SECURE COMMUNICATION SYSTEM

By

G.NITHYA
Reg No: 71202621024
of
KUMARAGURU COLLEGE OF TECHNOLOGY
COIMBATORE - 641006

A PROJECT REPORT
Submitted to the

FACULTY OF INFORMATION AND COMMUNICATION ENGINEERING

In partial fulfillment of the requirements
for the award of the degree
of

MASTER OF COMPUTER APPLICATION

June, 2005

BONAFIDE CERTIFICATE

Certified that this project report titled

SECURE COMMUNICATION SYSTEM

Is Bonafide work of

Ms. G.NITHYA (Reg. No: 71202621024)

Who carried out the research under my supervision Certified further, that to the best of my knowledge the work reported herein does not form part of any other project report or dissertation on the basis of which a degree or award was conferred on an earlier occasion on this or any other candidate.

Project Guide

Head of the Department

We examined the Candidate with University Register No. 71202621024

in the project Viva-Voce examination held on 24-06-2005

Internal Examiner

External Examiner

24/6/05

ABSTRACT

This project entitled "SECURE COMMUNICATION SYSTEM" aims at Digital Signature, which helps in authenticating users. The encryption package helps in Transferring and Receiving secure data between users.

The server has the right to generate the keys for different users. The key is used to authenticate the users when they get connected to the server. The digital signature is verified in the client system, whether the user has the right key. The user authenticated by the server can communicate with any authenticated users connected in the network.

The project is divided into 6 modules which are given below.

- Message management system
- Encryption and Decryption algorithm maintenance system
- Public and Private Key maintenance system
- Hashing Techniques system
- Attaching Digital Signature system
- Received message verification system

This proposed system is designed to improve the security and transfer valuable documents with other systems in that network and it helps the users to form a secure network, which is beyond the hackers.

ACKNOWLEDGEMENT

At this pleasing moment of having successfully completed the project work, I wish to acknowledge my sincere gratitude and heartfelt thanks to our beloved Principal **Dr.K.K.Padmanabhan** for having given me the adequate support and opportunity for completing this project work successfully.

I express my sincere thanks to **Dr. S.Thangasamy**, the ever active and sympathetic, Head of the Department of Computer science & Engineering, who with his careful supervision has ensured me in attaining perfection of work.

I extend my sincere thanks to **Mr.A.MuthuKumar M.C.A, M.Phil**, Project Coordinator, Department of Computer Science & Engineering for rendering us all the timely helps through out the project.

I regard my heartfelt thanks and everlasting gratitude to my Project Guide **Mr.S.Ganesh Babu M.C.A,** Lecturer, Department of Computer Science & Engineering for his uplifting ideas, inspiring guidance and valuable suggestions, which have been very helpful in refining upon the project.

TABLE OF CONTENTS

CHA

TITLE PAGE NO

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

1.1 Secure Communication System-An Overview

As the field of cryptology has advanced, the dividing lines for what is and what is not cryptology have become blurred cryptology today might be summed up as the study of techniques and applications that depend on the existence of difficult problems. Cryptanalysis is the study of how to compromise (defeat) cryptographic mechanisms and cryptology (from the Greek kryptos logos, meaning "hidden word") is the discipline of cryptography and cryptanalysis combined. To most people, cryptography is concerned with keeping communications private. Indeed, the protection of sensitive communications has been the emphasis of cryptography throughout much of its history. However, this is only one part of today's cryptography.

Encryption is the transformation of data into a form that is as close to impossible as possible to read without the appropriate knowledge. Its purpose is to ensure privacy by keeping information hidden from anyone for whom it is not intended, even those who have access to the encrypted data. Decryption is the reverse of encryption; it is the transformation of encrypted data back into an original form.

Encryption and decryption generally require the use of some secrete information, referred to as the key. For some encryption mechanisms, the same key is used for both encryption and decryption (symmetric key encryption/decryption) for other mechanisms, the key used for encryption and decryption are different.

Today's cryptology is more than encryption and decryption. Authentication is as fundamentally a part of our lives as privacy. We use authentication throughout our everyday lives-when we sign our name to some document for instance-and, as we move to a world where our decision and agreement are communicated electronically, we need to have electronic techniques for providing authentication. Cryptology provides mechanisms for such procedures. A digital signature binds a document to the possessor of a particular key, while a digital timestamp binds a document to its creation at a particular time.

While modern cryptography is growing increasingly diverse, cryptography is fundamentally based on problems that are difficult to solve. A problem may be difficult because its solution requires some knowledge, such as decrypting an encrypted message or signing some digital document. The problem may also be hard because it is intrinsically difficult to complete, such as finding message that produces a given hash value.

Objectives of the Project

Cryptography is extremely useful. It contains multitude of applications, many of which are currently in use. A typical application of cryptography is System built out of the basic techniques. Such systems can be of various levels of complexity. Some of the more simple applications are secure communication, identification, and authentication and secrete sharing. More complicated applications include systems for electronic commerce, certification, secure electronic mail, key recovery and secure computer access.

In general, the less complex the application, the more quickly it becomes a reality. Identification and authentication schemes exist widely, while electronic commerce systems are just beginning to be established.

Secure communication: Secure communication is the most straight forward use of cryptography. Two people may communicate securely by encrypting the messages sent between them. This can be done in such a way that third party who is eavesdropping will never be able to decipher the messages. While secure communication has existed for centuries, the key management problem has prevented it from becoming common place. Thanks to the development of public key cryptography, the tools exist to create a large scale network of people who can communicate securely with one another even if they have never communicated before.

Identification and authentication: Identification and authentication are two widely used application of cryptography. Identification is the process of verifying someone's or something's identity. For example, when withdrawing money from a bank, a teller asks to see the identification (for example, a driver's license) to verify the identity of the owner of the account.

Electronic commerce: Over the past few years there has been a growing amount of business conducted over the internet- this form of business is called electronic commerce or E-commerce. However, simply entering a credit card number on the internet leaves one open to fraud. One cryptographic solution to this problem is to encrypt the credit card number (or other private information) when it is entered online, another is to secure the entire session. When a computer encrypts this information and sends it out on the internet it is incomprehensible to a third party viewer. The web server ("internet shopping centre") receives the encrypted information, decrypts it precedes with the sale without fear that the credit card number (or other private information) slipped into the wrong hands. As more and more business is conducted over the internet, the need for protection against fraud, theft and corruption of vital information is essential.

Certification: Another application of cryptography is certification; it is scheme by which trusted agents such as certifying authorities vouch for unknown agents, such as users. The trusted agents issue vouchers called certificates which each have some inherent meaning. Certification technology was developed to make identification and authentication possible on a large scale.

1.2 The Organization Profile

DHS Informatics Private Limited is a multi-national IT consulting, software development, and outsourcing firm with head offices by name IntersoftKK in Japan and branch offices in the United States, Singapore, and an offshore development center in Bangalore, India. We work globally to deliver locally.

Vision

DHS Informatics mission is to provide top quality software engineering services to help our clients achieve and maintain a competitive advantage. Collaboration is key; our international team of engineers brings together decades of expertise in various systems, deep knowledge of information technology and cutting-edge business know-how.

Services

With a focus on finance, including banking, insurance and security, we offer the following services:

- Complete Help Desk outsourcing
- Outsourcing of Engineers
- Software development (onshore & offshore)
- Market Data Consulting
- Business analysis & system design

Trade Surveillance System

Trade Surveillance System – HawkEye was developed for the Compliance Department of a financial broker to detect and monitor irregular or suspicious transaction behavior that may jeopardize the reputation of your business. HawkEye has been designed with a sophisticated, yet flexible architecture to consolidate all exchange-trade transactions into a central enterprise repository and applies a set of customizable business rule to allow you to perform complex data mining. The system has been designed to work with all the major stock exchanges. It delivers full transparency to the data flow between a firm's trading activities and its clients' by generating reports to detect:

- Market manipulation
- Cross trading
- Short selling
- Insider trading
- Front Running
- Technologies:

  IE/Netscape, IIS 5.0/Apache, JSP/ASP, Oracle 8i/MS-SQL

SWORDFISH-Enterprise Workflow System

Swordfish is the first enterprise tool of its kind to provide you with end-to-end business process integration, by facilitating your intra-company communication via one central database. With this vital database as the nerve of your company, you will be able to capitalize on the centralized management of your company information with the click of mouse.

By enhancing the transparency of your company information, SWORDFISH becomes a powerful tool for your business to optimize and control your business processing, including:

- IT Order Management
- Legal and Compliance
- eHelp Desk
- Expenses
- eProcurement
- Personal Information
- Physical & Virtual Assets
- Error Logging
- Broker Management
- Vacation/Holidays
- Technologies:

  E/Netscape, Web logic 6.1, IIS5.0/Alliance iPlanet, JSP/ASP, Oracle 8i/MS-SQL

SWORDFISH and HAWKEYE are modular, scaleable, customizable, secure, reliable, maintenance free and above all easy to use.

