

p-779  
**CRYPTOGRAPHIC COMMUNICATION SYSTEM**

PROJECT WORK DONE AT  
SakthiSri Infotech Pvt Ltd, Coimbatore

**PROJECT REPORT**

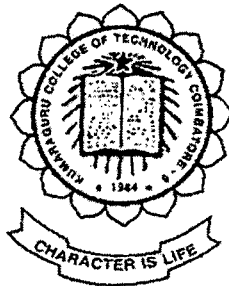
SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS  
FOR THE AWARD OF THE DEGREE OF  
**MASTER OF COMPUTER APPLICATIONS**  
OF BHARATHIAR UNIVERSITY, COIMBATORE.

**SUBMITTED BY**  
**P.KanagaSabapathi**  
Reg.No 9938M0610

**GUIDED BY**

**EXTERNAL GUIDE**  
Mr.V.Pradeep Kumar B.E

**INTERNAL GUIDE**  
Mrs.S.Devaki B.E.,M.S



Department of Computer Science & Engineering  
**KUMARAGURU COLLEGE OF TECHNOLOGY**

Coimbatore – 641 006

May 2002

Department of computer Science & Engineering

**Kumaraguru College of Technology**

(Affiliated to the Bharathiar University)

Coimbatore – 641 006

## CERTIFICATE

This is to certify that the project work entitled  
**CRYPTOGRAPHIC COMMUNICATION SYSTEM**  
Done by

**P.KanagaSabapthi**  
Reg.No 9938M0610

Submitted in partial fulfillment of the requirements for the award of the degree of  
**Master of Computer Applications of Bharathiar University.**

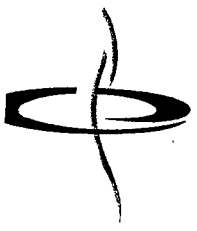
*S. Jeyaraj*  
30/4/02  
**Professor and Head**

*S. Arunali*  
30/4/2002  
**Internal Guide**

Submitted for the University Examination held on 9/5/2002

*[Signature]*  
9/5/02  
**Internal Examiner**

*[Signature]*  
**External Examiner**



**SakthiSri Infotech**

TO WHOMSOEVER IT MAY CONCERN

This is to certify that Mr.P.KANAGASABAPATHI final year M.C.A (Master of Computer Applications) student of Kumaraguru College of Technology, Coimbatore has successfully completed the project titled "Cryptographic Communication System" during the period January 2002 to April 2002.

Since the source code is of strict confidentiality it cannot be provided in any format.

We wish him all success in future endeavors.

For Sakthisri Infotech Pvt Ltd,

for V. Pradeep Kumar  
Project Co-ordinator

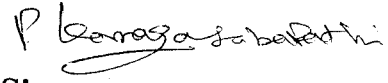
**SakthiSri Infotech (Pvt) Limited**

Floor, Srinivasaperumal Complex, 207, 100 Feet. Road, Coimbatore - 641 012. Telefax : + 91-422-498980. 495216  
Visit us : [www.sakthisri.com](http://www.sakthisri.com) e-mail : [sakthisricbe@yahoo.com](mailto:sakthisricbe@yahoo.com)

# DECLARATION

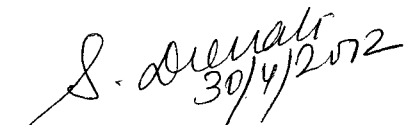
I hereby declare that the project entitled "Cryptographic Communication System", submitted to **Bharathiar University** as the project work of Master of Computer applications Degree, is a record of original work done by me under the supervision and guidance of **Mr.V.Pradeep Kumar B.E, SakthiSri Infotech Pvt Ltd, Coimbatore** and **Mrs.S.Devaki B.E.,M.S, Kumaraguru College of Technology, Coimbatore** and this project work has not found the basis for the award of any Degree/Diploma/Associate ship/ Fellowship or similar title to any candidate of any university.

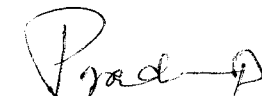
Place: COIMBATORE

  
Signature of the Student

Date: 30/4/2002

Countersigned by

  
(Internal Guide)

  
(External Guide)

**ACKNOWLEDGEMENT**

---

## ACKNOWLEDGEMENT

I express my heartfelt thanks to **Dr.K.K.Padmanabhan B.Sc(Engg).,M.Tech.,Ph.D**, Principal, Kumaraguru College of Technology, for having given me an opportunity to serve the purpose of my education

I am indebted to Prof **Dr.S.Thangasamy Ph.D**, Head of Department of Computer Science and Engineering, for his valuable guidance and useful suggestions during the course of project.

I am deeply indebted to my project guide, **Mrs.S.Devaki B.E.,M.S**, Asst Professor of Department of Computer Science and Engineering, Kumaraguru College of Technology, for her helpful guidance and valuable support given to me throughout the project.

With immense pleasure, I express my esteemed gratitude to **Mr.N.Venkatesan**, Managing director of Sakthisri Infotech Pvt Ltd, for providing me the opportunity to do the project in reputed organization.

I take privilege of expressing my sincere thanks to my external guide **Mr.V.Pradeep Kumar B.E**, for his keen interest and efforts in guiding and encouraging me throughout the project and also providing all necessary resources needed for the project in the organization.

I would like to thank all the staff members of the Department of Computer Science and Engineering of my college, for their constant encouragement and guidance throughout the course.

I would like to thank all, who have directly or indirectly assisted me in completing this project successfully.

**P.Kanagasabapathi**

**SYNOPSIS**

## SYNOPSIS

This project titled “**Cryptographic Communication system**” has been developed for SakthiSri Infotech Pvt Ltd, Coimbatore.

This “**Cryptographic Communication System**” will work on Intranet only. This system is very useful to send and receive secret messages because all the messages will be sending on intranet in the encrypted form. So no one can understand this encrypted message. In this new system one of the famous public key cryptographic algorithms has been implemented. This system consists of three options. They are,

1. Chatting.
2. Mailing.
3. File.

The RSA algorithm has been implemented in this software. This RSA algorithm is Asymmetric key or Public Key algorithm. It provides two keys. One is public key and another one is private key. The public key is used to encrypt the message and the private key is used to decrypt the encrypted message. The length of the key is 24 bit and the text length is 16 bit.

The Chatting system is used to send online messages to the current users. All the users should be know the public key of all other users. Using receiver’s public key will encrypt the plain text and the encrypted message will be sent to receiver by using the IPaddress of that receiver’s system.



The Mailing system is used to send offline messages to the registered users. The message to be sent is encrypted using receiver's public key and it will be sent to receiver. In the receiver end cipher text or encrypted message is decrypted using private key of that particular receiver. Now the original message or plaintext will be displayed. Mailing system consists of Check Mail and Compose options.

The third option is used to encrypt the files and some important documents. This is useful to keep our personal information secure.

This Cryptographic software has been developed using Visual Basic 6.0 Professional Edition as Front end and Ms Access as the Backend for the database under Windows NT Operating System.

