

p-977

SECURE DATA TRANSMISSION SYSTEM

PROJECT WORK DONE AT
SOFTEX COMPUTER CONSULTANTS Pvt. Ltd.
TECHNOPARK, TRIVANDRUM

PROJECT REPORT

SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS
FOR THE AWARD OF THE DEGREE OF
MASTER OF COMPUTER APPLICATIONS
OF BHARATHIAR UNIVERSITY, COIMBATORE.

SUBMITTED BY

ARAVIND.M.K
0038M1017



GUIDED BY

EXTERNAL GUIDE
Roshin Saran,
Project Leader,
SOFTEX,
Trivandrum.

INTERNAL GUIDE
Mrs. S. Devki, M.S.,
Assistant Professor,
Dept. of Computer Science & Engg.,
Kumaraguru College of Technology,
Coimbatore.



Department of Computer Science and Engineering
Kumaraguru College of Technology
Coimbatore - 641006
April 2003.



Department of Computer Science and Engineering
KUMARAGURU COLLEGE OF TECHNOLOGY
COIMBATORE – 641 006.



CERTIFICATE

PROJECT REPORT 2002 - 2003

Certified that this is a bonafide report of
the project work done by

ARAVIND.M.K

(Reg. No. 0038M1017)

S. Devaki

Mrs. S.DEVAKI, M S

Project guide

Computer Science & Engineering

S. Thangasamy

Prof. S. THANGASAMY, Ph.D.,

Head of the Department

Computer Science & Engineering

Place: Coimbatore

Date:

Submitted for viva-voce examination held on

16-04-03

G. Anand

Internal Examiner

S. Thangasamy

External Examiner

CERTIFICATE

This is to certify that Mr Aravind M K, a student of Kumaraguru College of Technology, Coimbatore has successfully completed the project work at our organization. The project he has undertaken is titled **Secure Data Transmission System**.

He is committed to his work and has exhibited excellent learning capabilities. I wish him all success for his future endeavors.



(Anil Nambiar)

H R Manager

DECLARATION

I here by declare that the project entitled **SECURE DATA TRANSMISSION SYSTEM** submitted to Bharathiar university as the project work of Master of Computer Applications degree, is the record of the original work done by me under the supervision and guidance of **Mr.Roshin Saran**, Softex Computer Consultants, Technopark Trivandrum and **Mrs.S.Devaki** (Asst Prof.), Dept of Comp Science and Engineering, Kumaraguru College of Technology, Coimbatore and this project work has not found the basis for the award of any degree / diploma / associateship / fellowship or similar title to any candidate of any university.

Place ~~8-04-03~~ COIMBATORE

Date 8-04-03



Signature of the student

Acknowledgement

I express my profound respect and gratitude to **Dr.K.K.Padmanabhan**, Principal, Kumaraguru College of Technology for his kind co-operation and allowing me to take up this project work

I record my sincere thanks to **Dr.S.Thangasamy** Head of the Dept, Comp Science and Engineering for allowing me to take up the project at Softex Computer Consultants Ltd, Technopark, Trivandrum

I wish to extend my gratitude to Softex Computer Consultants Ltd. Technopark, Trivandrum for allowing me to carry out the project at their organization and guiding me in completing the project work successfully.

I'm greatly privileged to express my deep gratitude to my guide **Mrs.S.Devaki**, Dept of Comp Science and Engineering, Kumaraguru College of Technology for her valuable advice and encouragement.

I also owe my sincere thanks to **Mr.Muthu Kumar**, Course Coordinator, Master of Computer Applications, Kumaraguru College of Technology, Coimbatore for his guidance and immense support throughout my project work.

I am highly indebted to **Mr.R.P.Lalaji**, Managing Director, Softex Computer Consultants Ltd, Technopark, Thiruvananthapuram to do this

project. I thank my project manager **Mr.Raju Harilal** and my external guide **Mr.Roshin Saran**, for the observations, innovative and useful suggestions towards the completion of my project.

I am thankful to all the staff members of the Department of Computer Science and Engineering, Kumaraguru College of Technology, for the various suggestions given to me.

Above all I thank the **LORD Almighty** for all His blessings.

Aravind M K

SYNOPSIS

The project entitled Secure Data Transmission System has been done for Softex Computer Consultants Pvt. Ltd .The product does encryption of textual data. It is ideal for systems in which there is high security risk in storing and transferring data. The product has been built in Microsoft Visual C++ 6.0. The package should be able to do the following.

- Selecting a data file which contains the plain text
- Encrypting the original plain text data to cipher text using some encryption method parameterized by a key
- Transmitting the encrypted data through a communication medium or network. (Internet, Intranet and the like).
- Decrypting the cipher text using the decryption key so as to get the original textual data
- This package ensures the secure transmission of messages from one machine to another machine through the network

CONTENTS

1. Introduction	
1.1 Project overview	8
1.2 Organization profile	9
2. System study and analysis	
2.1 Existing system available and its limitations	19
2.2 Proposed system	20
2.3 Requirements of the new system	21
2.4 User characteristics	22
3. Programming environment	
3.1 Hardware configuration	24
3.2 Software requirements and description	24
4. System analysis and development	
4.1 Input Design	33
4.2 Process Design	34
4.3 Output Design	38
5. System implementation and testing	
5.1 System testing	40
5.2 System implementation	47
5.3 System refinements and feedback	49

6. Conclusion	52
7. Scope for future development	55
8. References	57
9. Appendix	
9.1 Sample screens	60

1. Introduction

1.1 Project Overview

Objectives

The main objective of the project is secure data transmission system in a networking environment. Data transmitted from a computer system to another must be safe and correct and free from unauthorized disclosure of information, unauthorized alteration or destruction of information, unauthorized service, and denial of service to legitimate users. This is ensured using the idea of cryptography in the project.

Cryptography is concerned with keeping communications private. It provides a method for increasing the confidence in the secrecy of the information in transit and in the storage. The way used here to strengthen security in computer systems is to encrypt sensitive records and messages in transit and storage. It hence maintains computer security thereby maintaining the integrity, availability and the privacy of the information entrusted to the system.

The software developed will function on both sides of the communication system, i.e. in the client side and the server side. In this project data transmitted from an application is transmitted only to the intended user thereby maintaining user authentication. The objective is to minimize false acceptance and rejection ratios at reasonable cost and with high user acceptance.