CHAPTER 2

SYSTEM SPECIFICATION

2.1 HARDWARE SPECIFICATION:

CPU	:	Pentium IV Processor
Hard Disk	:	80 GB
RAM	:	512 MB DDR RAM
Keyboard	:	109 keys Logitech
Mouse	:	Logitech Scrolling Mouse
Monitor	:	Samsung
Floppy Disk	:	1.44 MB
CD-Drive	:	LG

2.2 SOFTWARE SPECIFICATION:

Front End	:	ASP.Net 1.1
Back End	:	MS-SQL Server 2000
Platform	:	Microsoft Windows 2000

2.3 SOFTWARE OVERVIEW

.NET is a library, one that is just as extensive as the Windows API. We can use it to call up all the same sorts of features that have traditionally been the role of the Windows operating systems; displaying windows and dialog boxes, verifying security credentials, calling on base operating systems services, creating threads and so on, as well as newer areas such as accessing databases or connecting to the internet or providing web services.

.NET provides the environment in which our program is run. When .NET aware code is executed, it will be .NET that starts up your code, manage the running threads, provides various background services, and in real senses is the immediate environment seen by the code.

ADVANTAGES:

- Object Oriented Programming
- Good Design
- Language Independence
- Better support for dynamic web pages
- Efficient Data Access
- Code Sharing
- Improved Security

INTRODUCTION TO ASP.NET:

ASP.NET is the latest version of Active Server Pages (ASP), Microsoft's server-side web technology for building dynamic, interactive, and database-driven web sites.

ASP.NET is a unified web platform that provides all the services necessary for to build enterprise-class applications. It hopes to do for the web what visual basic has done for windows. It is based on the .NET framework, which provides a platform independent of programming languages and operating systems for developing and deploying web applications.

ANTAGES:

- Support for programming languages
- Language-independence
- Support for separation of code and content
- Simplified development
- Client platform independence
- Web services
- Support for .NET framework
- Backward compatibility

ASP.NET ELEMENTS:

Web Forms:

Web forms give the developer the ability to drag and drop ASP.NET server controls onto the form and easily program the events that are raised by the control. User controls, mobile controls and other third-party controls can be added to extend web forms.

Server Controls:

A server control is a control that is programmable by writing server-side code. Server controls automatically maintain their state between calls to the server. Two types of server controls; HTML and web server controls.

View State:

When a web form is rendered to the browser, a hidden HTML input tag is dynamically created, called view state. This input contains base64-encoded data that can be used by any object that inherits from system.

ADVANCED CONTROLS:

Panel control:

Instead of setting the visible property for controls one by one, we can use the panel control to hide controls as a group.

Ad Rotator control:

It is used to display banner advertisements randomly. The advertisements with this control that contains a list of the properties of banner advertisements to display.

Data grid control:

It is used to display the records without using templates. We can simply bind a data source to the data grid, and it automatically displays the records. We can create columns to control how records are formatted or to display links for editing records.

ADO.NET:

It contains several namespaces with dozens of classes devoted to database access. The System.Data.Sqlclient namespace includes the following three classes:

- SqlConnection
- SqlCommand
- SqlDataReader

ction:

This sqlconnection need to create and open a database connection. the connection in different ways depending on the type of database ant to access.

mand:

It is used to create a database command that represents the SQL atement to execute.

Reader:

It represents a forward-only stream of database records. This means e data reader represents only a single record at a time. To fetch next in the stream we must call the read () method. To display all the records ed from a query, we must call the read () method repeatedly until we reach nd of the stream.

SET:

A dataset can contain one or more DataTables that represent base tables. Relationships between the tables can be defined using Relation classes.

A ADAPTER:

It represents the bridge between a Dataset and the data source it sents. We use a DataAdapter to populate a DataSet from an existing base table. We can also use a DataAdapter to update and existing database with changes made to a DataSet.

QL Server 2000

Microsoft SQL Server 2000 extends the performance, reliability, nd ease-of-use of Microsoft SQL Server version 7.0. Microsoft SQL 2000 includes several new features that make it an excellent database n for large-scale online transactional processing (OLTP), data ousing, and e-commerce applications.

The OLAP Services feature available in SQL Server version 7.0 is w called SQL Server 2000 Analysis Services. The term OLAP Services has en replaced with the term Analysis Services. Analysis Services also includes a new data-mining component.

Features of SQL Server 2000

- **Internet Integration**

The SQL Server 2000 database engine includes integrated XML support. It also has the scalability, availability, and security features required to operate as the data storage component of the largest Web sites. The SQL Server 2000 programming model is integrated with the Windows DNA architecture for developing Web applications, and SQL Server 2000 supports features such as English Query and the Microsoft Search Service to incorporate user-friendly queries and powerful search capabilities in Web applications.

- **Scalability and Availability**

The same database engine can be used across platforms ranging from laptop computers running Microsoft Windows® 98 through large, multiprocessor servers running Microsoft Windows 2000 Data Center Edition. SQL Server 2000 Enterprise Edition supports features such as federated servers, indexed views, and large memory support that allow it to scale to the performance levels required by the largest Web sites.

prise-Level Database Features

he SQL Server 2000 relational database engine supports the features uired to support demanding data processing environments. The abase engine protects data integrity while minimizing the overhead of anaging thousands of users concurrently modifying the database. SQL erver 2000 distributed queries allow you to reference data from multiple ources as if it were a part of a SQL Server 2000 database, while at the ame time, the distributed transaction support protects the integrity of any updates of the distributed data. Replication allows you to also maintain multiple copies of data, while ensuring that the separate copies remain synchronized. You can replicate a set of data to multiple, mobile, disconnected users, have them work autonomously, and then merge their modifications back to the publisher.

Data warehousing:

SQL Server 2000 includes tools for extracting and analyzing summary data for online analytical processing. SQL Server also includes tools for visually designing databases and analyzing data using English-based questions.

Views:

A database object that can be referenced the same way as a table in SQL statements. Views are defined using a SELECT statement and are analogous to an object that contains the result set of this statement.

Index:

In a relational database, a database object that provides fast access to data in the rows of a table, based on key values. Indexes can also enforce uniqueness on the rows in a table. SQL Server supports clustered and no clustered indexes. The primary key of a table is automatically indexed. In full-text search, a full-text index stores information about significant words and their location with in a given column.

Stored Procedure:

A precompiled collection of Transact-SQL statements stored under a name and processed as a unit. SQL Server supplies stored procedures for managing SQL Server and displaying information about databases and users. SQL Server-supplied stored procedures are called system-stored procedures.

CHAPTER 3

SYSTEM ANALYSIS

3.1 EXISTING SYSTEM

In traditional cryptography, the sender and receiver of a message know and use the same secret key; the sender uses the secret key to encrypt the message, and the receiver uses the same secret key to decrypt the message. This method is known as secret key or symmetric cryptography. The main challenge is getting the sender and receiver to agree on the secret key without anyone else finding out. If they are in separate physical locations, they must trust a courier, a phone system, or some other transmission medium to prevent the disclosure to the secret key. Anyone who overhears or intercepts the key in transit can later read, modify and forge all messages encrypted or authenticated using that key. The generation, transmission and storage of keys is called key management: all cryptosystems must deal with key management issues. Because all keys in a secret-key cryptosystem must remain secret, secret-key cryptography often has difficulty providing secure key management, especially in open systems with a large number of users.

The main problem with the secret key cryptosystems is getting he sender and receiver to agree on the secret key without anyone else finding out. This requires a method by which two parties can communicate without fear of eavesdropping faster than public key cryptography. Cryptanalysis is the study of how to compromise (defeat) cryptographic mechanisms and cryptology (from the Greek kryptos logos, meaning “hidden word”) is the discipline of cryptography and cryptanalysis combined.

Everyday, people sign their names to letters, credit card receipts, and other documents, demonstrating they are in an agreement with the contents. That is, they authenticate that they are in fact the sender of the item. This allows others to verify that a particular message did indeed originate from the signer. However, this is not foolproof, since people can "lift" signatures off one document and place them on another, thereby creating fraudulent documents. Written signatures are also vulnerable to forgery because it is possible to reproduce a signature on other documents as well as to alter documents after they have been signed.

3.2 PROPOSED SYSTEM

Authentication is any process through which anyone proves and verifies certain information. Sometimes one may want to verify the origin of a document, the identity of the sender, the time and date a document the identity of a computer or user and so on. A digital signature is a cryptographic means through which many of these may be verified. The digital signature of a document is a piece of information based on both the document and the signer's private key. It is typically created through the use of a hash function and a private signing function.

- Generating keys for the user to communicate with the server and to other user.

- Authenticating the user with the keys, when they are entering into the network for the transaction.

- Transferring the encrypted documents to the validated users who are connected properly in the network.

based on the difficulty of computing discrete logarithms and is based s originally presented by ELGamal and Schnorr.

There are three parameters that are public and can be common to a users. A 160-bit prime number q is chosen. Next a prime number p is with a length between 512 and 1024 bits such that q divides (p-1). g is chosen to be of the form $h^{(p-1)/q}$ mod p, where h is an integer between 1) with the restriction that g must be greater than 1.