**CONTENTS**

# TABLE OF CONTENTS

<b>1. Introduction</b>	
1.1 Project Overview	1
1.2 Organization Profile	2
<b>2. System Study and Analysis</b>	
2.1 Existing system – Limitations	4
2.2 Proposed system	5
2.3 Requirements on new system	6
2.4 User Characteristics	7
<b>3. Programming Environment</b>	
3.1 Hardware configuration	8
3.2 Description of software and tools used	9
<b>4. System Design and Development</b>	
4.1 Input Design	18
4.2 Output Design	20
4.3 Process Design	21
4.4 Database Design	27
<b>5. System Implementation and Testing</b>	
5.1 System Implementations	29
5.2 System Testing	30
<b>6. Conclusion</b>	33
<b>7. Scope for future development</b>	34
References	
Appendices	35

## **INTRODUCTION**

---

# 1. INTRODUCTION

## 1.1 Project Overview

“**Cryptographic Communication System**” is very useful software to send and receive messages within the Intranet with better security. **Cryptography** is the process of encryption and decryption of data. This method is used to send and receive secret messages in secure manner on network. In this “**Cryptographic Communication System**”, the famous RSA Asymmetric algorithm has been implemented. It is very easy to implement this RSA algorithm and it gives strong security than symmetric key algorithms by providing two separate keys for encryption and decryption.

This Software involves the following steps,

- Choosing the application among Chatting, Mailing and File.
- If it is Chatting, encrypt the message using the receiver’s public key and send it to the receiver by using IPaddress of the receiver’s system.
- Receiving the encrypted message and decrypt the encrypted message to get the original message by using receiver’s private key.
- If it is Mailing, encrypt the message using receiver’s public key and send it to the receiver by using receiver’s Mail\_id.
- Receiving the encrypted message and decrypt the encrypted message by using receiver’s private key.
- If it is File, select the file to be encrypted and set the path to store the Encrypted file. Encrypt the selected file by using our public key.

- To decrypt the encrypted file, select the encrypted file and set the path to store the decrypted file. The private key is used to decrypt the File.

In **Data encryption**, a plaintext message is encoded by using RSA algorithm. Encryption is the process of converting plaintext into some unreadable form; the encrypted text is called **ciphertext**. The message can be ASCII text, a database file or any text data that you want to store or transmit secure. When the message is encrypted, an encryption key is used. This key is called public key.

In **Data Decryption**, ciphertext is decoded using the same algorithm, which is used for encryption. To decrypt the message, the corresponding decryption key must be used. This key is called private key.

## 1.2 Organization Profile

The company SakthiSri Infotech Pvt Ltd is one of the leading software consultancies in Coimbatore. Mr.N.Venkatesan is the Managing Director of this company. He had been in the computer field for the past 15 years.

The organization has developed software for various concerns located in and around coimbatore. The organization has more than 200 clients for whom they develop various software.

The organization currently has 18 staff members. In these, three persons are in sales, two in customer support and ten in software development.

The main focus of SakthiSri Infotech Pvt Ltd is the business of software training, software development and consultancy services, Projects and Products.

### **Technology Services**

SakthiSri Infotech Pvt Ltd provides project management and contract services for the analysis, design, programming, and implementation of Internet Commerce, Client Server, and enterprise-wide business applications. They develop Internet and data communications systems along with legacy systems to GUI interface middleware applications that utilize the latest Java based technologies. They have experience with a wide range of platforms, networks, databases, and languages.

### **Staffing Services**

SakthiSri Infotech Pvt Ltd recruiting process starts with a complete understanding of the needs which are then entered into the system which scans a number of databases for qualified matches, then they contact the candidates, ensure their resume and skills are accurate and up to date, establish their interest in your position, and agree on the terms and availability. Sakthisri Infotech performs technical interviews and follows up with a minimum of five reference checks.

# SYSTEM STUDY AND ANALYSIS



## 2. SYSTEM STUDY AND ANALYSIS

### 2.1 Existing system - Limitations

The Existing system is “**Cryptographic Chatting system**” in which DES algorithm has been implemented. This DES algorithm is a symmetric key algorithm that is only one key will be used for both encryption and decryption. To develop the chatting application, Winsock ActiveX control has been used and UDP(User Datagram Protocol) protocol has been set to transmit data between the systems.

Limitations of the Existing system:

- We cannot send the message to more than one user at a time by using this software.
- There is no guarantee that whether the message will be delivered or not, because UDP protocol is a connectionless protocol.
- It is very difficult to send the key to the receiver secure.
- There is no option to encrypt the file or document.
- There is no option to send offline messages to the users.

## 2.2 Proposed System

The Proposed system, **Cryptographic Communication System**, will work on Intranet only. This system consists of three options. They are,

1. Chatting.
2. Mailing.
3. File.

RSA algorithm has been implemented in the Proposed system. This RSA algorithm is Asymmetric key or Public Key algorithm. It is very easy to implement this RSA algorithm and it provides strong security than symmetric key algorithms. This algorithm provides two keys. One is public key and another one is private key. The public key is used to encrypt the message and the private key is used to decrypt the encrypted message. The encrypted message is called cipher text. The length of the key is 24 bit and the text length is 16 bit.

TCP protocol has been used to transmit the message from one system to another system in this software. This TCP protocol is Connection oriented protocol. So when we connect our system with others, this protocol creates one virtual circuit between these two systems. Through this circuit only all the data transmission takes place. Now it is sure that the message will be delivered to the receiver correctly.

This Chatting system is used to send online messages to current users. All the users should be know the public key of all other users. The plaintext will be encrypted by using receiver's Public Key and the Encrypted message will be sent to the receiver by using the IPaddress of the receiver's system.

The Mailing system is used to send offline messages to the registered users. The message to be sent is encrypting using public key of the receiver and

this message will be sent to the receiver. The receiver can decrypt the cipher text using private key. Now the original plaintext will be displayed.

The third option is used to encrypt the files and some important documents. This is useful to keep our personal information securely.

## **2.3 Requirements on New System**

Existing system has lot of disadvantages. In order to overcome these limitations of the existing system and to improve the performance of the existing system, this new system has been proposed and developed.

Now the RSA Asymmetric algorithm has been implemented in this new system, so there is no need to send the encryption key to the receiver to decrypt the message as in the Symmetric key algorithm.

To develop this software we need RSA algorithm, Winsock ActiveX control, Tcp protocol and some basic controls in visual Basic. We need LAN or Intranet connection to run this Cryptographic Communication System.

This public key algorithm provides better security than Symmetric key algorithms.

This new system provides options to encrypt the file and to send mail to others. So users can send offline messages to others by using this mailing option.

## **2.4 User Characteristics**

User should be known the public key of the other users and both public key and private key of his system.

User should be aware of something about encryption and decryption, algorithm, others mail-id and System name or Ipaddress of the receiver.

**PROGRAMMING ENVIRONMENT**

---

### **3. PROGRAMING ENVIRONMENT**

#### **3.1 Hardware Configuration**

- Operating System : Windows NT
- CPU : Pentium III 850 MHz
- RAM : 64 MB RAM
- Hard Disk drive : 10 GB
- Cache Memory : 256 KB
- Floppy Disk Drive : 1.44 MB
- Monitor : SVGA SAMTRON 45Bn  
Color
- Keyboard : 104 Keys
- Mouse : Logitech

## **3.2 Description of Software and Tools used**

Front End : Visual Basic 6.0

Back End : Ms Access

Plate Form : Windows NT

### **About Microsoft Visual Basic 6.0**

Visual Basic is an ideal programming language for developing sophisticated professional applications for Microsoft Windows. It makes use of Graphical User Interface for creating robust and powerful applications. Coding in GUI environment is quite a transition to traditional, linear programming methods where the user is guided through a linear path of execution and is limited to a small set of operations.