1.2 Organization profile

Softex Computer Consultants (Pvt.) Ltd.

Pamba

Technopark

Trivandrum

Softex Computer Consultants is a leading software development and exporting company, that develops enterprise information management software, portal building Internet tools, e-commerce tools educational software, Multimedia applications etc. It is also specialized in Web Page designing and multimedia presentations with related consulting and outsourcing support services in all the above. Aimed at providing the lowest cost information technology infrastructure, Softex provide business and

competitive advantage through highly reliable professional support. Softex group consists of Softex computer consultants, Seaview Support Systems, Softxl Technology Services Ltd, National Institute of Computer Technology and Cosmomart.com Pvt. Ltd

Softex group situated at technopark Trivandrum is spread over an area of 12000sq.ft Softex being a 100% software-exporting unit licensed under the STP scheme of the govt. of India. This STP status of Softex bestows upon it an attractive set of privileges including duty free importing of hardware, software and several inputs to structure its infrastructure facilities.

Softex computer consultants (P) Ltd. develop readymade IT products and custom-made software solutions. They specialize in providing consulting for a wide range of software solutions including enterprise internet/intranet applications, mobile applications and games, client/server systems, etc. with their commitment to excellence and their extensive experience in software development they deliver effective and timely software solutions to their clients.

Siemens is bundling their mobile games along with their s145i phones in Singapore and South Asia. Siemens is also providing their mobile applications as content over carrier networks in Asia Pacific region using their mobile provisioning system.

Software expertise

Java 1.2, Enterprise Java Beans, Servlets, JDBC, JNDI, Java Server Pages,
XML, JavaScript, HTML, DHTML

Oracle 8i, Oracle Reports 6.0

Platform / OS

Linux, Solaris

Hardware

Client/Server Network
IBM S/390
IBM AS/400

Communication links

128K + 128K + 128K through three independent ISP's for redundancy

Services

1. Mobile applications and games

In addition to its large portfolio of mobile products, Softex also develops wireless applications and games for a number of clients. Their expertise in this area includes J2ME-MIDP applications and applications in personal java. They are also capable of developing wireless applications in C++ on the Symbian OS.

2. Enterprise internet applications

Softex has worked on a large number of intranet and Internet applications in domains that include eLearning, eBusiness, eHRM and ERP.

3. HL7 interface engines and messaging solutions.

Softex has developed HL7 interfaces solutions for a number of IT enabled services from catering to healthcare sector. The interface developed is capable of handling different existing vendor implementations of HL7.

4. MIS

Softex has developed traditional client server based systems for prestigious clients like Parthas (one of the largest textile showrooms in India), Nirmala Automobiles, and Seaview Support Systems.

5. Networking Applications

Softex has developed a number of networking applications ranging from a search engine based on agent technology, various agents like the FTP client/server monitors and the like.

6. Digital audio processing applications

Softex has developed audio processing tools such as digital audio filters and equalizers, noise reduction tools and other audio enhancement software. These products are currently deployed in large production environments.

7. Website designing and graphics

A team of UI designers and graphics artists can design websites suited to any requirement. Be it a corporate web site, academic institution, online store, online club or group site, etc. The UI team also develops high quality graphics for mobile devices.

Products

➤ Mobile applications

Mobile money minder

Quick Silver Messenger 1.0.1

MIDP games

Mobile scribe

➤ Internet and intranet applications

Overseer : HR management package

KnowHow : Knowledge management system

➤ Digital audio signal processing

➤ Educational multimedia packages

➤ Entrance examiner

➤ IT enabled services

Site monitor

➤ **Management information systems**

Scheduler

Cine ERP

➤ **Smart card technology**

Softex clients

They have built their success on enabling change- helping their clients adapt to new markets and better exploitation of existing ones. The success of their clients is important to them and they ensure that their services provide an excellent return on investment for their growing list of satisfied clients.

Their clients range from local businesses to multinational corporations and they are proud of the successes that have helped them to achieve. Softex has been privileged to work closely with a variety of individuals and the following companies to provide them with complete and reliable services. The clients include

- **Siemens**
- **WBT Systems Inc. Dublin, Ireland**
- **Anfy**

- Online Benefits Inc, Boston (USA)
- SoftXL Technologies (P) Ltd. Indo Irish joint venture
- VERIFONE Inc. Bangalore
- Parthas textiles
- Seaview Support Systems Pvt. Ltd,
- Cosmomart.com Pvt. Ltd.

Partners

Siemens mobile

The Siemens Information and Communication Mobile Group (IC Mobile) offers the complete range of mobile solutions including mobile devices, infrastructure and applications. Devices include mobile phones, wireless modules, mobile organizers and cordless phones as well as products for wireless home networks. The infrastructure portfolio includes GSM, GPRS and 3G mobile network technologies from base stations and switching systems to intelligent networks, e.g. for prepaid services. Mobile applications cover end-to-end solutions for Messaging, Location Based Services or Mobile Payment. For the fiscal year 2001 (September 30), IC Mobile recorded sales of EUR 11.3 billion and employed 30,730 people worldwide.

4th pass INC

4th Pass is a leading mobile provisioning system developer with customers like LG TeleCom, Research In Motion, Sun Microsystems and Telefonica. It's Mobile Application System is being adopted by wireless telecom carriers worldwide. Softex is also a member of the 4th Pass Midlet Alliance. 4th Pass is based in Seattle, USA.

Jippii Oyj.

The Jippii Group based in Finland, has portals in twenty countries. In addition to Internet and telecommunications services Jippii offers content and value-added services to both businesses and consumers. Jippii is also well known for its innovative research and development projects. The company has made major developments in mobile Java gaming and wireless Internet. Softex has partnered with Jippii for the marketing and distribution of mobile games and applications developed by Softex.

Pixo inc

Pixo is a leading developer of wireless infrastructure software. Its range of products include the Pixo Mobile Download server, Pixo Internet Microbrowser and Pixo OS. Pixo is based in San Jose, California.

2. System Study & Analysis

2.1 Existing system & its limitations

Modern and powerful encryption processes protect company data and confidential information exchanged over the Internet from unauthorized access by third parties. The 'Krypto Card' – a hardware encryption device with the size of a credit card has now been presented by the Fraunhofer Institute for Microelectric Circuits and Systems IMS in Dresden.

