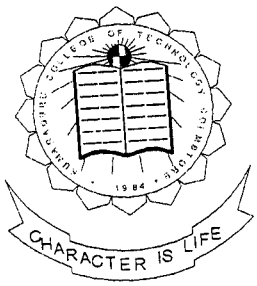
Virtual Private Networks-An Implementation

Project Work



1997 - 2001

Submitted By

Karthik G
Karthik R
Saravanaan A
Sethupathy V

Under the guidance of

Mrs. L.S.Jayashree M.E, MISTE.,

In partial fulfillment of the requirements for the award of the degree of Bachelor of Engineering (B.E) in Computer Science and Engineering of the Bharathiar University, Coimbatore.

Department of Computer Science and Engineering

Kumaraguru College of Technology

Coimbatore - 641 006

Kumaraguru College Of Technology

Coimbatore-641006

Department of Computer Science and Engineering

Certificate

This is to certify that the Project Report entitled

Virtual Private Networks-An Implementation

has been submitted by

Mr G. Karthik, R. Karthik, A. Saravanan, V. Sethupathy

In partial fulfillment of the requirements for the award of Degree in Bachelor of Engineering in Computer Science and Engineering of the Bharathiar University, Coimbatore during the year 2000-2001

Guide

S. Jha 9/3

Head of the Department

Certified that the candidate was examined by us in the Project viva-voce examination held on 12.3.2001 **and the University Register Number is**

.....

Internal Examiner

External Examiner

Declaration

We, Karthick G, Karthik R, Saravanaan A, Sethupathy V hereby declare that this project work entitled **'Virtual Private Networks-An Implementation'** submitted to Kumaraguru College of Technology, Coimbatore (Affiliated to Bharathiar University) is a record of original work done by us under the supervision and guidance of Mrs. L.S.Jayashree M.E, Department of Computer Science and Engineering.

Name of the candidate	**Register Number**	**Signature of the candidate**
Karthik G	9727 k0 149	
Karthik R	9727 k0 150	
Saravanaan A	9727 k0 174	
Sethupathy V	9727 k0 176	

countersigned:

Staff in Charge:

Mrs. L.S. Jayashree M.E, MISTE.,
Lecturer
Department of Computer Science and Engineering
Kumaraguru College of Technology
Coimbatore – 641 006

Place : Coimbatore
Date : 9-3-2001.

ACKNOWLEDGEMENT

We express our deep sense of gratitude to **Dr. K.K. Padmanabhan .Ph.D.** , Principal , Kumaraguru College of Technology , Coimbatore , for providing permission to carry out this project work.

With profound sense of gratitude and regards , we acknowledge with great pleasure the guidance and support extended by **Prof. S.Thangasamy Ph.D.** , Head of the Department of Computer Science and Engineering , for his valuable and continuous guidance , suggestions , constructive criticisms and persistent encouragement.

We express our deep sense of respectful gratitude to our guide **Ms. L.S.Jayashree M.E.,** Lecturer, Department of Computer Science and Engineering for her valuable guidance, keen suggestions, innovative ideas, inspiration, discussions, helpful criticisms and kind encouragement in all the phases of this project work. It had been indeed a great pleasure to work under her guidance.

It is our duty to express our thanks to **Mr.V.Krishnan,** Project Manager, Atna Technologies India Pvt Ltd., Coimbatore and to all the Faculties of IBM ACE for guiding us to do this project work and their kind encouragement during the course of the project.

We like to express our special thanks to all staffs and lab technicians in the Department of Computer Science and Engineering who helped us for the successful completion of the project.

Finally we express our deep sense of gratitude to our parents, friends and all other persons who directly or indirectly involved with this project, for their invaluable help and consideration towards us.

SYNOPSIS

The project entitled VIRTUAL PRIVATE NETWORKS - AN IMPLEMENTATION" provides a software-based solution to overcome the security risks in a public network like Internet.