The most significant features included are as follows.

#### **Native Code Compilation**

VB6.0 is the first version of Visual Basic to offer ability to generate executables in native code format. Native code is code that can be executed directly by the operating system without requiring the assistance of another layer of software known as the interpreter to carry out their instructions. Visual Basic programs can now be compiled to native stand-alone code, if one requires, one can still compile to Pseudo-code (P-code).

#### **Creating ActiveX Controls**

ActiveX control creation is an exciting new VB capability that greatly expands the range of software a Visual Basic programmer can provide. ActiveX controls serve as the building blocks for other programs and Web pages. It is a set of component technologies that can be integrated by other applications.

### **Interface Enhancements**

You can now configure almost all aspects of your working VB environment to suit the way you like to work.

### **Add-ins**

The much more robust and fully Object-Oriented Visual Basic hierarchy makes it easy to create your own add-ins and wizards and seamlessly integrate them with the VB IDE.

### **Firing Events**

In Visual Basic 6.0, custom events are a reality. Events are fired using the Raise Event statement and received with the help of the With Events keyword.

### **Multiple Projects**

It is possible to work with multiple projects simultaneously.

### **Database Connectivity**

Visual Basic applications can connect to any external database with an ODBC driver installed.

### **Reason for choosing Visual Basic**

Visual Basic provides a powerful environment for developing graphical user interfaces. The available graphic algorithms are efficient enough and give a good performance in visual basic. The development of the application which requires both graphical user interface combined with graphic algorithms are met with Visual Basic and has therefore been selected to develop this project.



## **Windows NT**

Windows NT has many features that place it in the upper ranks of Operating systems for microcomputers and workstations. Windows NT is a multitasking, multithreading, and scalable operating system with easy graphical user interface and compatibility with DOS and Windows 95.

The major features of Windows NT are listed below.

- Portability of programs to other machines.
- Multitasking and Multithreading.
- Multiprocessor support.
- Scalability so as to increase performance.
- Internet services.

### **Multi processor Support**

Windows NT supports the use of more than one processor on a complete running NT. Windows NT provides support for computers with symmetric, multiprocessor setups.

### **Multi platform Support**

Windows NT runs on a number of powerful desktop platforms. You can run Windows NT on RISC based platforms such as R3000, R4000, DEC Alpha AXP machines.

### **Multitasking and Multithreading**

Windows NT truly lets you do more than one task at a time. Windows NT uses a pre-emptive multitasking scheme to manage multiple applications. Rather

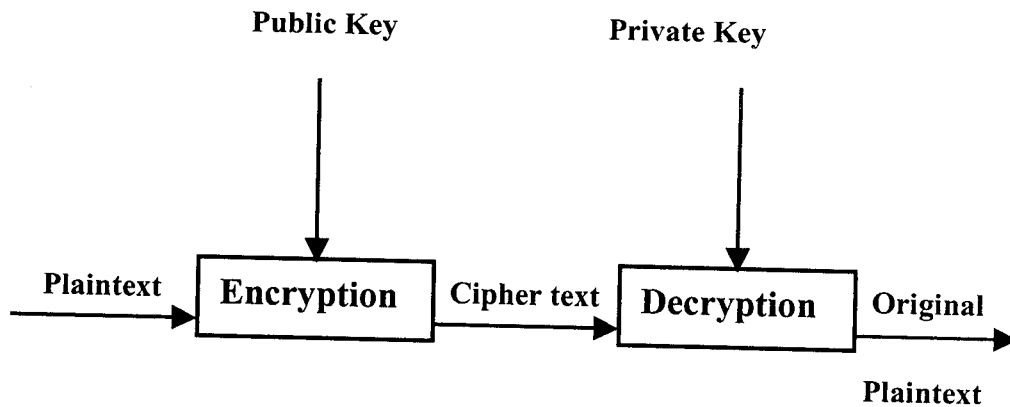
than applications co-operatively releasing control to the CPU to other applications. NT's pre-emptive multitasking system lets the CPU manage its own time.

Windows NT is a secure system and it offers the flexibility of securing individual files instead of entire directories or drives.

## **Asymmetric Encryption**

Public/private key pairs are used for a more secure method of encryption called asymmetric encryption. Asymmetric encryption is used mainly to encrypt and decrypt session keys and digital signatures. Asymmetric encryption uses public-key encryption algorithms.

Public-key algorithms use two different keys: a public key and a private key. The private key member of the pair must be kept private and secure. The public key, however, can be distributed to anyone who requests it. The public key of a key pair is often distributed by means of a digital certificate. When one key of a key pair is used to encrypt a message, the other key from that pair is required to decrypt the message. Thus if user A's public key is used to encrypt data, only user A (or someone who has access to user A's private key) can decrypt the data. If user A's private key is used to encrypt a piece of data, only user A's public key will decrypt the data, thus indicating that user A (or someone with access to user A's private key) did the encryption.



*Figure: Asymmetric encryption.*

If the private key is used to sign a message, the public key from that pair must be used to validate the signature. For example, if Alice wants to send someone a digitally signed message, she would sign the message with her private key, and the other person could verify her signature by using her public key. Since presumably only Alice has access to her private key, the fact that the signature can be verified with Alice's public key indicates that Alice created the signature.

Unfortunately, public-key algorithms are very slow, roughly 1,000 times slower than symmetric algorithms. It is impractical to use them to encrypt large amounts of data. In practice, public-key algorithms are used to encrypt session keys. Symmetric algorithms are used for encryption/decryption of most data.

It is difficult to determine the quality of an encryption algorithm. Algorithms that look promising sometimes turn out to be very easy to break, given the proper attack. When selecting an encryption algorithm, it is often a good idea to choose one that has been around for a while, and has successfully resisted all attacks.

Plaintext is denoted by  $M$ , for message. It can be stream of bits, a text file, or html document. Cipher text is denoted by  $C$ : sometimes the same size as  $M$ , sometimes larger. The encryption function  $E$ , operates on  $M$  to produce  $C$ . Or, in mathematical notation:

$$E(M) = C$$

In the reverse process, the decryption function  $D$  operates on  $C$  to produce  $M$ :

$$D(C) = M.$$

Since the whole point of encrypting and then decrypting a message is to recover the original plaintext, the following identity must hold true:

$$D(E(M)) = M$$

## About RSA Algorithm

RSA stands for Rivest, Shamir, and Adleman, they are the inventors of the RSA cryptosystem. RSA is one of the algorithms used in PKI (Public Key Infrastructure), asymmetric key encryption scheme. RSA is a block cipher, it encrypt message in blocks (block by block).

RSA can be used for security (encryption), confidentiality (signature), and key exchange purposes. Nowadays, it is often used for signature and key exchange only, this is because the encryption and decryption are slow, and it consumes times.

RSA security is so much depends on the difficulty of factoring large prime number. At this time the calculation required to find the factor the value to break the key is slow, many cryptanalysts consider that linear attack and differential attack are difficult to applied in RSA, only mathematical attack and brute force

are feasible, but the time needed to use these attacks are quite long, therefore they are considered as impractical. May be later in the future as computer speed increased, this encryption algorithm may consider insecure and unused, but don't forget we can just simply increase the size of the key to prevent it from attacker. The common size for the key length now is 1024 bits for P and Q, therefore N is 2048 bits, if the implementation (the library) of RSA is fast enough, we can double the key size.