With these numbers in hand, each user selects a private key and erates a public key. The private key x must be a number from 1 to (q-1) and hould be chosen randomly or pseudo randomly. The public key is calculated from the private key as $y=g^x$ mod p. The calculation of y given x is relatively traightforward. However, given the public key y. it is believed to be computationally infeasible to determine x, which is the discrete logarithm of y to the base g, mod p.

To create a signature, a user calculates two quantities, r and s , that are functions of the public key components (p,q,g), the user's private key(x), the hash code of the message, H(M), and an additional integer k that should be generated randomly or pseudo randomly and be unique for each signing.

At the receiving end, verification is performed using the formulas. The receiver generates a quantity v that is a function of the pubic key components, the sender's public key, and the hash code of the incoming message. If this quantity matches the r component of the signature, then the signature is validated.

[illegible] Public-Key Components

[illegible] re $2^{L-1}<p<2^{L}$ for 512<=L<=1024 and L a [illegible] bit length of between 512 and 1024 bits in [illegible] 4 bits.

[illegible] (p-1), where $2^{159}<q<2^{160}$ [illegible] th of 160 bits

[illegible] p , where h is any integer with 1<h<(p-1) [illegible] at $h^{(p-1)/q}$ mod p > 1 (3.1)

User's Private Key

[illegible] or pseudorandom integer with 0<x<q.

User's Public Key

[illegible] mod p. (3.2)

User's Per-Message Secret Number

[illegible] ndom or pseudorandom integer with 0<k<q. (3.3)

Signing

[illegible] $(g^{x}$ mod p) mod q. (3.4)

[illegible] = $[k^{-1}$ (H(M) + xr)] mod q (3.5)

[illegible] ignature = (r,s). (3.6)

Verifying

$W = (s^{1})^{-1}$ mod q (3.7)

U1 = $[H(M^{1})w]$mod q (3.8)

U2 = (r^{1})w mod q (3.9)

d p]mod q. (3.10)

(3.11)

message to be signed

hash of M using SHA-1

= received versions of M, r, s

(M),k ,x, r, q) = (k-1 H(M) + xr))mod q

p, q, g) = (gx mod p)mod q

w = f

v = f

Fi

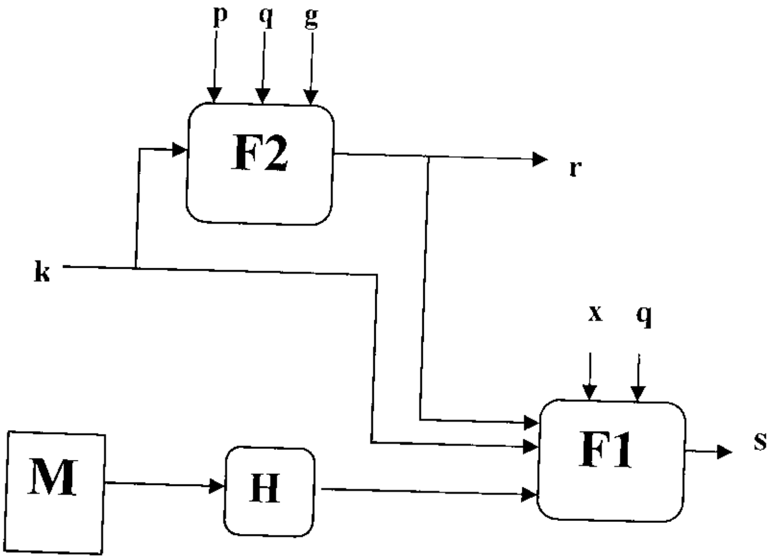


Fig 3.2.1 Digital Signature Sign

s = f1(H(M),k ,x, r, q) = (k-1 H(M) + xr))mod q

r = f2(k, p, q, g) = (gx mod p)mod q

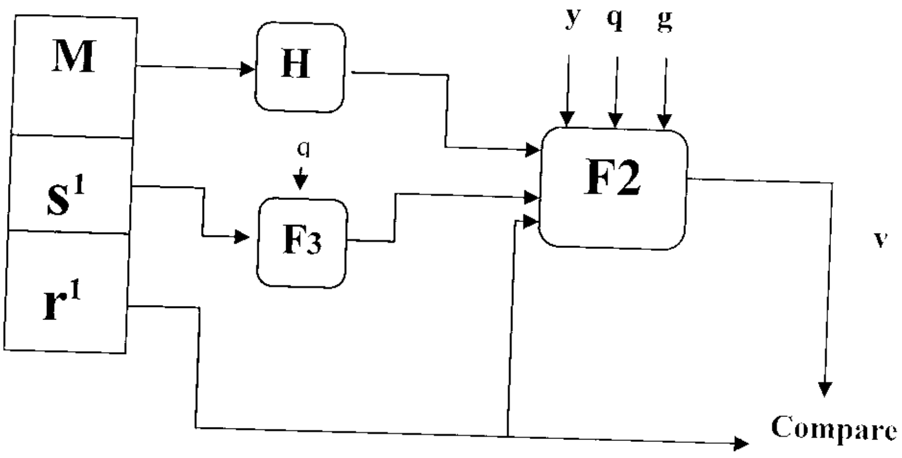


Fig 3.2.2 Digital signature Verifying

w = f3(s1,q) = (s1)-1 mod q

v = f3(y, q, g, H(M1), w, r1) = ((g(H(M1)w)mod q yr1w mod q)mod p)mod q

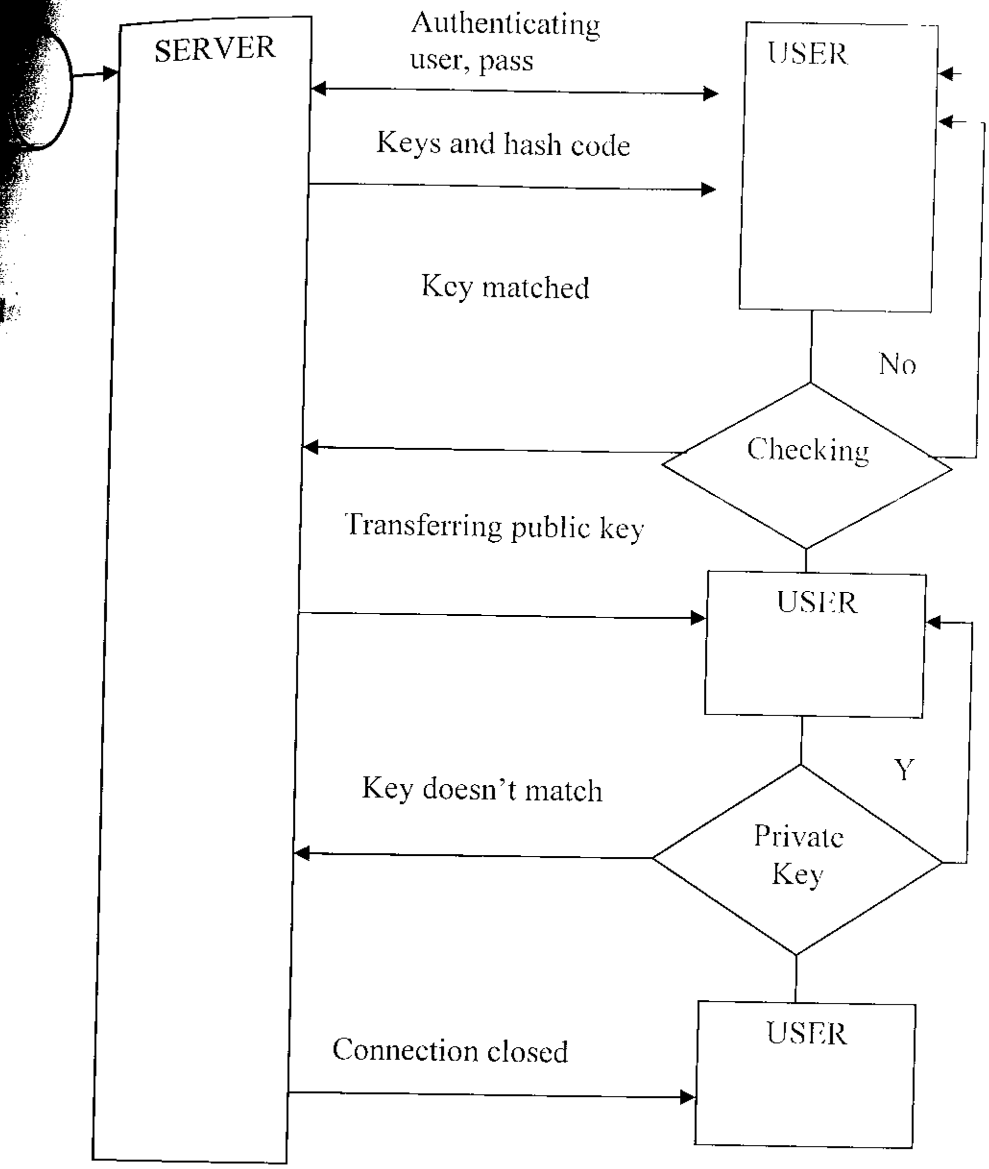
Final Outline of the Proposed System

Random number generation is used in a variety of cryptographic operations, such as key generation and challenge/response protocols. A random number generator is a function that outputs a sequence of 0's and 1's such that at any point, the next bit cannot be predicated based on the previous bits. However, true random number generation is difficult to do on a computer, since computers are deterministic devices. Thus if the same random number generator is run twice, identical results are obtained. True random number generators are in use, but they can be difficult to build.

