gratitude **Dr. Deepak Arora, HOD, Computer Science and Engineering Department, ASET, Amity University Lucknow,** for giving me inspiration and requisite facility by giving me a chance to show my capabilities and also for making me feel comfortable in the strictly professional environment of the college premises.

**I am also thankful to Mr. Shashwat Shukla, Assistant Professor, Computer Science and Engineering Department, ASET, Amity University Lucknow,** for his guidance throughout the work with his help and suggestions. I am also grateful to him for cooperation in providing with all required resources.

I extend special thanks to my friends and family for their constant support.

This work could not have been completed without the help of the above mentioned people.

**Name of student – Ujjwal Pengoria**

**Date – 19/12/15**

**Abstract**

The mapping or binding of IP addresses to host names has become a major problem in the rapidly growing internet and the higher level binding effort went through different stages of development up to the currently used Domain Name System (DNS).

The DNS Security is designed to provide security by combining the concept of both the Digital Signature and Asymmetric key (Public key) Cryptography, here the public key is sent instead of private key. The DNS security uses Message Digest Algorithm to compress the message (text file) and PRNG(Pseudo Random Number Generator) Algorithm for generating public and private key. The message combines with the private key to form a signature using DSA Algorithm, which is sent along with the public key.

The receiver uses the public key and DSA Algorithm to form a signature. If this signature matches with the signature of the message received, the message is decrypted and read else discarded.

**Table of Contents**

**Declaration i**

**Certificate ii**

**Acknowledgement iii**

**Abstract iv**

**Table of Contents v**

**List of Figures vii**

**List of Tables viii**

**1. Introduction 1**

1.1 Scope of project 1

1.2 Problem Statement 2

**2. Overview of DNS 3**

2.1 Fundamentals of DNS 4

2.1.1 The Domain Name Space 4

2.1.2 DNS Components 6

2.2 Proposed System 6

**3. Future Implementation Steps 8**

**4. JAVA Swings 11**

4.1 Swing Features 11

4.2 Swing Controls 11

4.2.1 Swing UI Elements 12

4.2.2 Swing Layouts 13

4.2.3 Swing Event Handling 14

**5. Development Environment 15**

5.1 Hardware Environment 15

5.2 Software Environment 15

**6. Testing 16**

6.1 System Testing Requirements 16

6.2 Phases of Testing 16

6.2.1 Unit Testing 16

6.2.2 Integration Testing 16

6.2.3 System Testing 17

6.2.4 Performance Testing 17

6.2.5 Validation Testing 17

**7. Conclusion 18**

**References 20**

**List of Figures**

**FIGURES: PAGE NO.**

**1)** Domain Name Space Example 5

**2)** Example of inverse domain and the DNS 6

**3)** Authentication Process 8

**4)** Message Encryption Process 9

**5)** Key Generation Process 9

6) Signature Generation Process 10

**7)** Verifying Signature & Decryption Process 10

**List of Tables**

**FIGURES: PAGE NO.**

**1)** Swing Using Element 12-13

**2)** Layout Manager 13-14

**3)** Hardware Requirements 15

**4)** Software Requirements 15