**A Cryptology-based Approach for Web Information Security**

**Objective:**

The main objective of this project (Crypto Log) is to send the confidential details and related confidential files and documents to their recipients in a securable way. Crypto log will use the numerous kinds of algorithms to generate the encrypted strings, files and decrypted strings, files.

The Secure Sockets Layer (SSL) is a common Encryption protocol used in Crypto log. When you see a URL in your Web browser that starts with "https" instead of "http", it is a secure connection that is using SSL. Some methods of cryptography used a "secret key" to allow the recipient to decrypt the message. The most common secret key cryptosystem is the Data Encryption Standard (DES), or the more secure Triple-DES which encrypts the data three times.

The purposeful algorithms used by Crypto log will be in the forms of:

1. MD5

2. SHA1

3. RijndaelManaged

**Existing System:**

1) In Existing system, the data will be secure through the network because data transmission is done in encrypted format.

2) In Existing system, data will not be accessed through the authorized person.

3) The system does not provide security to the data store in database.

4) In Existing System, the security is not provided throughout the server and database.

**Proposed System:**

1) In Proposed System, the data will be secure using the web technology by using https enabled.

2) In Proposed System, the data will be accessed through the authorized person.

3) The system provides security to the data store in the database.

4) In Proposed System, the security is provided throughout the server and database by disabling the cookies etc.

The Cryptology has been divided into 5 different modules:

1. Administrator

2. User

3. Cryptic messages

4. Cryptic files

5. Image transformation

**Administrator:**

Administrator is a super user in the system. He will monitor all the users’ activities in the system. He has privileges to do anything at any point of time. He is responsible for providing secure mechanism for the user of the system to send their confidential data in a secure way.

**User**:

User will register in to site and send his confidential data in a secured way by using Crypto log technology facility provided in the application.

**Cryptic messages:**

In this module user will send his confidential messages in an encryption format so that receiver will receive the data and he will decrypt to get original data. So that data will transmit in a secure way.

**Cryptic files**:

In this module user will send data file in an encryption format so that receiver will receive the data and he will decrypt to get original data. Application provides a facility to send files in a secured way.

**Image transformation:**

In this module user will transmit data in the form of image and he can encrypt the image and transform to receiver. Receiver will receive the data and he will decrypt to get original data. By using this application user can send images also in a secured way.

**Software Requirements:**

Operating System : Windows XP/2003 or Linux/Solaris

User Interface : HTML, CSS

Client-side Scripting : JavaScript

Programming Language : Java

Web Applications : JDBC, JNDI, Servlets, JSP

IDE/Workbench : My Eclipse

Database : Oracle10g

Server Deployment : Tomcat

# Hardware Requirements:

Processor : Core 2 Duo

Hard Disk : 160GB

RAM : 1 GB