Virtual Private Networks is a way to simulate a private network over a public network that effectively reduces the cost, accessing data World Wide using Internet rather than going for a leased line can achieve this.

This project is done for a virtual company called **"CENTWIN AUTOMOBILES"** based in Chennai and has two factories in Calicut and Hosur with Managing Director for the former and Factory Managers for latter. The data transfer between these three must be secured.

The data while rolling over the network should be impermeable. Similarly the other data's in the source and destination (i.e. client and server) should be protected from network viruses, worms and Trojans.

An attempt is made to resolve these security risks using Firewalls, Authentication, Encryption and Tunneling techniques.

CONTENTS

1.INTRODUCTION

There are two types of networks namely,

- Public Networks
- Private Networks

A public network is a large collection of unrelated peers that exchange information more or less freely with each other. Some of the public networks are public Telephone system and the Internet.

A private network is composed of computers owned by a single organization that share information specifically with each other. Some of the private networks are Corporate LAN and WAN.

When the companies are spread all over the world, their LANs are treated as separate, isolated islands. Each branch office might have their own naming scheme, e-mail system and unique protocol. Interconnection between these offices is traditionally done using leased phone lines. By using leased phone line a company can be assured that the connection is always available, and private, however this can be expensive. If the company has offices across the country, this cost can be prohibitive.

VPNs allow us to create a secure, private network over a public network using software, hardware or a combination of both. This is done through Authentication, Encryption, Firewalls and Tunneling. VPNs are more cost effective for large companies and well with in the reach of smaller ones.

VPNs can be used to expand the reach of an Intranet.

The world "VIRTUAL" in VPN refers to the public network treated as private network though it is not the case. Here we use the Internet as a public network which saves a lot of money for remote access.

Usage of Internet Service Provider (ISP) to access the Internet who have Point-Of-Presence (POP) Internationally provides a good chance that our LAN will be a local phone call away. For situations where Corporate office networks are in separate cities, having each office get a T1, Frame relay, or ISDN line to an ISPs local POP would be much cheaper than connecting the two offices using these technologies. The scope of accessing the data is expanded with the help of Internet by means of equipments like cell phone, laptop etc.,

The risks associated with the Internet are advertised every day by the trade and mainstream media. The risks are more real and apparent for companies. Stolen

or deleted corporate data may cause adverse effects. Before we put our private data out on the Internet, we should make sure a VPN is robust enough to protect it.

When we think of protection through VPN the first things come to mind are Files, Documents, Financial Analysis and Customer records.

There are several technologies that VPNs use to protect data traveling across the Internet. The most important concepts are firewalls, authentication, encryption and tunneling.

An Internet firewall serves the same purpose as firewalls in buildings and cars: to protect a certain area from the spread of fire and a potentially catastrophic explosion. The idea is to use the firewall to keep unwanted visitors from entering our network.

Authentication techniques ensure the communicating parties that they are exchanging data with the correct user or host. It is analogous to "logging in" to a system with a username and password.

Encryption techniques help to insure that the information within a session is not compromised. This

includes not only reading the information within a data stream, but altering it, as well.

Tunneling hides from the intruders about the source and destination IP addresses by encapsulating them with in the data packet itself.

2. CONCEPTUAL PERSPECTIVE

2.1 Firewall:

Definition:

A firewall is a system or a group of systems that enforces a access control policy and its purpose is to control the flow of traffic.

Situation where firewall is used:

- Dial-in modem pool

  E.g. an organization may have access control policy that dial-in users may only access a single mail system. The organization does not want to access to other internal servers or Internet.

- External connections to business partners

  Many organizations have permanent connection to remote business partners. This can create a difficult situation-the connection is required for business, but now someone has access to internal network from an area where security is not controlled by the organization .A firewall may be used to regulate the document access from this links

- Between Departments

Some organizations are required to maintain firewalls between different areas of networks. This is to insure that internal users only have access to the information they require. A firewall at the point of connection between these two networks enforces access control.