Extremely powerful mathematical algorithms are used today to encrypt important data. They convert text or other sequence of characters into an apparently random sequence of numbers and letters, which is meaningless. Only authorized recipients, equipped with appropriated decryption key are able to reconstruct the original information – a principle similar to encoded broadcasts on pay-TV.

A process now in common use is 'Data Encryption Standard (DES). Synchronous in this means that one and the same key is used for encryption and decryption.

A new hardware solution developed by researchers at the IMS is based on this standard. In contrast to software-based solutions, the Krypto Card can be used in laptops and Microsystems, which have insufficient room or power for high performance universal processors. A further advantage of hardware variant is that it operates extremely fast and effectively – processing at least a million characters per second with a key field width of 56 bits. Corresponding software solutions can only encrypt around 50,000 bits per second. If the key field width is increased to increase security, processing speed is lower – doubling the key field width reduces the speed by a third.

The new hardware solution, a personal computer memory card (PCMICA) is the size of a credit card and approximately 5 mm in thickness. In order to encrypt data, the Krypto card is inserted into the PCMICA drive of pc or laptop. ‘The user can encrypt the emails before sending them’ explains Dr. Andreas Heining of the IMS, or make company data or any number of files inaccessible to others. Similar technology is employed in the KryptoBox, which can be easily installed in existing data transmission systems.

2.2 Proposed system

The proposed system to develop secure data transmission system software should be user friendly and should cope with all needs of the user i.e., safe,

correct and free from unauthorized disclosure of information, unauthorized alteration or destruction of information, unauthorized use of service and denial of service to legitimate users. This is ensured using the idea of cryptography in the project.

The software developed will function in both sides of the communication system i.e. at the transmitters side and at the receiver's side. The application will open a temporary data file, write the data to be sent and the IP address of the machine to which the data has to be sent. At the destination the data is received and decrypted in the same format as it was sent.

2.3 Requirements of the new system

Easy to use interface is the primary concern. The user should not fear that he/she is using a complicated system and so must be very careful in usage nor should any complications be felt while using the system.

The system should not interfere in normal working of other processes nor cause any operating system violations.

Since this is a technical software, an extensive help system is required to guide new users in its usage.

After usage, any intermediate files created by the software should be removed from the system to avoid unauthorized access.

A text file is created recording the details including the most recent date on which the system was used, the time at which the system was used, etc.

2.4 User characteristics

The system is ideal for military and industrial use. This product can be used in situations whereby it is catastrophic to use conventional encrypting software as mentioned in the system study and limitations page. The system makes use of the text document files like notepad files, WordPad files, etc. Upon clicking some buttons one can easily encrypt or decrypt a text document and could be sent to a remote machine as per the requirement of the user.

3. Programming environment

3.1 Hardware configuration (minimum requirements)

Processor	Pentium 233 MHz
RAM	32 MB
Modem	standard
Ethernet card	10/100
Cable connection	twin coaxial
Hard disk	10 GB
Monitor	14" color
Keyboard	108 keys
Mouse	standard 2 button

3.2 Software requirements

Operating system

The system was developed in the Windows 98 environment, which is the most commonly used operating system today. The

windows environment is a boon for the users of DOS. The developed system will also work efficiently on other Windows platforms like Windows NT, Windows 95, Windows 2000, Windows ME and Windows XP.

The advantages of using the windows platform are

- Device independent program
- Pre installed code
- Standard user interface

Device independent programs : Windows lets you write device independent programs. You don't have to concern yourself with what type of printer, mouse, keyboard, printer, monitor, soundcard or other devices you own.

Preinstalled code : This is a very important feature of windows operating system. The application programmer can invoke the windows functions through his routines. This mainly makes use of the DLL files in windows.

Standard user interface : This mechanism is same for all windows applications. They make use of the buttons in the window like the OK and CANCEL and also maximize, minimize and close buttons.

Additional features of the windows operating system are

- Innovative easy to use features including
 - Web integration
 - Multiple display support
 - Power management
 - Universal Serial Bus
 - Accessibility wizard
 - Help

- Improved reliability by introducing new wizards, utilities and resources like
 - Windows update
 - System file checker
 - Scandisk
 - Registry checker
 - Backup

- A faster operating system using tools that help your computer run faster than Windows 95 without adding new hardware. Windows 98 includes a suite of programs designed to optimize computers efficiency, when used together.

Maintenance wizard

Drive converter

Disk defragmenter

- True web integration including

Improved web features

Internet connection wizard

Active desktop

Channels

E-Mail

Net meeting

Front page express

- Some more features are

Multitasking and multithreading support

Multiple connectivity support

Multiple environment support

Multiple platform support

Multiple client support

Language

The language used to develop the system is Visual C++. Visual C++ makes use of the Microsoft Foundation Class (MFC) library and facilitates the program by making use of a good number of tools like the menu editor and the dialog editor. VC++ provides the facility of various wizards that lead us through a step-by-step process of building the skeleton of the application. It also has a set of integrated debugging tools.

Some of the important facilities of VC++ include

- Code reusability
- Application wizards for MFC applications, DLLs, ActiveX Controls, ATL
- Integrated project development environment
- Portability across platforms

Visual C++ components are

Visual C++ 6.0 developer studio: an integrated application that provides a set of programming tools

Visual C++ 6.0 runtime libraries : these are standard libraries that provide standard functions like strlen, strcpy, etc. that can be called from a standard C or C++ methods

MFC and template libraries : the extensive c++ class library especially designed for creating GUI programs.

Visual C++ built in tools : it comprises of the C/C++ compiler, the linker, resource compiler especially designed for compiling resources and some other tools required for generating 32 bit windows programs.

ActiveX

Data Access Components (DAO) : this includes database drivers controls and other tools required by VC++ to interact with databases.

Enterprise tools : these are advanced tools like application performance explorer or visual studio analyzer

Graphics : consist of bitmaps, metafiles, cursors and icons available for inclusion in the application.

4. System Design and Development

Design is the first step in the development phase for every engineered product or system. Computer software designing, like engineering design approaches in other disciplines, changes as better methods, better analysis and broader understanding evolve.

System design involves translating information requirements and conceptual design into technical requirements of the firm, needs are identified, related information is gathered to verify the problem after evaluating the existing system, a new system is proposed. The proposed system consists of various modules, their maintenance and working and finally report generation.

For secure data transmission, developing an efficient system, which is user friendly as well as high in performance, is the main aim. It has been assured that the system will have functions and promises of the proposed system. In the design various techniques are used to present a simple efficient system.