They typically take input from something in the physical world such as the rate of neutron emission from a radioactive substance or a user's idle mouse movements.

Because of these difficulties, random number generator on a computer [illegible] only pseudo-random number generation. Pseudo-random number generators are often based on cryptographic function s like block ciphers or [illegible] ciphers. For instance, iterated DES encryption starting with a 56-bit seed produces a pseudo-random sequence.

The combinations of such randomly generated value and hash function [illegible] transferred together to the client. Random number should be known to the client with that the hash code is combined, then it matches to with the sender [illegible] digital signature then its authenticated.



3.2.3 THE PROPOSED SYSTEM

CHAPTER 4

SYSTEM DESIGN

Fundamental Design Concepts

System design is the solution, a 'how to' approach to the creation of new system. This phase focuses on the detailed implementation of the system recommended in the feasibility study. Emphasis is on the translating performance specifications into design specifications. The design phase is a transition from the user oriented documentation to the documented oriented to the programmers or database personnel.

System design goes through two phases of development: Logical and the Physical design.

The logical design covers the following:

- Reviews the current physical system – its data flows, file content, volumes, frequencies, etc.

- Prepares output specifications- that is, determines the format, contents and frequency of reports, including terminal specification and locations.

- Prepares input specifications – format, contents and most of the input functions. This includes determining the flow of the document form the input data source to the actual input location.

- Prepares edit, security, and control specifications. This includes specifying the rules for edit correction, backup procedures, and the controls that ensure processing and file integrity.

cifies the implementation plan.

repares a logical design walkthrough of the information flow, utput, input, controls and implementation plan.

Reviews benefits, costs, target dates, and system constraints.

llowing logical design is the physical design. This produces the tem by defining the design specifications that tell programmers t the candidate system must do. In turn, the programmer writes the rograms or modifies the software package the accepts input from the rms the necessary calculations through the existing file or database, the report on a hard copy or displays it on a screen and updates the at all times.

Specifically the physical design consists of the following steps:

sign the physical system

a. Specify input/output media.
b. Design the data base and specify backup procedures.
c. Design physical information flow through the system and the physical design walkthrough

lan system implementation

a. Prepares a conversion schedule and a target date.
b. Determine training procedure, courses and timetable.

Devise a test and implementation plan and specify the new hardware/software.

Update benefits, costs, conversion date and system constraints (Legal, Financial, Hardware, etc.)

Every intellectual discipline is characterized by fundamental concepts of software design.

