# **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.

# **4. DEVELOPMENT ENVIRONMENT**

# **4.1 HARDWARE ENVIRONMENT**

The minimum configuration required to run this project are:

1. Main processor : Pentium III (or) IV
2. RAM : 128MB
3. Hard Disk : 4.2GB
4. Clock Speed : 550 MHZ
5. System Bus Speed : 400 MHz
6. Cache RAM : 256 KB

# **4.2 SOFTWARE ENVIRONMENT**

Language : JDK1.3 (or) Higher.

Front End Design : Swings

Operating System : Windows