4.1 Input Design

The collection of input data is the most expensive part of the system in terms of the equipment used and the no. of people involved. In input design, data is accepted for computer processing and input into the system is done through mapping via some map support or links.

In this project the user interface is done using a highly flexible and efficient input design. Input design is a process of converting user inputs into computer-based format. The project requires a set of information from the user to prepare a report, well-organized input data are needed from external application, which needs high security. The external applications like banking, military, etc. presents data in the form of messages or information in plain text files, which needs to be transmitted after encryption. These are accepted by the programmer in his project either by using input forms, which include push buttons, radio buttons, edit boxes, dialog boxes, etc.

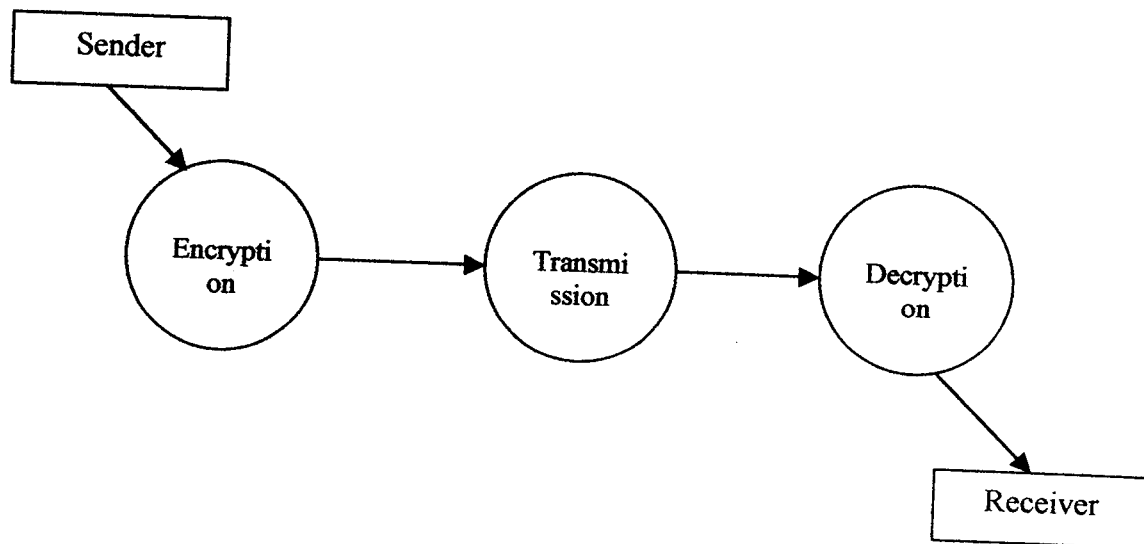
During the design time the programming task is accomplished by using keyboard and mouse to visually design and to write application. Here I have selected controls like push buttons, radio buttons and scroll bars with the

mouse, drag them to the application or to the designed dialog as it is built. In other words we will be able to see how the application will look like before executing it.

Input to the secure data transmission system is done through the selection of a text file or by typing the message to be encrypted in the edit box specified. The pass phrase, which is used to encrypt the message, is also given as the user input. Another source of input is the random number generator, which serves as the input vector.

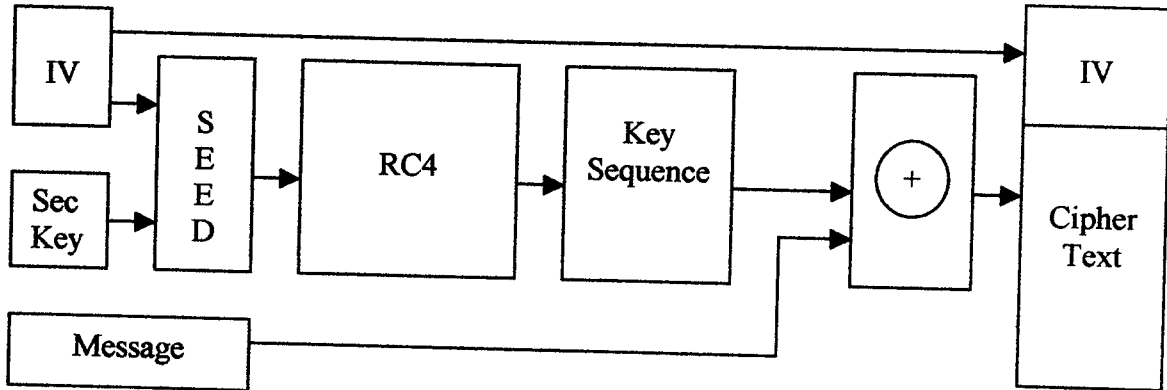
4.2 Process Design

The processes that take place in the system is as shown below.