w Diagram

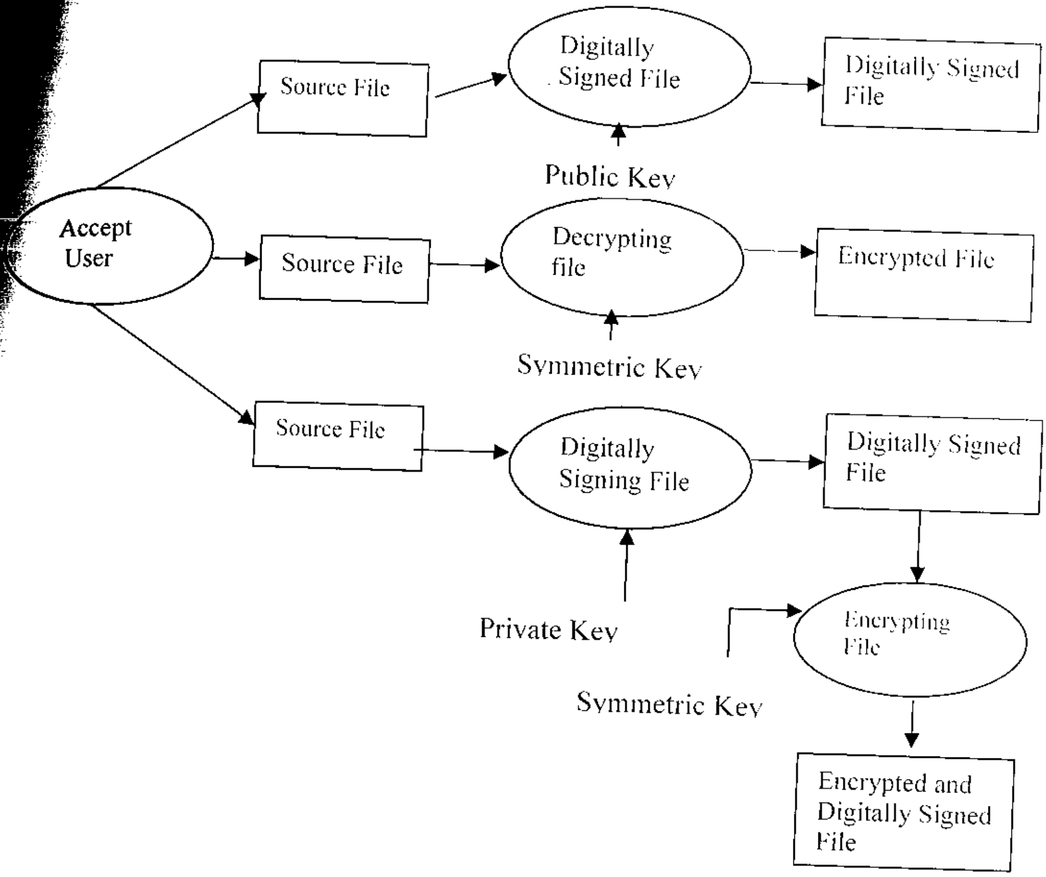


Fig 4.2.1 DFD FOR ENCRYPTION

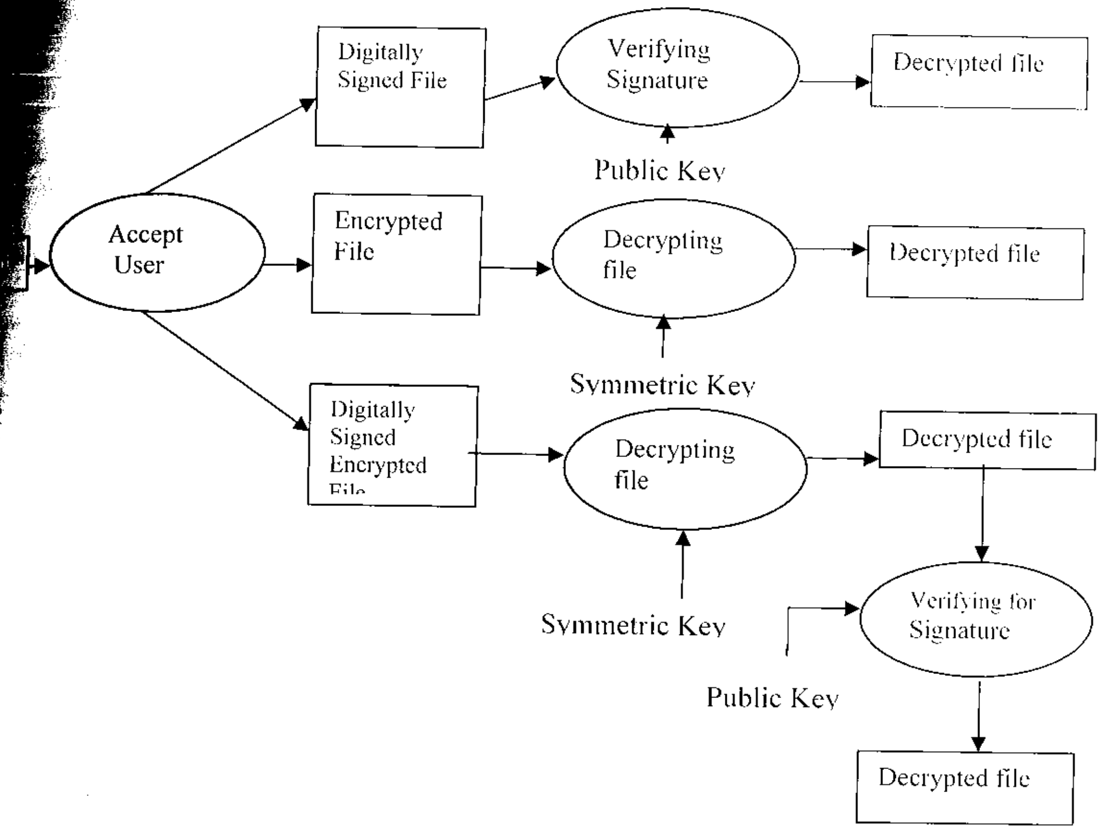


Fig 4.2.2 DFD FOR DECRYPTION

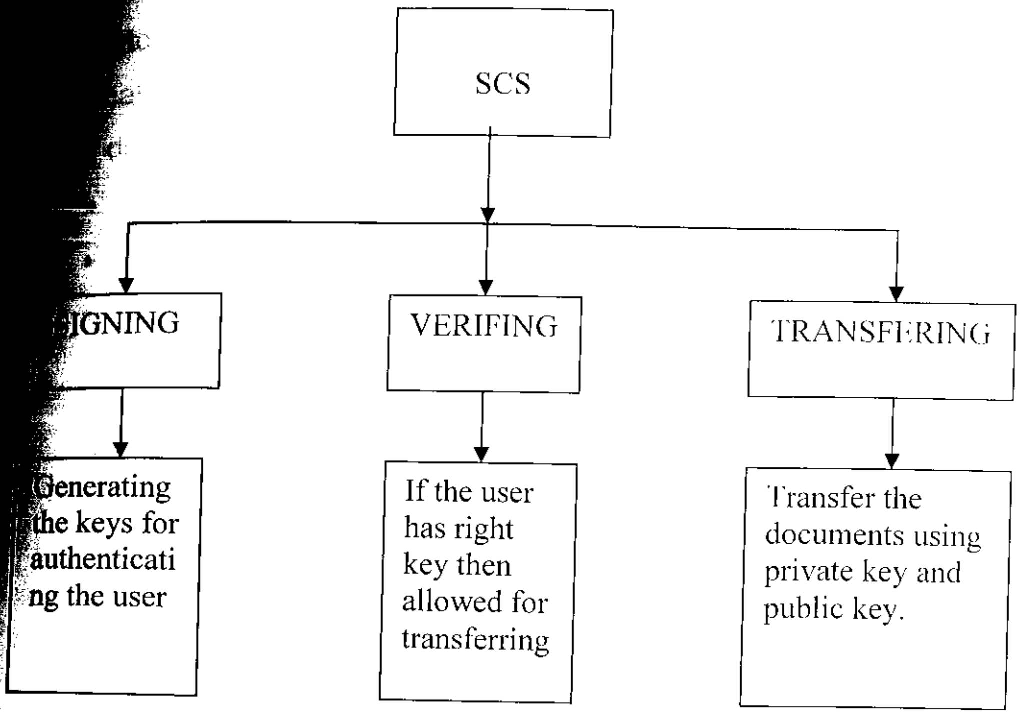

SCS
SIGNING
VERIFING
TRANSFERING
Generating the keys for authenticati ng the user
If the user has right key then allowed for transferring
Transfer the documents using private key and public key.

Fig 4.2.3 Structure Chart

4.3 Database Design

A database is a collection of information, which contains data shared with redundancy to server users quickly and efficiently. The general objective is to make information access easy, quick, inexpensive and flexible for the user. During the database design the major issues considered are:

- Redundancy
- Data Independence
- Accurate integrating
- More information at low cost
- Recovery form failure
- Privacy and Security
- Performance
- Easy of learning and use

Integration means the collecting of data, which are scattered on different devices. Integrity checks that the logical information is consistent Owing to differences in duplicated physical data. Data independence is the organization of independent data and the knowledge of the data organization and access technique to build into the application logic.

Database design is required to manage large bodies of information. The management of data involves both the definitions of structures for the storage information and provision of mechanisms for the manipulation of information. In addition the database design must provide for the safety of the information handled despite system crashes or due to attempts at unauthorized access.

Having identified all the data in the system it is necessary to arrive at the logical database design. The requirements of the user are taken into account to decide the data that needs to be stored in the system.

4.4 TABLE DESIGN

There are four tables used in this project that form the database. They are

Authentication Table:

In the user name and password are stored in the server. Which does the program use when a client sends its particular user name, password. So that many no of can connect to the server for authentication. And the database is connected only to server that make more secure from the hacker and unauthorized user.

Table 4.4.1 Authentication

Field Name	Type	Width	Remark
User_code	Numeric	8	Primary Key
User_id	Varchar	15	Unique, Not Null
User_password	Varchar	10	Not Null
User_name	Varchar	40	Not Null
User_address	Varchar	200	
User_area	Varchar	40	
User_city	Varchar	40	
User_state	Varchar	40	
User_pin	Varchar	6	
User_phone	Varchar	20	
User_mobile	Varchar	20	
User_fax	Varchar	20	
User_email	Varchar	60	

Keys table:

The private key, public key and the secret number are maintained in the database to transfer it to user randomly. With this no repetition of key will not occur, and user after generating their digital signature that can be verified their in the system. Authentication is any process through which anyone proves and verifies certain information. Sometimes one may want to verify the origin of a document, the identity of the sender, the time and date a document the identity of a computer or user and so on. The digital signature of a document is a piece of information based on both the document and the signer's private key. It is typically created through the use of a hash function and a private signing function.

Table 4.4.2 Keys

Field Name	Type	Width	Remark
User_code	Numeric	8	Foreign Key
K_private	Varchar	50	Not Null
K_public	Varchar	50	Not Null
Signature	Varchar	200	Not Null

Message Table:

It consists of message number, message subject and date of the messages send.

Table 4.4.3 Message

Field Name	Type	Width	Remark
User_code	Numeric	8	Foreign Key
M_No	Numeric	3	Primary Key
M_date	Datetime	8	Not Null
M_subject	Varchar	200	
M_message	Varchar	500	

Feedback Table:

It consists of feedback number, date and feedback which the user entered in the feedback column.

Table 4.4.4 FeedBack

Field Name	Type	Width	Remark
Date	datetime	8	
Sno	int	4	
FeedBack	Varchar	50	

Input Design

The objectives of input design are as follows:

Controlling amount of input: wherever user input is required, the amount of user keystrokes is reduced by giving possible input values as default in the area. Thus the user can pass on to next data without much typing. This makes the data entry much fast and error free. When the user has the format of input to be given, it will be very easy for user to give, it will be very easy for user to give input in the same format.

The important features are

- The input screen is not crowed, as the user can understand the information from the screen.
- The input validation is being done at program level to check errors & help messages are to be provided.

The Main Menu:

The project the home page is the first page of the project which consist of five modules, Generating key, hash code generation, encryption, decryption, transferring. Under each of these there are panels containing the activities under them. Before entering the main menu, the user name and password have to be given for security purpose.

Administration Panel:

It obtains the user name and password for authenticating.

Hash code:

It is generating by the message, which is selected by the user at the time of authentication. The hash code is transferred combining with the private key and public key. The secret number will not be given; it must be transmitted secretly to the particular user through mail (or) by other connection.

Generating key Panel:

The values of p, q, g are generated uniquely and with that private key, public key and a secret no is generated. This operation is done every time when clients enter into the server for authentication purpose. Finally it is transmitted to the user with hash code Encrypted form.

Creates a message digest of the information to be sent.

1. Represents this digest as an integer m between 0 and n-1.
2. Uses her private key (n, d) to compute the signatures s = m^ d mod n.
3. Sends this signature s to the recipient B.

Encryption Panel:

This is done using RSA algorithm. It can generate the public key and private and transfer any single key. Otherwise the receiving user should have the any corresponding key to decrypt the encrypted data. Suppose Alice wants to send message m to Bob. Alice creates the cipher text c by exponent: c=me mod n, where e and n is Bob's public key. She sends c to Bob.

1. Obtains the recipient B's public key (n, e).
2. Represents the plaintext message as a positive integer m<n. [See note 4]
3. Computes the cipher text c = m^ e mod n.
4. Sends the cipher text c to B.

Decryption Panel:

It is a process after receiving the encrypted data it is decrypted but it will be there in sender and receiver side. Bob exponentiates: m=cd mod n; the relationship between e and d ensures that Bob correctly recovers m. Since only Bob knows d, only Bob can decrypt this message.

1. Uses his private key (n, d) to compute m = c^ d mod n.
2. Extracts the plaintext from the integer representative m.

Transfer Panel:

The file to be transferred and host address and destination address are mentioned. And the location the file to be saved can also be mentioned. The file is better to transfer it in executable only. It gives more protection and safe to digital signature.

Output Design

The output design generally refers to the results and information that are generated by the system. For many end users, output is the main reason for developing the system and the basis on which they will evaluate the usefulness of the application. Most end users will not actually operate the system or enter data through workstations, but they will use the output from the system.

When designing output, system analysts must accomplish the following:

- ❖ Determine what information to present
- ❖ Decide whether to display or print the information and select the output medium.
- ❖ Arrange the presentation of information in an acceptable format.
- ❖ Decide how to distribute the output to intended recipients.

Accomplishing the general activities listed above will require specific decisions, such as whether to use preprinted forms when preparing reports and documents, how many lines to plan on prints page, or whether to use graphics and color.

The input and output operation are different in this project and designing is also differ many of the panel available in input will not be presented in output. The panels in outputs are verification, encryption, decryption and transfer.