Below is the RSA algorithm for creating key and to encrypt and decrypt the message.

### Creating keys

1. Generate (find) two large prime numbers (P and Q)
2. Calculate  $N = PQ$
3. Calculate  $M = \phi(N) = (P - 1)(Q - 1) =$  (Euler totient function)
4. Select any integer E, the rules to select E are:
  - a. E is positive integer
  - b.  $0 < E < M$
  - c.  $\text{GCD}(M, E) = 1 \dots$  (GCD = Greater Common Divisor)

Note: It is recommended to use  $E = 65537$  (17 bits).

5. Calculate D a use Extended Euclid Theorem (mod inverse)

$$(E * D) = 1 \pmod{M}$$

$$(E * D) \pmod{M} = 1$$

**Public key** : E, N

**Private key** : D and N

**Encryption** :

Original plain text (a block value) = X ...  $X < N$

Chipertext = C ...  $C = (X^E) \pmod{N}$

**Decryption** :

Chipertext = C

Dechipertext = Y =  $(C^D) \pmod{N}$

If everything goes fine, the value of Y and X should be equal ( $Y = X$ ), otherwise there is something wrong with the program (implementation).

Note that both encryption and decryption in RSA involve raising a large integer power followed by mod operation. If the exponential is first done over the two values and then reduced by the modulo, this operation requires very big space and many computing power, but we can reduce (divide) the exponent value by 2 then continue with mod operation, repeating this simple operation is faster and use less space and less computing power. A SIMPLE pseudo code for this algorithm is below:

E = exponential value,  
M = message to encrypt,  
N = modulo value  
C = chipertext value  
C = 1 ... set it as default value

While E

If E is odd

$C = C * M$

$C = C \% N$

$E = E / 2$

$M = M * M$

$M = M \% N$

While Loop

The main advantage of RSA algorithm is that it is feasible for applications with limited memory (e.g.: smart cards) .

The main disadvantage of RSA algorithm is that it is very slow when compared to Symmetric key algorithms.

## **Speed of RSA**

In hardware, RSA is about 1000 times slower than DES. The fastest VLSI hardware implementation for RSA with a 512-bit modulus has a throughput of 64 kilobits per second. There are also chips that perform 1024-bit RSA encryption.

In software, DES is about 100 times faster than RSA these numbers may change slightly as technology changes, but RSA will never approach the speed of symmetric algorithms.

**SYSTEM DESIGN AND DEVELOPMENT**



## **4. SYSTEM DESIGN AND DEVELOPMENT**

### **4.1. Input Design**

Input design is the part of overall system design that requires careful attention and it is most important phase. Input to the system is very important and it should be validated. According to the input only we can get accurate output. So input data should be validated before processing starts.

Objectives during input design are as follows,

- a. Achieve high level accuracy
- b. Ensure input is free of ambiguity

Input design involves converting the user-originated inputs into a computer-based format. The aim of input design is to make data entry easier and logical error free. It helps us to filter errors in the input data that otherwise entered into the database might have brought in a lot of consistency.

It involves procedures for capturing data, verifying and then passing them on to system. After choosing input medium, attention is focused on designing of error handling, control, and grouping and validation procedures.

During application development, care has been taken to make the proposed system extremely user friendly and organize the screens such that the possibilities of making error are maintained.

Input to this system is only the text data. We cannot give images and pictures as input.

If it is Chatting system, the user should give the following inputs.

In the New user form,

1. User Name
2. Password1
3. Password2
4. Designation

In the Authentication form,

1. User Name
2. Password

In the Chatting form,

1. Message to be sent
2. Receiver's Public Key
3. Ippaddress
4. Private Key

When we use the Mailing system, the user should give the following inputs.

In the new user form,

1. User Name (ex : kanagu@sri.com)
2. Password1
3. Password2
4. Designation

In the Authentication form,

1. User Name
2. Password

In the Compose form,

1. Receiver's Mail-id
2. Message to be sent
3. Receiver's Public Key
4. Private Key

If it is File option, the user should provide the following inputs.

When you encrypt the file,

1. File name to be encrypted
2. Public key (Encryption key)
3. Output File name with path

When you decrypt the file,

1. File name to be decrypted
2. Private key (Decryption key)
3. Output File name with path

## **4.2 Output Design**

An inevitable activity in the system is the proper design of input and output in a form acceptable to the user. Outputs from the system are required primarily to communicate the result of processing to user.

An output also provides a permanent copy of the results for later consultation. An intelligible output design will improve system relationships with the user and help in the decision making process.

The approach to output design is very dependent on the input and the nature of data. Special attention has to be made to data editing. The choice of appropriate output medium is also an important task. The output design must be

specified and documented; data items have to be defined and arranged for clarity and easy comprehension.

If it is Chatting system, the output will be as follows,

1. Encrypted message or Plain message
2. Name of the sender

If it is Mailing system, the output will be as follows,

1. Encrypted message or Plain message
2. Mail-id of the sender
3. Subject
4. Date

If it is file option, the output will be an Encrypted file when we encrypt the file and the output will be an original or plaintext file, when we decrypt the file.

### **4.3 Process Design**

A computer procedure is a series of operations designed to manipulate data to produce output from a computer system. A procedure may be a single program or set of programs. Simple definition of process is program under execution.

The process design is the heart of the system design. The system specification is designed here. In this software, encrypting the data, sending and decrypting the data are main processing activities.

Accurate process in the encryption side is as follows,

- Dividing the given message into number of blocks but each block should be 16-bit block.

- Converting the first 8-bit from the first block from the given message into its ASCII value. Then the ASCII value is converted into byte.
- Left shifts the first 8-bit value by performing AND operatin between the first s bits vale and the hexadecimal number h100.
- Converting the second 8-bit value from the first block into its ASCII value. Then the ASCII value is converted into byte.
- Add the second 8-bit value with first 8-bit value. Now we can get only one value for first block.
- Then the original value of first block will be converted into some other number by using encryption formula.
- The new value of the first block is converted into two 8-bit number by performing some operations.
- Converting these two values into characters. Now two some other characters will be displayed instead of first block original data. This is called cipher text. We cannot understand this text.
- Repeat step1 to setp8 to convert all the blocks into cipher text. Now the whole encrypted message will be displayed.