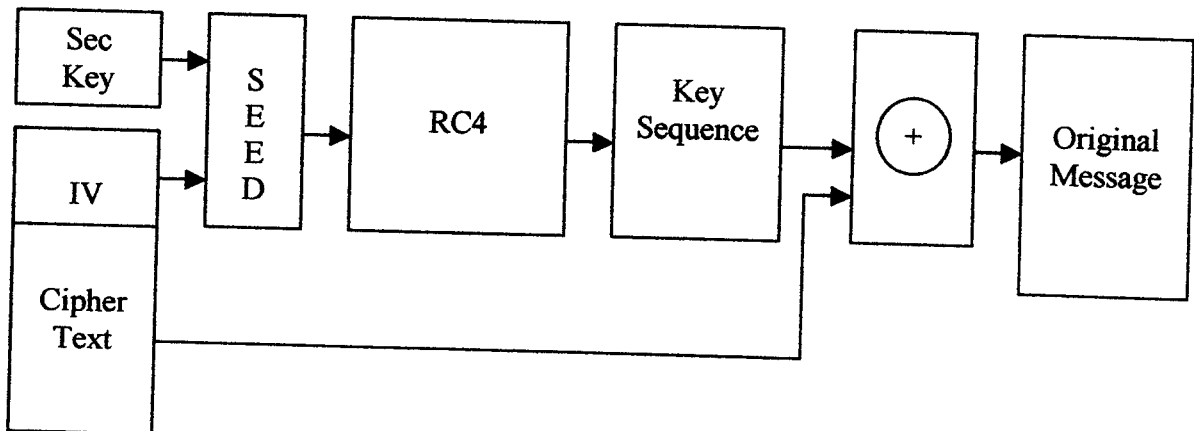


Functional Unit Diagrams

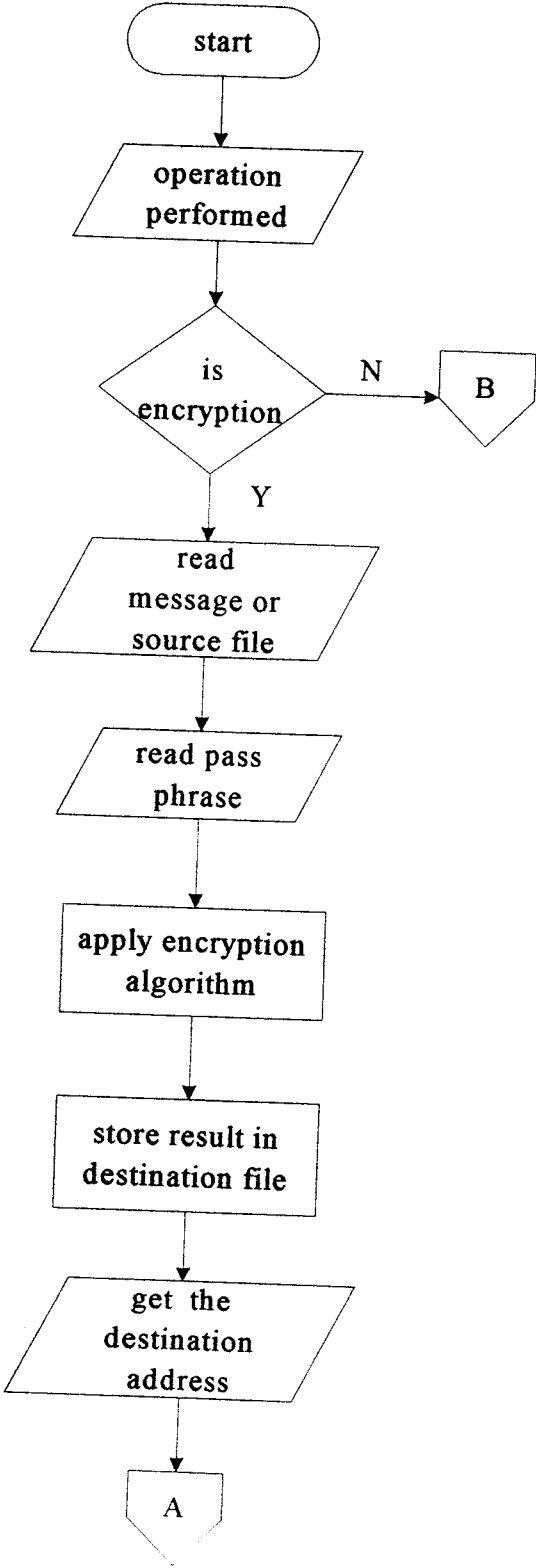
Encryption

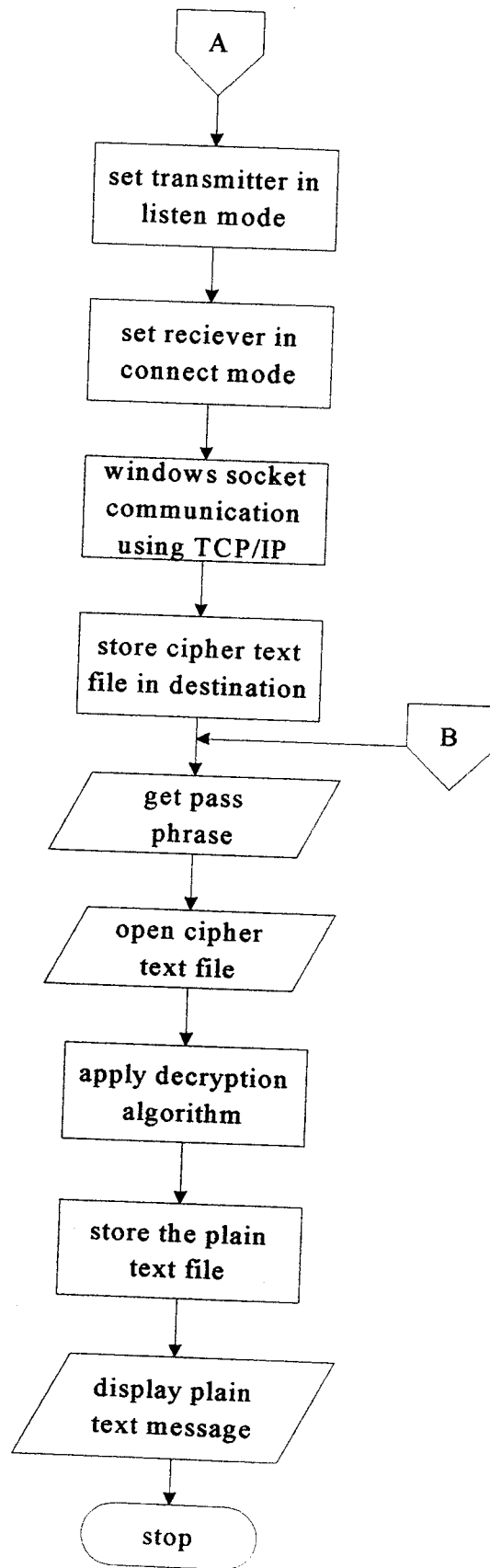


Decryption



Flow chart





4.3 Output Design

Output here means windows and forms. These forms displaying forms and dialogs are generated from stored or designed values. Various dialogs for data reception, data transmission, data encryption, data decryption, making connection, etc. are generated. Outputs are the most important and direct source of information to the user of the computer who wants to transmit secure data. Intelligent output design will improve the systems relationship with the user and help much in secure data transmission. Outputs are also used to provide a permanent hardcopy of results for later use. Output can be meant for the users as well as the management. To convey data securely to the intended recipient, output designs help to display any transmission errors, data losses, and useful information and warnings with the help of the message boxes as and when required in the course of the entire project.

5. System Implementation and Testing

5.1 System Testing

Testing is a set activity that can be planned in advance and conducted systematically. Testing begins at the module level and work towards the integration of the entire computer based system. Nothing is complete without testing, as it is vital for the system.