Verification panel:

The receiver receives the digital signature file. If the receiver is a authenticated user then receiver will have the key, finally if it matches then encryption and decryption process can be continued with other user.

1. Uses sender A's public key (n, e) to compute integer v = s^ e mod n.
2. Extracts the message digest from this integer.
3. Independently computes the message digest of the information that has been signed.
4. If both message digest are identical, the signature is valid.

Encryption Panel:

This is done using RSA. The user can generate the public key and private and transfer any single key. Otherwise the receiver should have the any corresponding key to decrypt the encrypted data. Suppose Alice wants to send message m to Bob. Alice creates the cipher text c by exponent: c=me mod n, where e and n is Bob's public key. She sends c to Bob.

1. Obtains the recipient B's public key (n, e).
2. Represents the plaintext message as a positive integer m<n.
3. Computes the cipher text c = m^ e mod n.
4. Sends the cipher text c to B.

Decryption Panel:

It is a process after receiving the encrypted data it is decrypted but it will be there in sender and receiver side. Bob exponentiates: m=cd mod n; the relationship between e and d ensures that Bob correctly recovers m. Since only Bob knows d, only Bob can decrypt this message.

1. Uses his private key (n, d) to compute m = c^ d mod n.
2. Extracts the plaintext from the integer representative m.

Transfer Panel:

The file to be transferred and host address and destination address are mentioned. And the location the file to be saved can also be mentioned. The file is better to transfer it in executable only. It gives more protection and safe to digital signature.

CHAPTER 5

TESTING AND IMPLEMENTATION

5.1System Testing

Testing is a process of executing a program with the intent of finding an error. A good test case is one that has a high probability of finding an as yet undiscovered error. These tests should be planned long before testing begins, then goal will be successfully achieved.

The first test of a system is to see whether it produces the correct outputs. Following this step a variety of other tests are conducted.

- Online response time testing
- Volume testing
- Stress testing
- Usability documentation test and procedure
- Validation testing

The proper choice of the test data is as important as the test itself. Test data can be artificial (created solely for test purpose) or live (taken from users actual files).The first step in system testing is to prepare a test plan that will test all aspects of the system in a way that promotes its credibility among potential users. Network security using digital signature is tested by giving all types of data and was found successfully working without any bugs.

The test plan entails the following activities:

- Prepare test plan.
- Specify conditions for user acceptance testing.
- Prepare test data for program testing.
- Prepare test data for transaction path testing.
- Plan user testing.
- Prepare operational documents.

System testing consists of program testing, string testing, system testing, system documentation, user acceptance testing, etc. System testing involves two kinds of activities: Integration testing and Acceptance testing. The integration strategy dictates the order in which modules are written, debugged and unit tested. Acceptance testing involves planning and execution of functional tests, performance tests and stress tests to verify that the implemented system satisfies its requirements. Acceptance tests are typically performed by the quality assurance and/or customer organization.

In addition to functional and performance tests, stress tests are performed to determine the limitations of the system. Acceptance tests will incorporate test cases developed during unit testing and integration testing. Additional test cases are added to achieve the desired level of functional performance and stress testing of the entire system. Tools of special importance during acceptance testing include a test coverage analyzer, a timing analyzer, and a coding standards checkers.

At the end of the integration testing the software is completely assembled as a package. Interfacing errors have been uncovered and corrected and final series of software functions in manner that can be reasonably expected by the customer. Software validations are achieved through a series of black box tests. A test plan outlines the classes of tests to be conducted, and a test procedure defines specific test cases that will be used in an attempt to uncover errors in conformity with requirements are achieved, documentation is correct and human engineering and other requirement are met.

Testing Methodologies

Unit testing:

Unit testing comprises the set of tests performed by an individual programmer prior to integration of the unit into a large system. There are four categories of tests that a programmer will typically perform on a program unit.

- Functional tests.
- Performance tests.
- Stress tests.
- Structure tests.

Functional tests:

Functional test cases involve exercising the code with normal input values for which the expected results are known as well as boundary values and special values such as logically related inputs. Functional test cases specify typical operating conditions, typical input values and typical expected results. Functional tests and performance tests are based on the requirement specification they are designed to demonstrate that the system satisfies its requirements. The test plan can be only as good as the requirements, which in turn must be phrased in quantified testable terms.

Performance tests:

Performance tests are designed to verify response time under varying loads, percent of execution time spent in various segments of the program, throughput, primary and secondary memory utilization and traffic rates on data channels and communication links.

Stress tests:

Stress tests are designed to overload a system in various ways. This includes attempting to sign on more than the maximum number of allowed terminal, processing more than the allowed number static levels, or disconnecting a communication link.

Structure tests:

Structure tests are concerned with examining the internal processing logic of software system. The goal of structure system is to traverse a specified number of paths through which each routine in the system to establish thorough testing.

In this project testing is done by giving sample values. This satisfies the entire user requirement.

5.2 Quality Assurance

5.2.1 Generic Risk

Controls are developed to ensure a quality product. Basically quality assurance defines the objective of the project and reviews the overall activities so that errors are corrected early in the development process. It makes certain that the user receives a quality system tailored to the requirements set in advance.

The factors that determine system quality include

- security
- Correctness
- Reliability
- Efficiency

- Usability
- Maintainability
- Testability
- Portability

Quality assurance specialists use three levels of quality assurance

- Testing a system to eliminate errors
- Validation to test the quality of software in both simulated and live environments
- Certification that the program or software package is correct and confirms to standards.

Some of the problems or generic risks found practically were turn-around time, backup, file protection. The planned test of a system should include a thorough auditing technique and introduce control elements unique to the system.

Security Technologies and policies

Security is critical in system development. The amount of protection depends on the sensitivity of data, the reliability of the user and the complexity of the system. The organization running, protects data as an asset, and seeks management support for more installations.

There are three categories of controls in data security physical security, database integrity and control policies or measures. Potential threats to system security include errors and omissions, disgruntled and dishonest employees, fire and natural disasters. Error and omissions cause the most damage. There are several security measures like identification, access control, audit controls, system integrity, etc.

This project is based fully concentrated and building a better security system. It starts its security feature from the beginning to end. Such as, it allows the authenticated user to enter the system and the password files are maintained in the server. The digital signature is the most important factor in this project which is very difficult to break by the user. Once the authenticated user is entered into the network user can transfer the valuable documentation and communicate to other user with maximum satisfaction with security.

The other security is provided when the transferring is taking place also. Encryption and decryption of data is done between the clients, server. So the a known and unauthorized, hackers can't able to view the exact document and alter it.

To maintain an adequate level of security, the system is analyzed for the risks, exposure, and costs and specified security technologies described above will maintain and help the user to transfer their data successfully.

5.3 System Implementation

Implementation Procedure

Implementation is the process of converting a new system design into operation. Conversion entails several steps:

- ✓ Review the project plan, test documentation and implementation plan.
- ✓ Convert the files
- ✓ Conduct parallel processing
- ✓ Log of the computer run for reference
- ✓ Discontinue the old system
- ✓ Plan for post-implementation review

The prime concern during conversion is copying the old files to the new system. Once a particular file is selected, the next step is to specify the data to be converted. A file comparison program is best suited for verifying the accuracy of copying process.

Well planned test files are important for successful conversion. A test file should contain predictable results, simplified error finding routines, and printed results in seconds. It should also show how the new system handles the most difficult tasks. A good audit trial is the key to detecting errors and fraud in a new system. To detect fraud, many system designs do not allow the easy deletion of many records on the file. This feature makes it difficult to cover up problem or conceal fraud.

All these above mentioned constraints are considered during the implementation of Digital signature algorithm and the implementation procedure is carefully handled and may give some problem in future. Because being it is based on security daily the security levels are moving forward and to compensate that virus and hacking programs are growing.

Implementation is the key stage in achieving a successful new system as it involver a lot of upheaval in the user department. This is carefully planned and controlled. The three major tasks of preparing for implementation are education and authorizing of users and testing of the system.

The main stages over implementation are:

- Security after entering
- Adding security while transferring
- Amendment procedure
- Change over
- System audit

5.3.2 User Training

During user training, the resident expert emerges. Being it is an newly developed system and function idea will be less. He is the one who should be authenticated whether a proper person to learn about the system, probably has the most interest in the system, works the hardest to learn it, and consequently benefits from the unique role of being an "expert" in the group.

Experience in user training suggests that

- Authenticated users should be reluctant to read manuals but learn well from demonstrations and while executing and referring authorized officers.
- Users tend to natural teachers.
- The resident expert is a natural trainer since he speaks the user group's language and uses samples based on common experiences to teach the new system.

The primary teaching aids in user training are the user manual, "help screens", data dictionary, etc. The tools and procedures are designed to minimize the users sample based on common experience to teach the new system.

The training program is followed by preparation of the user training manual and other test materials. Facility requirement and the necessary hardware are specified and documented. A common procedure is to train supervisors and department heads who in turn train their staff as they see first.