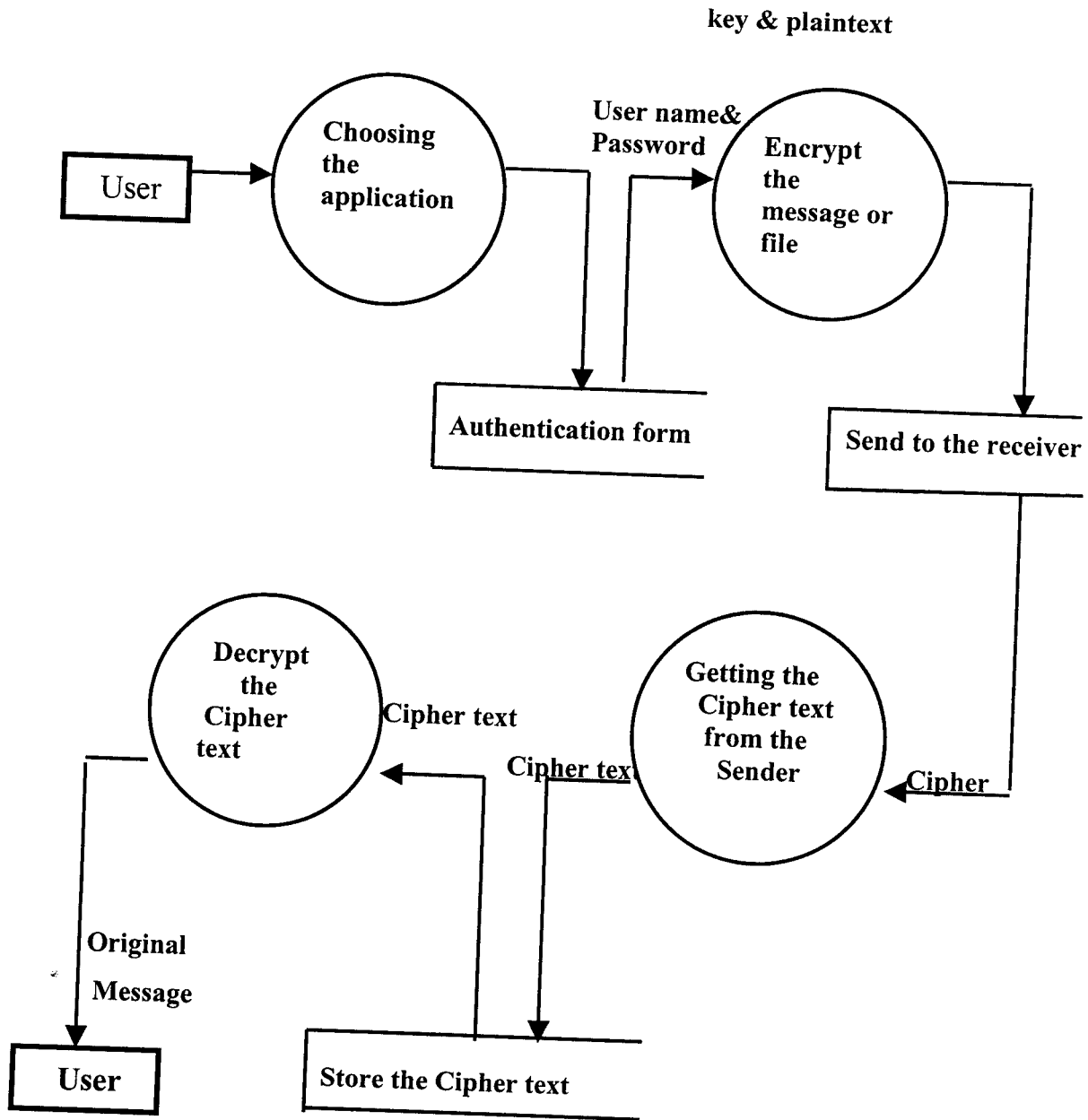
When we decrypt the encrypted message following process will be happen,

- Dividing the encrypted message into number of blocks but each block should be 16-bit block.
- Converting the first 8 bit from the first block from the into its ASCII value. Then the ASCII value is converted into byte.

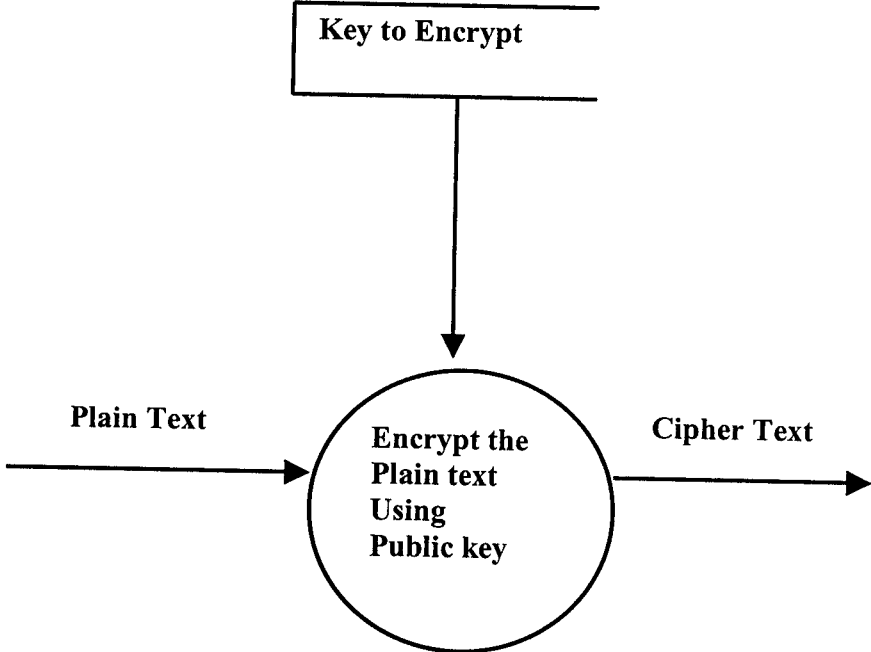
- Left shift the first 8-bit value by performing AND operation between the first 8-bit value and the hex decimal number h100.
- Converting the second 8-bit value from the first block into its ASCII value. Then the ASCII value is converted into byte.
- Add the second 8-bit value with first 8-bit value. Now we can get only one value for first block.
- Then the original value of first block will be converted into some other number by using Decryption formula.
- The new value of the first block is converted into two 8-bit numbers by performing some operations.
- Converting these two values into characters. Now two Original characters will be displayed instead of encrypted data of first block. This is called Plain text.
- Repeat step1 to step8 to convert all the blocks into Plain text. Now the whole decrypted message will be displayed. This is called original message.

When we sending the message to someone, the TCP protocol makes one virtual circuit between sender and receiver. Through this circuit only the data transmission will be happen.

# Process Diagrams

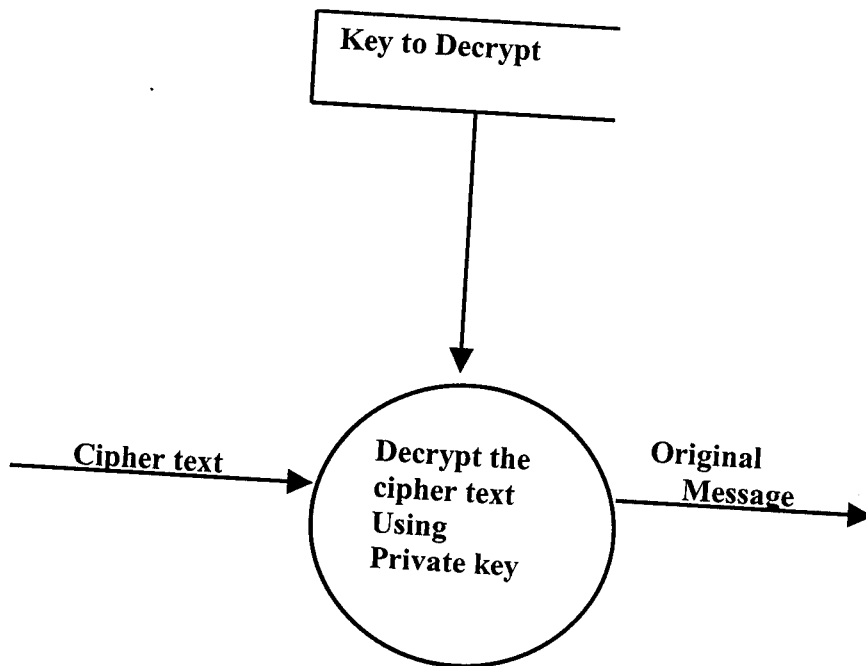


**Data Encryption**





## Data Decryption



## 4.4 Database Design

Database design aims at storing the data and enabling one or more users to share the common data, thereby eliminating redundancy and maximizing the efficiency of data processing system. Normalization techniques are used to reduce redundancy and improve data consistency.