Testing objectives.

There are several rules that can serve as testing objectives. They are

- Testing is the process of executing a program with the intent of finding an error
- A good test case is one that has high probability of finding an undiscovered error.
- A successful test is one that uncovers an undiscovered error.

If testing is conducted successfully according to the objectives as stated above, it would uncover errors in the software. Also testing

demonstrates that the software functions are working according to the specification and the performance requirements are met.

There are three ways to test a program.

- For correctness
- For implementation efficiency
- For computational complexity

Tests for correctness are supposed to verify that a program does exactly what it was designed to do. This is much more difficult than it may at first appear, especially for large programs.

Tests for implementation efficiency attempt to find ways to make a correct program faster or use lesser storage. It is a code refining process, which re-examines the implementation phase of algorithm development

Tests for computational complexity amount to an experimental analysis of the complexity of an algorithm or an experimental comparison of two or more algorithms, which solve the same problem.

Preparation of test data

Test data should be prepared carefully since the data only determines the accuracy and efficiency of the system. Artificial data are prepared solely for the purpose of the testing. Every program validates the input data. Test files are used for performing testing. The test files have been provided to assist in the development of software being written to handle the specified format. These files do not always comply 100% of the written standard but do not represent files commonly found. They do not claim to cover all possible allowed variations but are a good starting point to test the software. If we cannot read these files then something is wrong.

In this project the data file is fed to the encryption module to perform encryption. The encrypted file should represent the correct encrypted information of the data file that was sent for encryption. This file being transmitted should retain the same old file after decryption process. All these test files should comply 100% of the written standard. The project was found good with the test data implemented correctly and securely.

Testing correctness

The following ideas should be part of any testing plan

- Preventive measures
- Spot checks
- Testing all parts of the program
- Test data
- Looking for trouble
- Time for testing
- Retesting

For the project secure data transmission, the output is verified by first accessing a message (data) that needs to be transmitted through the network. Data or the plain text message is entered and its original contents are verified. After the file has been fed to the encryption module, the data in the temporarily stored cipher text file is checked. One cannot read the original contents from it. Hacking becomes a problem, i.e. the encryption is a success. Again this cipher text data is transmitted through the system to intended user. The data received at the destination is checked with the records of the source system. If the original information is found to be the same at destination, there is no error in transmission or decryption. Hence data is purely correct and secure. The project completely follows the intended function. Care is taken while data is being entered and this has been taken as highest priority

while system testing. The data is entered in a prescribed file in a particular path.

While testing whenever an error is occurred, it is corrected then and there. A quality team deputed by the firm verified all the necessary documents and tested the software by entering the data. The entire testing was divided into 3 phases.

- Unit testing
- Integration testing
- Final/system testing

Unit testing

As this system is basically a network-based application, the following things were tested at each phase.

1. Accessing data
2. Encryption
3. Transmission
4. Decryption

In my system, unit testing has been successfully handled. The test data was given to each and every module in all respects and got the desired output. Each module has been tested and found to be working properly.

Code module testing

In this phase all the code modules were tested individually one after the other. The following were the important things that were tested

- Loop testing
- Boundary value analysis
- Equivalence partitioning testing

It was found that all the modules were working successfully without any side effects on other programs.

Final/System testing

This is the final step in testing. In this the entire system was tested as whole with all forms, code modules and class modules. This form of testing is popularly known as black box testing or system testing

Black box testing methods focus on the functional requirement of the software. That is, the black box testing enables the software engineer to derive sets of input conditions that will fully exercise all functional requirements for a program.

Black box testing attempts to find errors in the following categories; incorrect or missing functions, interface errors, errors in data structures or external data access, performance errors and initialization and termination errors.

User acceptance testing

The system considered is tested for user acceptance; here it should satisfy the firm's need. It should be done with the perspective of the user of the system at the time of development and making changes whenever required. This is done with regard to input screen design, output screen design, online message to guide user and the like.

5.2 System implementation

Implementation is one of the most important tasks in the project. Implementation is the phase in which one has to be cautious, because all the efforts undertaken during the project will be fruitful only if the software is properly implemented according to the plans made.

The implementation phase is less creative than the system design. It is primarily concerned with user training, site preparation and file conversion. Depending upon the nature of the system, extensive user training must be required. Programming itself is a design work. The initial parameters of the management information system should be modified as a result of programming efforts. Programming provides a reality test for assumptions made by the analyst.

System testing checks the readiness and accuracy of system access update and retrieve data from new files. Once the program becomes available, the test data are read into the computer and processed. In most conventions, parallel run was conducted to establish the efficiency of the system.

The secure data transmission system is implemented in the firm, where the prime need was security. The implemented software satisfied their need

and ensured correct transmission to the intended user and no problem of data loss or data authenticity.

The system implementation was carried out using five main aspects.

- Transition planning
- Training
- Security
- Protection
- Quality control

Keeping the above aspects in mind secure data transmission system was implemented accurately and efficiently in the firm.

5.3 Post implementation review

The step of systems approach recognizes that an implemented solution can fail to solve the problem for which it was developed. The real world has a way out confronting even the most well defined solutions. Therefore the results of implementing a solution should be monitored and evaluated. This is called post implementation review process, since the success of the solution

is reviewed after it is implemented. The focus of this step is to determine if the implemented solution has indeed helped the firm and the selected business units meet their system objectives. If not, the system approach assures to cycle back to a previous step and make another attempt find a better workable solution.

5.4 System Maintenance

The definition of software maintenance can be given by describing four activities that are undertaken after the program is released for use.

The first maintenance activity occurs since it is reasonable to assume that software testing will uncover all the errors in a large software system. The process of including the diagnosis and correction of one or more errors is called corrective maintenance.

The second activity that contributes to the definition of a maintenance activity occurs since rapid change is encountered in every aspect of computing. Therefore adaptive maintenance modifies the software to properly interact with a changing environment.

The third activity involves recommendations for new capabilities, modifications to the existing functions and the general enhancements when the software is used. To satisfy requests perceptive maintenance is performed.

The fourth maintenance activity occurs when the software is changed to improve future maintainability and reliability. This is called preventive maintenance.

This project is prone to all types of maintenance activities as they can be carried out quite well.