The reasons are for this:

- User supervisors are knowledgeable about the capabilities of the staff and the overall operation.
- Staff members usually respond more favorably and accept instructions from their supervisors than from outsiders.

- Familiarity of users with their particular problems makes them better candidates for handling user training than the system analyst. The analyst gets feedback to ensure that proper training is provided.

User training is needed for any system to be operated. At the implementation stage the emphasis must be on training on new skills to give staff confidence that they can cope with the new system and transaction can be done safely. The training will be most successful if conducted by the supervisor in the presence of the system analyst.

CHAPTER 6

CONCLUSION

The Secure Communication was successfully established using RSA, Hash function. This is used to enter authenticated users to the network and transfer their files with more security.

This being a professional level project, we learnt the various aspects of cryptography that remained in the realms of theory till now.

This is being our professional level project is also the reason where one may find very few loopholes in the project and there is definitely a scope for further improvement.

CHAPTER 7

SCOPE FOR FURTHER ENHANCEMENT

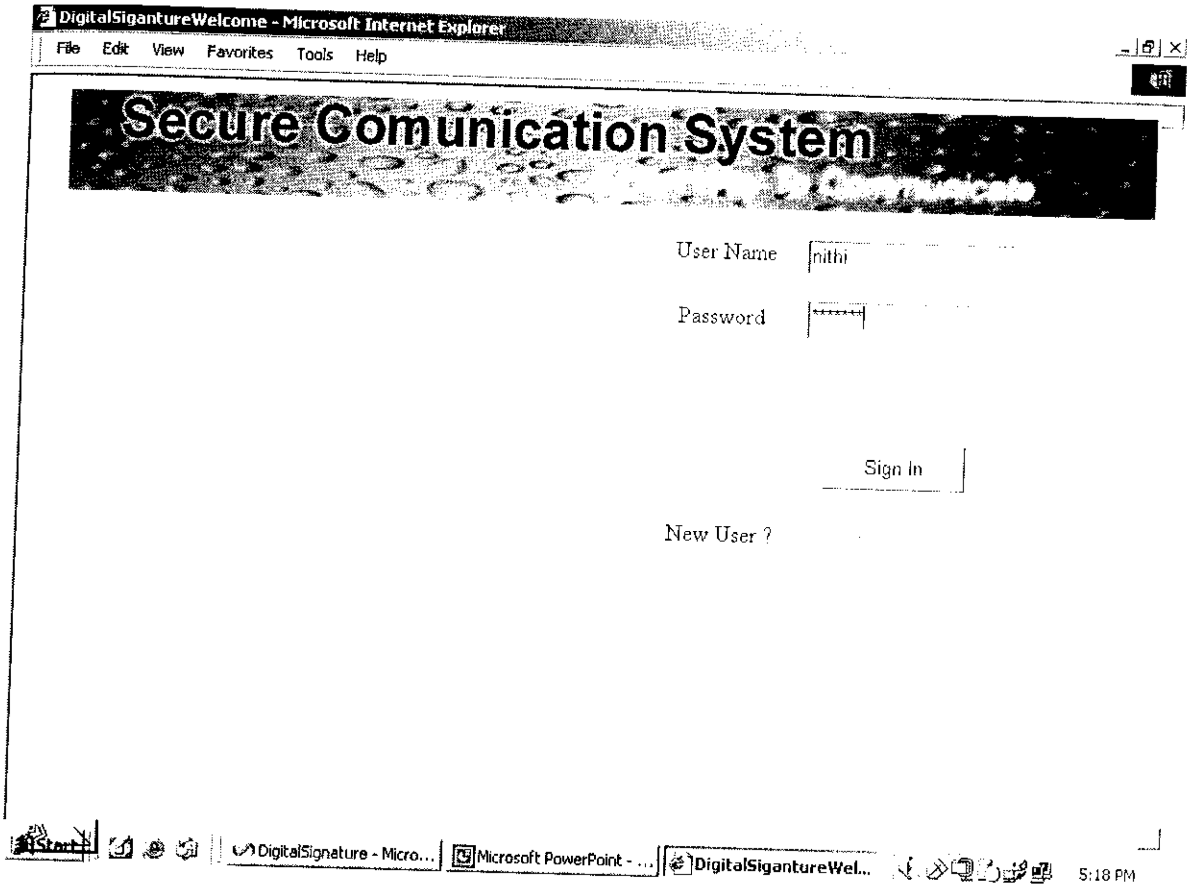
Every end line is the new beginning for this project. According to cryptography and virus it keeps on new invention. The authentication may be little more added, some which existing in the project will be supporting.

The security can be improved by adding the authentication. Such as online voice reorganization, video tracking of the user can be controlled using the user. The algorithm which is new will be defeated by global hackers and there will be new digital algorithm to develop new security program.

The designing face is well and it is suitable for future enhancement and with that the existing algorithm can be used with some other combination to keep the system and data transferring in the network secure.

APPENDIX

SAMPLE SCREEN SHOTS

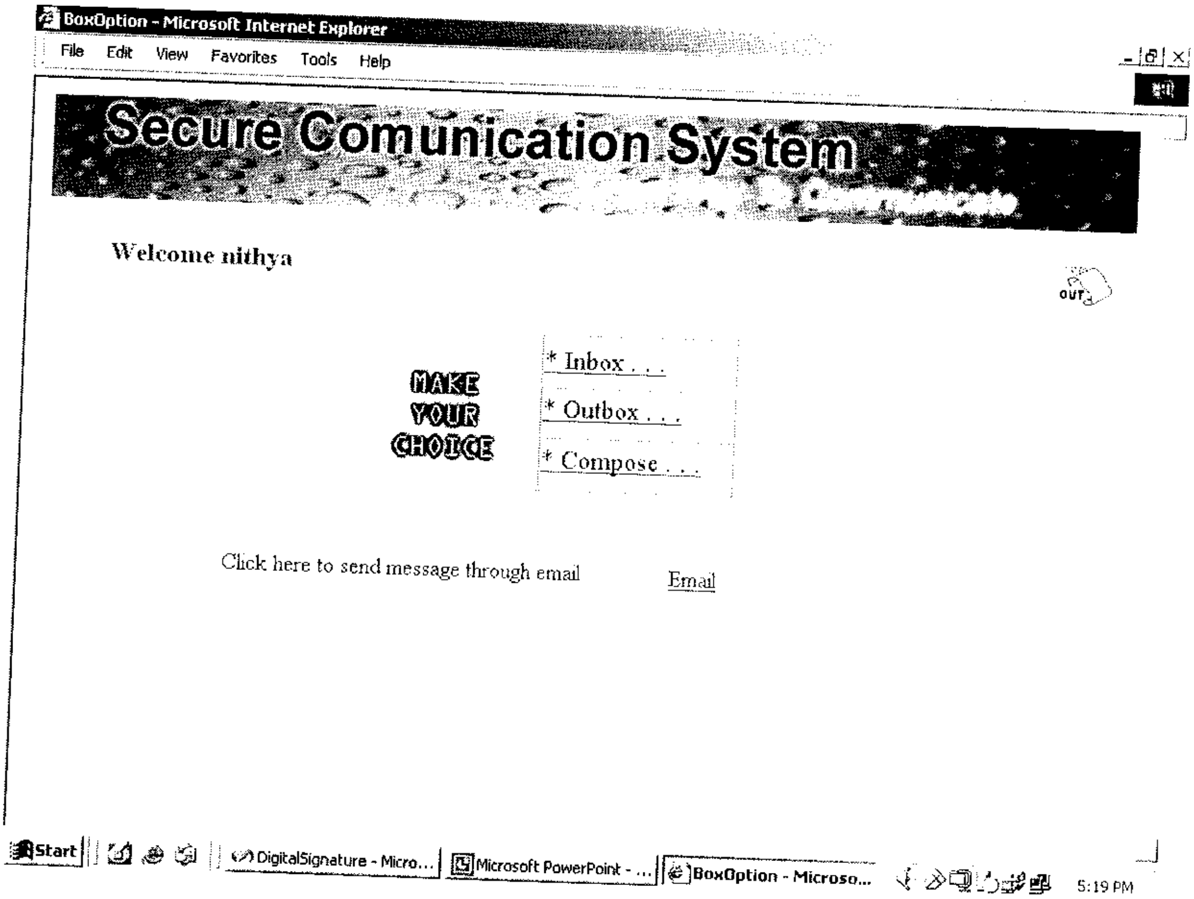


User Name nithi

Password *******

DigitalSigantureWelcome - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Secure Comunication System
Sign In
New User ?
Start
DigitalSignature - Micro...
Microsoft PowerPoint - ...
DigitalSigantureWel...
5:18 PM