Description of the tables are given below :

- Chatting Authentication table – This table is used to store information about users. This table contains five fields. The structure of this table is

Field	Description	Type
Username	New user name	Text
password1	Password	Text
password2	Password-Retype	Text
Desig	Designation of the User	Text
Date	Registration Date	Date

- Server Table – This table contains only two fields. This is used to store the incoming messages and sender's name. The structure of this table is

Field	Description	Type
Ser_from	Sender name	Text
Ser_receive	Message received	Text

- Client table – This table contains only two fields. This is used to store the incoming messages and sender’s name. The structure of this table is

Field	Description	Type
C1_from	Sender name	Text
C1_receive	Message received	Text

- Mailing Authentication Table – This is used to store information about the users. This table contains 4 fields. The structure of this table is

Field	Description	Type
Name	User name	Text
Password	Password	Text
Confirm	Password - Retype	Text
Date	Registration Date	Date

- Mailing Table – This is used to store messages , from-id, to-id, subject and Date. The structure of this table is

Field	Description	Type
from_id	Sender Id	Text
to_id	Receiver Id	Text
Subject	Subject of the Message	Text
Message	Message	Memo
Date	Received Date	Date

# SYSTEM TESTING AND IMPLEMENTATION

## **5. SYSTEM IMPLEMENTATIONS AND TESTING**

### **5.1 Implementations**

Implementation is the process that includes all those activities that take place to convert from the existing system to new system. The new system should be totally user-friendly, replacing an existing manual and automated system. Proper implementation is essential to provide a reliable system to meet the organization requirements.

The system is at present implemented and checked by the authority person on a parallel basis and is found to be working more satisfactory.

## 5.2 System Testing

Software testing is a critical element of software quality assurance and represents the ultimate review of specification, design and coding. Testing is a process of executing a program with the intent of finding errors. The user tests the developed system and changes are made according to their needs. The testing phase involves the testing of developed system using various kinds of data.

System testing is actually a series of different tests whose primary purpose is to fully exercise the computer-based system. System testing is the state of implementation that is aimed at assuring that the system works accurately and efficiently before live operations commence.

Testing is vital to the success of the system. System testing makes the logical assumption that if all the parts of the system are correct, the goal will be successfully achieved. The candidate system is subject to variety of tests. A series of testing is performed for the proposed system before the system is ready for user acceptance test. The system is tested on all types of networks and the problem created by the system is identified and it is removed from the system after testing.

The testing steps involved in system testing are,

1. Unit testing
2. Integration testing
3. Validation testing
4. Output testing

## **1. Unit testing**

Unit testing focuses on the smallest unit of the software design module. This is known as module testing. The modules of the project are tested separately. The testing was carried out during programming stage itself. In this testing step each module was found to be working satisfactorily with regard to the expected output from the module.

## **2. Integration testing**

Strategies for integrating software components into a functioning product include the bottom-up strategy, the top-down strategy, and the sandwich strategy. Careful planning and scheduling are required to ensure that modules will be available for integration into the evolving software product when needed. The integration strategy dictates the order in which modules must be available, and thus exerts a strong influence on the order in which modules are written, debugged, and unit tested. All the modules are combined and tested as a whole. Thus in the integration testing step, all the errors uncovered are corrected for the next testing steps.

## **3. Validation testing**

Validation testing can be defined in many ways, but a simple definition is that validation succeeds when the software functions in a manner that can be reasonably expected by the client.

After validation test has been conducted, one of the two possible conditions exists. The function or performance characteristics conform to

specification and are accepted. A deviation from specification is uncovered and a deficiency list is created.

Proposed system under consideration has been tested by using validation tests and was found to be working satisfactorily.

#### **4. Output testing**

After performing the validation tests, the next step is the output testing of the proposed system. No system is useful, if it does not produce the required output in a specified format. Considering the format required by the users tests the output generated or displayed by the system under consideration. Here, the output format is considered on the monitor only.

The output format on the screen is found to be correct as the format was designed in the system design phase according to the user needs. The hardcopy output also comes out as specified requirements by the user. Hence, output testing does not result in any correction in the system. The system is tested in many networks.



**CONCLUSION**

---

## 6. CONCLUSION

The system is designed in such away that it can be extended to incorporate the future changes into the system easily. The various user-friendly features are introduced in this project.

The system has fulfilled the requirements of the users and this system will work on intranet only. This system is very useful to send encrypted online or offline messages to others. The famous RSA Asymmetric or Public key algorithm has been implemented in this system. This public key algorithm is better than symmetric key algorithms, because it provides separate keys for encryption and decryption.

All the procedures and assumptions made in designing this project were strictly followed. The system is developed according to the requirements produced by the organization.

Reviews have been collected from the users about this system and are found to be satisfactory. Maintenance of the system has to be undertaken to the new requirements that may pop-up during passage of time.

**SCOPE FOR FUTURE DEVELOPMENT**

---

## 7. SCOPE FOR FUTURE DEVELOPMENT

The system is implemented keeping in mind the possible future enhancements and the modules are designed in such a way that enhancements are possible without any change in the basic structure of the system.

- Encryption is a time consuming process. So the file to be encrypted may be compressed to speed up the encryption.
- Security is very important in this system so increasing the key value is also possible to provide better security.

## **BIBLIOGRAPHY**

---

## BIBLIOGRAPHY

### Text Books

1. Bruce Schneier, "Applied Cryptography", Second Edition, John Wiley & Sons, Inc.
2. Wayne S. Freeze, "Expert guide to Visual Basic 6.0", First Edition 1998, BPB Publications.
3. Evangelos Petroustos, "Mastering Visual Basic 5.0", First Edition 1997, BPB Publications.
4. Othmar Kyas, "Internet Security", First Edition 1997, International Thomson Publishing.
5. Ellis M. Awad, "System Analysis and Design", Galgotia Publications Pvt Ltd 1993.
6. Roger S Pressman "Software Engineering", McGrawHill International Edition 1997.