6. Conclusion

The project is fully functional as per requirements although the fact that clogging the system cannot be overlooked by huge volumes of data as the data has to be transmitted through the network. There are so many products for encryption available in the market. While undertaking this project I understood how it could be done, what are the challenges and significant advantages in implementing the system. The following objectives

- Encryption of an external system providing good security.
- Even if encrypted message get into unauthorized hands, there is no way of breaking it without the pass phrase
- The system can very quickly encrypt large volumes of data.

The system has been developed for the given conditions specified by the firm. The developed system is flexible and changes can be made easy and when required. Using the facility and flexibility of VC++ and windows 98, the software has been developed in a neat and simple manner by reducing the operator's work.

The system is highly flexible as well as efficient to make easy interactions with the client. The key focus is given on data security, as the product is working in a network. The data entered in a specified format is transmitted to the recipient without any data loss or eavesdropping or active line tapping.

Secrecy is maintained along with authenticity thereby ensuring computer security.

The user-friendly software successfully overcame strict validation checks performed using test data. Results obtained are fully satisfactory from the user point of view. The goal of computer security to maintain the integrity, availability and privacy of information entrusted to system was successfully obtained. An attempt was made to obtain maximum perfection in documenting the software in a simple, precise and self-explanatory manner. The system was verified with valid as well as invalid data in each module. The system is done with an insight into the necessary modifications that may be required in the future. Hence the system can be maintained successfully without much rework.

7.Scope for Future Development

The scopes of the project titled secure data transmission system are enormous. One can develop still speedier implementation of this software by using better algorithms and languages of their choice as they come.

Also in a vast developing environment like the networking field, more and more scope for data transmission still exists. Networking projects like this can make use of still more complicated design logics to produce a new and better one in any other working environment.

Another field of enormous scope is in the field of encryption of multimedia data. As audio files and video files can also be used for communication, the possibilities in this area are very high. Thus multimedia encryption is also of much significance.

8. References

1. Paul Yao & Richard .C. Linecker, Visual C++ 6.0 Programming Bible, Comdex Publishing
2. Charles Petzold, Programming Windows, Fifth Edition ,Microsoft Press, 1999
3. Yeshwanth Kanithkar, Visual C++ Programming, Tata McGraw-Hill
4. Kate Gregory, Using Visual C++ 6, Special edition, PHI,1998
5. Elias M. Awad, System Analysis and Design, Galgotia Publications
6. John Bates & Tim Tompkins, Practical Visual C++, PHI
7. Steve Burnett & Stephen Paine, RSA security's official guide to cryptography, RSA Press-Tata McGraw Hill, 2002
8. Bruce Schneier, Applied Cryptography, Second Edition, John Wiley & Sons

Internet resources:

<http://www.isaac.cs.berkeley.edu/>

<http://www.rsasecurity.com/>

<http://www.counterpane.com/whycrypto.html>

<http://csrc.nist.gov/encryption/>

<http://www.securitymanagement.com/library/000065.html>

<http://axion.physics.ubc.ca/crypt.html#Rivest>

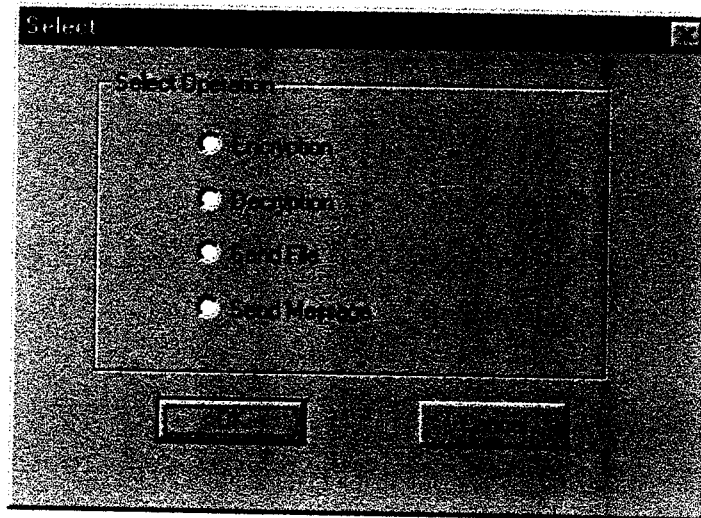
<http://www.cryptography.com/resources/index.html>

<http://www.counterpane.com/>

9. Appendix

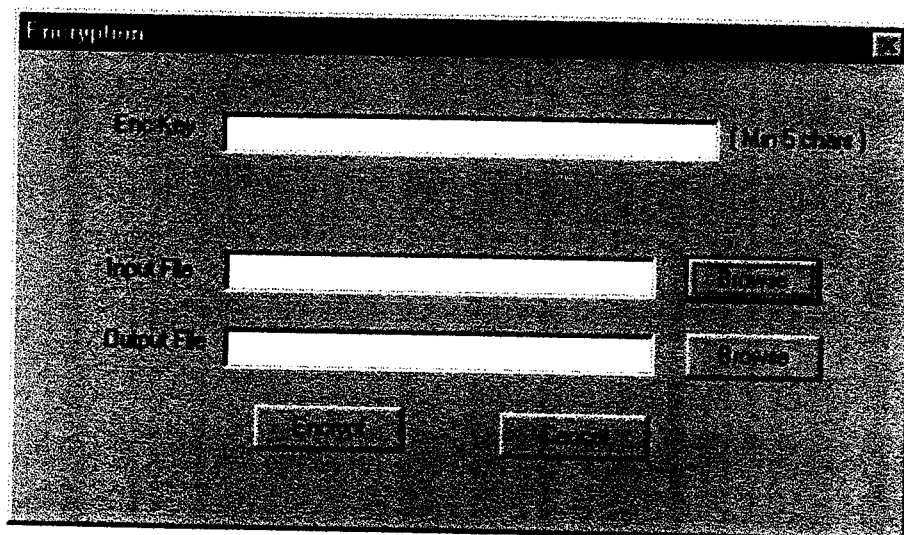
9.1 Sample Screens

Screen for selecting the operation to be performed.