Fig A.1 The Authentication Form



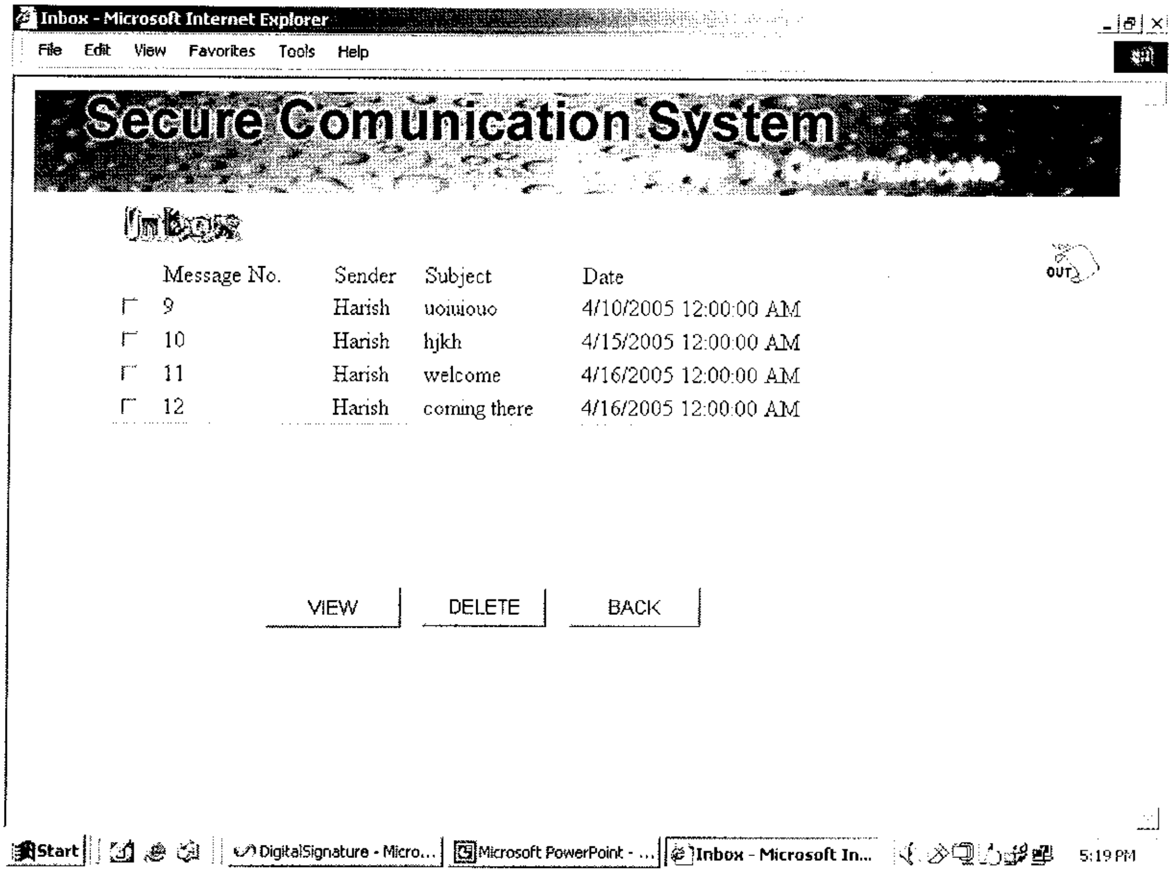
BoxOption - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Secure Comunication System
OUT
MAKE
YOUR
CHOICE
Start
DigitalSignature - Micro...
Microsoft PowerPoint - ...
BoxOption - Microso...
5:19 PM

Welcome nithya

* Inbox . . .
* Outbox . . .
* Compose . . .

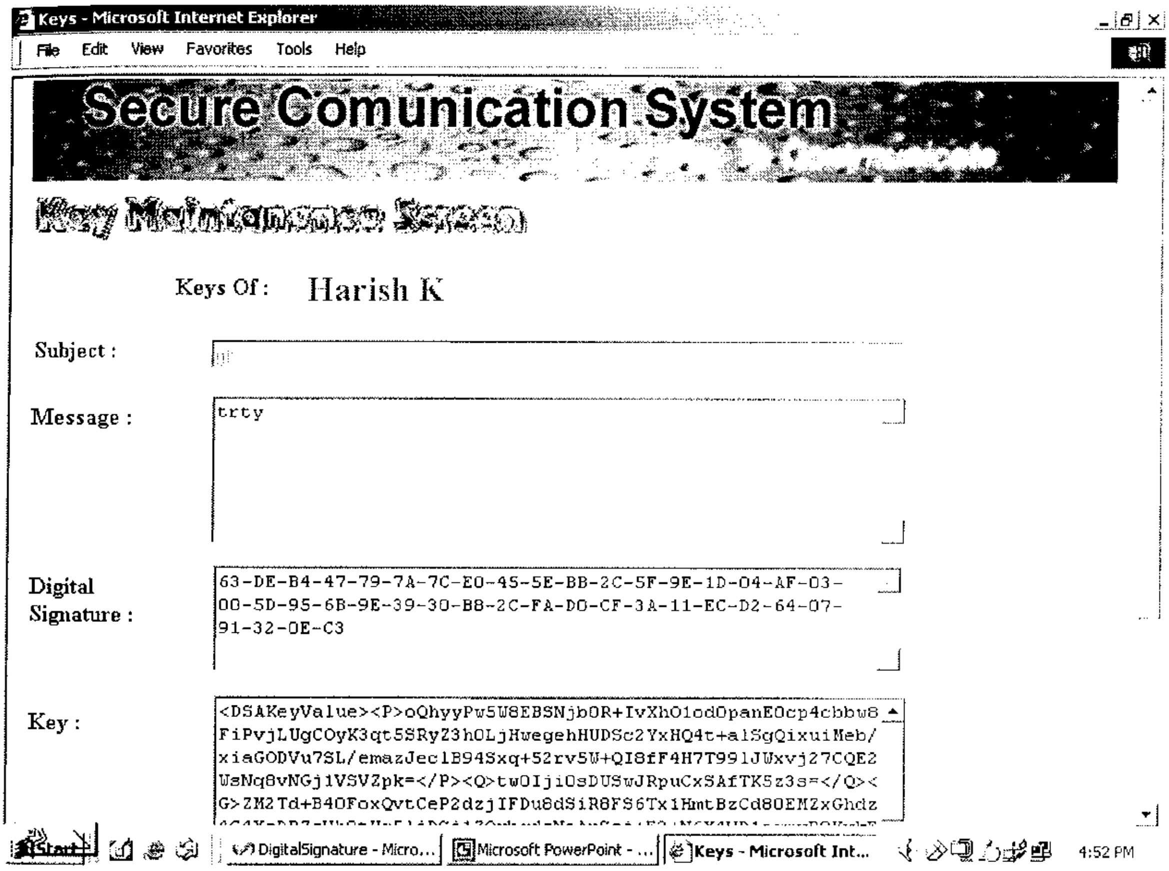
Click here to send message through email Email

Fig A.2 The Home Page


Inbox - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Secure Comunication System
Inbox
OUT
VIEW
DELETE
BACK
Start
DigitalSignature - Micro...
Microsoft PowerPoint - ...
Inbox - Microsoft In...
5:19 PM

	Message No.	Sender	Subject	Date
☐	9	Harish	uoiuiouo	4/10/2005 12:00:00 AM
☐	10	Harish	hjkh	4/15/2005 12:00:00 AM
☐	11	Harish	welcome	4/16/2005 12:00:00 AM
☐	12	Harish	coming there	4/16/2005 12:00:00 AM

Fig A.3 Inbox


Keys - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Secure Comunication System
Key Maintenance Screen
Start
DigitalSignature - Micro...
Microsoft PowerPoint - ...
Keys - Microsoft Int...
4:52 PM

Keys Of : Harish K

Subject :

Message : trty

Digital Signature :

```
63-DE-B4-47-79-7A-7C-E0-45-5E-BB-2C-5F-9E-1D-04-AF-03-
00-5D-95-6B-9E-39-30-B8-2C-FA-D0-CF-3A-11-EC-D2-64-07-
91-32-0E-C3
```

Key :

```
<DSAKeyValue><P>oQhyyPw5W8EBSNjbOR+IvXhO1odOpanE0cp4cbbw8
FiPvjLUgCOyK3qt5SRyZ3hOLjHwegehHUDSc2YxHQ4t+alSgQixuiMeb/
xiaGODVu7SL/emazJec1B94Sxq+52rv5W+QI8fF4H7T991JWxvj27CQE2
WsNq8vNGj1VSVZpk=</P><Q>tw0Iji0sDUSwJRpuCxSAfTK5z3s=</Q><
G>ZM2Td+B40FoxQvtCeP2dzjIFDu8dSiR8FS6Tx1HmtBzCd80EMZxGhdz
```

Fig A.4 The Key Maintenance Screen

REFERENCES

BOOKS

[1] Stephen Walther "Asp.net Unleashed", 2002 BPB Publications.

[2] Mridula Parihar "Asp.net Bible", 2004 Wiley Publishing, Inc.

[3] Ran Soukup and Kalen Delaney "Inside SQL Server 2000", 2001 Microsoft Press.

ONLINE REFERENCES

- www. w3schools.com
- www. microsoft.com
- www. devx.com
- www. asp.net
- www. dotnetspider.com