### Websites

1. [www.rsa.com](http://www.rsa.com)
2. [www.rsadatasecurity.com](http://www.rsadatasecurity.com)
3. [www.primenumbers.com](http://www.primenumbers.com)

**APPENDIX**

---

# Cryptographic Communication System

RSA Algorithm

Chatting

Mailing

File

Cancel



# Online Chatting

User Name	<input type="text" value="kanagu"/>		
Password	<input type="password" value="*****"/>		
<input type="button" value="New User"/>	<input type="button" value="Cng.Pass"/>	<input type="button" value="O.K"/>	<input type="button" value="Cancel"/>

TCP SERVER		Current Users	Buttons
From	kanagu To		
Local IP	168.0.0.12 Local Host Name	80.0.0.7 sava 80.0.0.6 saba	Selected Clients
Send	Cryptography is the process of Encryption and Decryption. The RSA algorithm is asymmetric or Public key algorithm.		All Clients
Receive			Deletion
Plain Text			Encrypt
		Message Queue	Decrypt
		Combo1	Clear
			Cancel
Date : 4/26/02 Time : 2:40:48 PM No.Of Messages ::			

TCP SERVER

---

From:  To:

Local IP:  Local Host Name:

Send:

Receive:

Plain Text:

Date: 4/26/02 Time: 2:43:23 PM No. Of Messages: 0

Current Users

- 80.0.0.7
- selva
- 80.0.0.6
- saba

Buttons

- 
- 
- 
- 
- 
- 
- 

Message Queue

Enter The Public Key

TCP CLIENT			
From	kanagu	To	seiva
Local IP	80.0.0.7	Local Host Name	celeron7
Send	<input type="text"/>		
Receive	<input type="text" value="0ES0\$R11IE?pu*A11'0LI01P11æU42..ItE11;97æeU1:Y11.ææ#-IGI01P11"/>		
Plain Text	<input type="text" value="0ES0\$R11IE?pu*A11'0LI01P11æU42..ItE11;97æeU1:Y11.ææ#-IGI01P11"/>		
Date : 4/26/02 Time : 3:01:08 PM		No. of Messages :: 1	
		Current Users	Buttons
		80.0.0.6	To Server
		seiva	Selected Clients
			All Clients
			Deletion
			Encrypt
		Message Queue	Decrypt
		kanagu1	Clear
		<input type="button" value="Cancel"/>	
		<input type="button" value="Disconnect"/>	<input type="button" value="Connect"/>

TCP CLIENT

From	<input type="text" value="kanagu"/>	To	<input type="text" value="selva"/>	<p>Current Users</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td style="padding: 2px;">80.0.0.6</td></tr> <tr><td style="padding: 2px;">saba</td></tr> </table>	80.0.0.6	saba
80.0.0.6						
saba						
Local IP	<input type="text" value="80.0.0.7"/>	Local Host Name	<input type="text" value="celeron7"/>	<p>Buttons</p> <p><input type="button" value="To Server"/></p> <p><input type="button" value="Selected Clients"/></p> <p><input type="button" value="All Clients"/></p> <p><input type="button" value="Deletion"/></p> <p><input type="button" value="Encrypt"/></p> <p><input type="button" value="Decrypt"/></p> <p><input type="button" value="Clear"/></p>		
Send	<input style="width: 100%;" type="text"/>			<p>Message Queue</p> <p><input type="text" value="kanagu1"/></p> <p><input type="button" value="Cancel"/></p> <p>Enter The Private Key <input style="width: 100%;" type="text"/></p> <p><input type="button" value="Disconnect"/> <input type="button" value="O.K."/> <input type="button" value="Connect"/></p>		
Receive	<input -igiöiñ<br="" style="width: 100%;" type="text" value="ØES8\$ñIIIIE?bJ%AñI'3LIÖI'PñæV/2, RÊñ:9ñæLJ.Yñ:ëë"/>  æð+"/>					
Plain Text	<input style="width: 100%;" type="text" value="Cryptography is the process of Encryption and Decryption. The RSA algorithm is asymmetric or Public key algorithm."/>					
<p>Date : 4/26/02 Time : 3:18:43 PM      No. of Messages :: 1</p>						

Borland®

# Security Service™

Secure and high performance for application developers

About Exit



click here  
ebooks3.com

Read bestselling  
books online, FREE!

User Name	<input type="text" value="kanagu"/>	<input type="checkbox"/>
Password	<input type="password" value="*****"/>	
<input type="button" value="Sign Up"/>		<input type="button" value="Login"/>



Developed by : Kanagu @ Kot

# Borland®



I wish I had a low rate APR of

17.9  
15.9  
13.9

Submit

About

Exit

kanagu@sri.com



kanan@sri.com

rsa

hai kannan,

Cryptography is the process of Encryption and decryption. The RSA algorithm is asymmetric or Public key algorithm.



Developed by: Kanagu @ Kct

# Borland®

# Naturopathy Online



Suzanne Lawton, ND

About | Etc

kanagu@sri.com

nextcard

APR as low as 2.99%  
or 9.99%  
Ongoing

kanagu@sri.com

see

Ua-UaIqZzIa@|@|EIEIE:HTMcl8-17nC0  
 %84tzm'spEIM#Ux,S18td0j.IIly-a'lc0  
 vIbM-A>18IIIEI@y7qIaQI\$#4isIIIUaI?  
 pdM-A>18IIUW/E



# Borland

Developed by : Kanagu @ Kct



Borland

# Security Service™

Securing your business applications

About Exit

kannan@sri.com

**eBooks**  
click here  
ebooks3.com  
Read best selling  
books online, FREE!

Sender	Date	Subject
kannagu@sri.com	4/26/2002	0rsa



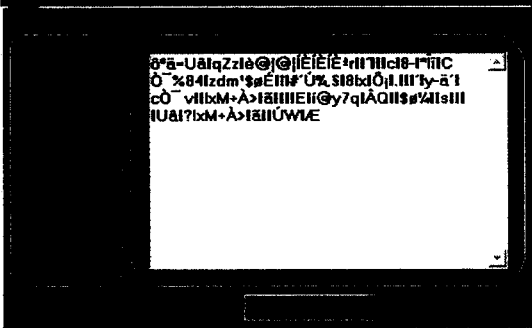
Developed by: Kanagu @ Kot

# Borland™

Launch console  
for latest audio/video 

About Exit

kannan@sri.com



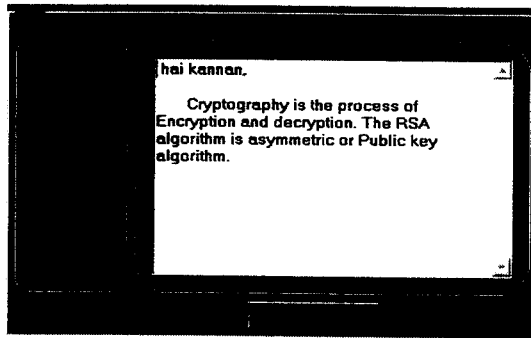
Developed by: Kanagu @ Kct

**Borland**<sup>®</sup>

**Borland**  
**Security Service™**  
Securing your business applications

About Exit

kannan@sri.com



Developed by: Kanagu @ Kct

**Borland®**

## File Encryption And Decryption

### EnCryption

Original Text File Name

Encryption Key

CipherText File Name

### Decryption

Encrypted File Name

Decryption Key

Decrypted File Name

Select File To Encrypt

Encrypt

Select File To Decrypt

Decrypt

Cancel

### About RSA Algorithm

RSA stands for Rivest, Shamir, and Adleman, they are the inventors of the RSA cryptosystem. RSA is one of the algorithms used in PKI (Public Key Infrastructure), asymmetric key encryption scheme. RSA is a block cipher, it encrypt message in blocks (block by block).