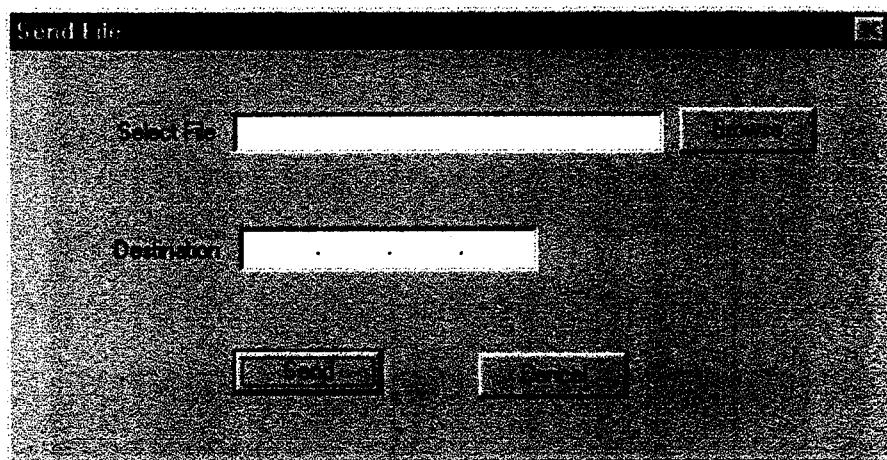
Encryption

Screen for selecting the file that has to be encrypted.



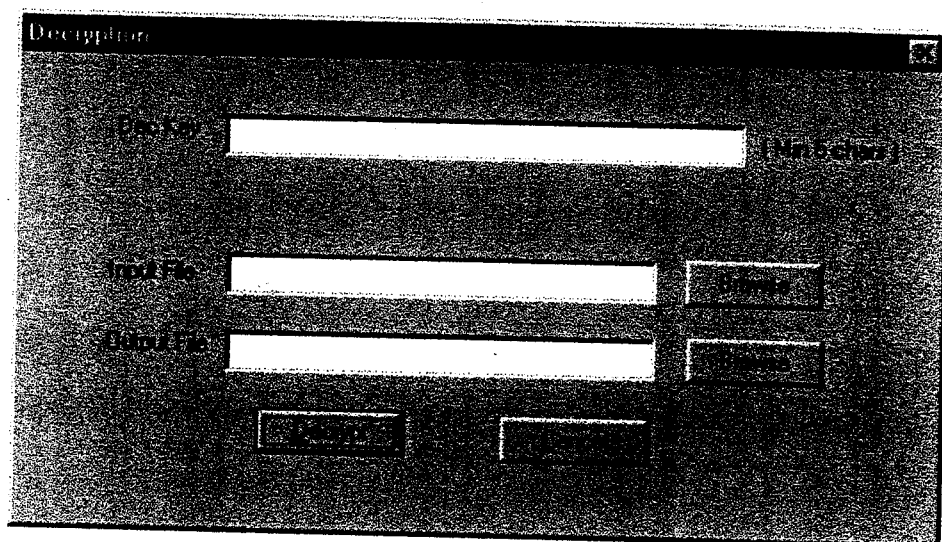
File transmission

Screen for specifying the destination of the file to be transmitted.



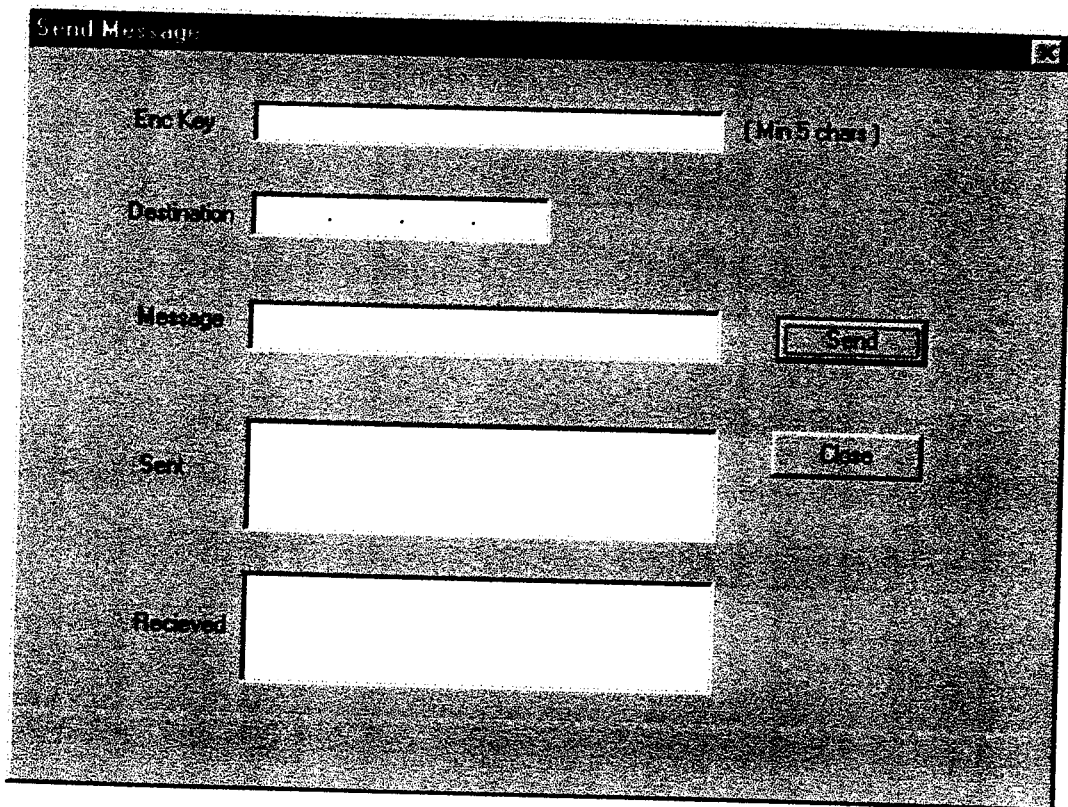
Decryption

Screen for selecting the file that has to be decrypted.



Send Message

Screen for sending message for from one machine to another by specifying the destination IP address.



The screenshot shows a window titled "Send Message" with a dark background and a light-colored title bar. The window contains the following elements:

- Enc Key:** A text input field with a label "Enc Key" to its left and "(Min 5 chars)" to its right.
- Destination:** A text input field with a label "Destination" to its left.
- Message:** A text input field with a label "Message" to its left.
- Sent:** A text input field with a label "Sent" to its left.
- Received:** A text input field with a label "Received" to its left.
- Buttons:** Two buttons are located on the right side of the window: "Send" (positioned to the right of the Message field) and "Clear" (positioned to the right of the Sent field).