**A**

**Minor Project Report**

**on**

**Security System for DNS Using Cryptography**

**Govt. Engineering College Bikaner**

**In Partial Fulfillment of**

**Bachelor of Technology**

**CSE/IT IV Year VII Semester**

**(Rajasthan Technical University, Kota)**

****

Submitted by

**HAWA SINGH**

**14EEBCS027**

**MADHUR DHODARIA**

**14EEBCS038**

**ASHOK KUMAR**

**14EEBCS014**

Submitted To:-

**HEAD**

**Department of Computer Science & Engg. / IT**

**Govt. Engineering College Bikaner**

**(An Autonomous Institute of Govt. of Rajasthan)**

**Appendix I**

**Govt. Engineering College Bikaner**

**Department of Computer Science & Engg. / IT**

**AKNOWLEDGEMENT**

This is opportunity to express my heartfelt words for the people who were part of this seminar in numerous ways, people who gave me unending support right from beginning of the training seminar report.

I am grateful to seminar guide “Mr. Ranu Lal Chouhan “ for giving guidelines to make the training seminar successful.

I want to give sincere thanks to the principal, **Prof. Dinesh Shringi,** sir for his valuable support.

I extend my thanks to **Mr. Maninder Singh Nehra,** HOD CSE Department for his cooperation and guidance.

Yours Sincerely,

Hawa Singh

Ashok Kumar

Madhur Dhodaria

|  |  |  |
| --- | --- | --- |
| **Sr. No.** | **Content** | **Page No.** |
|  | Abstract |  |
|  |  |  |
| 1 | **Introduction**   1. Scope Of Project 2. Problem Statement |  |
| 2 | **Overview Of DNS and DNSSEC**   1. Fundamental Of DNS    1. The Domain Name Space    2. DNS Component    3. DNS Transaction    4. Proposed System 2. DNSSEC    1. DNSSEC Objective    2. Performance Considerations    3. DNSSEC Scope    4. Key Distribution    5. Data Origin Authentication    6. DNS Transaction and Request Authentication    7. DNSSEC Resource Records    8. KEY RR    9. SIG RR    10. SIGRR |  |
| 3 | **Implementation of Security System For DNS Using Cryptography Algorithms**   1. Source Code 2. Server 3. Destination 4. RSA Key Desing 5. RSA Key Decryption |  |
| 4 | 1. Result |  |
| 4 | Conclusion and Future  Reference |  |

**SECURITY SYSTEM FOR DNS USING CRYPTOGRAPHY**

ABSTRACT

The mapping or binding of IP addresses to host names became 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 send 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 send 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.