RSA can be used for security (encryption), confidentiality (signature), and key exchange purposes. Nowadays, it is often used for signature and key exchange only, this is because the encryption and decryption are slow, and it consumes times.

RSA security is so much depends on the difficulty of factoring large prime number. At this time the calculation required to find the factor the value to break the key is slow, many cryptanalysts consider that linear attack and differential attack are difficult to applied in RSA, only mathematical attack and brute force are feasible, but the time needed to use these attacks are quite long, therefore they are considered as impractical. May be later in the future as computer speed increased, this encryption algorithm may consider insecure and unused, but don't forget we can just simply increase the size of the key to prevent it from attacker.

The common size for the key length now is 1024 bits for P and Q, therefore N is 2048 bits, if the implementation (the library) of RSA is fast enough, we can double the key size.

## File Encryption And Decryption

Open

Look in: Kanagu

EnCrption

Original Text File Name

Encryption Key

CipherText File Name

File name: note

Files of type: \*.bit

Open as read-only

Open

Cancel

Select File To Encrypt

Encrypt

Select File To Decrypt

Decrypt

Cancel

## File Encryption And Decryption

**EnCryption**

Original Text File Name

Encryption Key

CipherText File Name

**Decryption**

Encrypted File Name

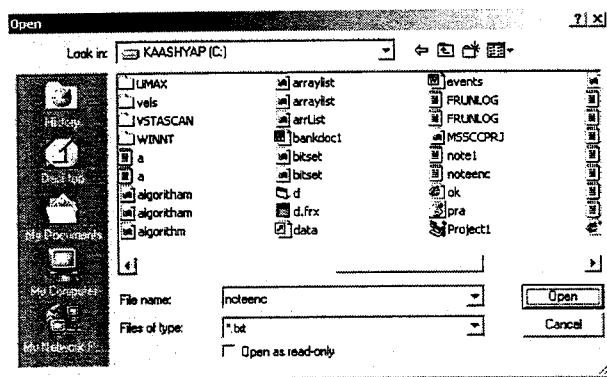
Decryption Key

Decrypted File Name

—òÓ)—zDvâ6uëive□wëú7™²/Dvâ6ra}â•ÔEš□□Á> v□□ŽÁ... ÓÈ□  
«š□â•8Ix•ÔÓ†:Y'G“q□šwë□?Ix'È□CÓ □,□\Ó7□□ÉDšE□wëšDvâ6#'Ú¼□□L□μ□'GÁuDvâ6ñšE•)šEÉ□wëš□J  
Ivè□wë>!--uw†jđAâ9gN...'-7□s□□□šé□□?□âCZc□μ□ñšæ>□œI□□šI@y7q□ÁQ□šUâ□?□>NB□“□y-, □BÓ □ÁuDvâ6ñIx  
>ø9ÚPÓ k\*p  
□-8□,-zÓ7#'Ú¼-zq□m'â#yšE9>ø9ÚPÓEš™<9ÚPÓ>ø□\*□□U□□'ÚW™'œ)ÍÉÍÉqi□□ k“q>øš»7(□□Á>ra.□□œ“â□\*·fÑ  
B□“□y-·È□š' CZÆaÓ7,š□J“â□\*ÁÍ-EZz□:Èš'Ix•ÔUâ□?□>?:šñfyš]a□Zf□ŽAÁuÁž×mM·  
□š“â□,Èš□óš',»7(□□Á>ra-EZz□:ÈIx•ÔUâ□?□>?:šñfyš“8:=□šwëñ□,ÈšE-»b7yšwëšÓ7#'Ú¼,š“8Ix•Ô,™.□□“□y-,1□  
yšóeÓá□š“qđA“â k“8“qq□Eš,šq□đ'@:ÍÉÍÉ@ÍDvâ6w†□é□;□□,Èšœ3ÇC□šD□ó  
□•ÔEš“8□CÓ-;™šEÁh°□CB□\*□ó□□†□□□é□ñI>œ1□ %68è□q□±}□¼È-□ÁÓ†-zweñ□C—žyšwëš>t,œi□6  
Qy-, ÈfH'ñ(□CæøÁh•Ô□CÓ□□†□□□¼□wëšFâ89yš□□>š'È□Ž□CÓ Uâ□?□,ÈšóeÓá□šÍE) k□“□q□J  
{□ k“8=œó¼□wë6Q>œEš□¼□6Q}âPÓIx•Ô;™šEšš'EUÝ□±Bo6Q}âPÓIx'È;™šEÁh°□CB□CæøD□ó□  
đóAâ9 v□□□š“8÷=CC6QÓ-šI,š»iBo6Q}âPÓIx•Ô>ñšš'□□Á>zdx'È□□š□=œ□□#m>ø, □CÓ □C—žyš\*)((□□Cæø7yšwë  
ŽÁyš6Q}âPÓEš1□yšfH“žyš9Úñi□šwë'1□Á>yšwë□?Ix'È k“8=œó'ÈóAí@□,»Rc<æ>□š□J  
Áus□□\*È>œ6Q'Í□,, wëš□□□:ÈIxšš'»R, 'Íra □(□,ÑB'Èi@(□šwëñ□>NB□“□y-, □J  
Ivè□wëQœšI□\* k“8=œó¼□□,^5.□□œyšIx•ÔÍE□□»7(□□Á-z;™š“8—ñÍE'ò>O5šÍEL□ k“q' »7-z=œ>R÷=□,ÑB'Èi@yšwëš=  
œÍLšEÉ□wëš-□\*□□%68'Èâ6ÚY□,-zLóçÁIxÈ;†□:-□ÁÍ™²/†qyš] >□“8raifš'ò¼□wëš:-□\*□Đñiwëz}Óá□,ÈšœUgß>ø“â  
Èš'ò¼□»,“qđAy□□CÓ-È'ò'È'É□,Èš□šÉ>ø“â□□,È□wëš-šó'  
GÓ7}â,š“8-7wëšQj6â1□“×šEÉ□Dvâ6ñ□□í@-zÓ7Ó)BQ□šL□ k“qi™Ó)□□yšwëš:-□\*œÍLÚW™'Á'



## File Encryption And Decryption



Decryption

Encrypted File Name

Decryption Key

Decrypted File Name

Select File To Encrypt    Encrypt    Select File To Decrypt    Decrypt    Cancel

### About RSA Algorithm

RSA stands for Rivest, Shamir, and Adleman, they are the inventors of the RSA cryptosystem. RSA is one of the algorithms used in PKI (Public Key Infrastructure), asymmetric key encryption scheme. RSA is a block cipher, it encrypt message in blocks (block by block).

RSA can be used for security (encryption), confidentiality (signature), and key exchange purposes. Nowadays, it is often used for signature and key exchange only, this is because the encryption and decryption are slow, and it consumes times.

RSA security is so much depends on the difficulty of factoring large prime number. At this time the calculation required to find the factor the value to break the key is slow, many cryptanalysts consider that linear attack and differential attack are difficult to applied in RSA, only mathematical attack and brute force are feasible, but the time needed to use these attacks are quite long, therefore they are considered as impractical. May be later in the future as computer speed increased, this encryption algorithm may consider insecure and unused, but don't forget we can just simply increase the size of the key to prevent it from attacker.

The common size for the key length now is 1024 bits for P and Q, therefore N is 2048 bits, if the implementation (the library) of RSA is fast enough, we can double the key size.