Types of firewall:

- ✓ Static packet filtering

It controls traffic by the using the information used by the packet headers. This is ease in TCP packet but in case of UDP packet condition is worse because UDP packet header provides only source and destination port number. A static packet filter can use the following information for regulating the traffic

- ➢ Destination IP address or subnet
- ➢ Source IP address or subnet
- ➢ Source and destination service port
- ➢ Flag (TCP only)
  - ACK-acknowledgment
  - FIN-transmitting session wishes to terminate the current session
  - PSH-prevent the transmitting system from queuing data prior to transmission
  - RST-reset the state of current communication

- SYN-used while initiating the communication system
- URG-indicates the presence of higher priority information

✓ Dynamic packet filtering

It takes static packet filtering one step further by maintaining a connection table in order to monitor the state of communication system. Every time the remote server tries to respond to the protected host the state table is referenced to insure the following

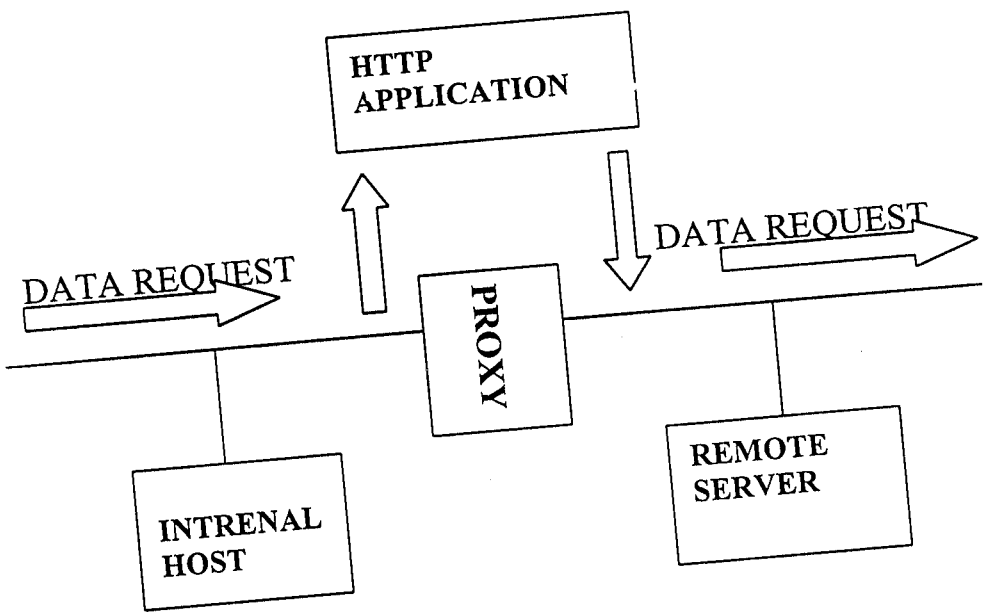
- ➢ The protected host actually made the data request
- ➢ Source port information matches the data request
- ➢ Destination port information matches the data request

In addition the dynamic packet filter may even verify the match of sequence of acknowledgment numbers. If all the data is correct the dynamic packet filter allows the packet to pass. This method can also be used for UDP packets by eliminating the disadvantage of less information by the header

✓ Proxies

A proxy server is a application the mediates traffic between two network segments. Proxies are often used instead of filtering to prevent traffic from passing directly between networks. When the proxy is acting as the mediator,

the source and destination systems never actually connect with each other.



For an analogy think of two people speaking thru language interpreter, in this case the two people never talk to

each other. The communication between them passes thru the interpreter.

Once the proxy receives the request it identifies the type of service the host is trying to access, verifies the request and it formulates a new request to the remote

words the proxy does not simply pass the request along; it generates a new request for the remote information and this new request is sent to the remote server in turn the remote server process the request and sends the response to the proxy server. Then the proxy server generates new response to the host.

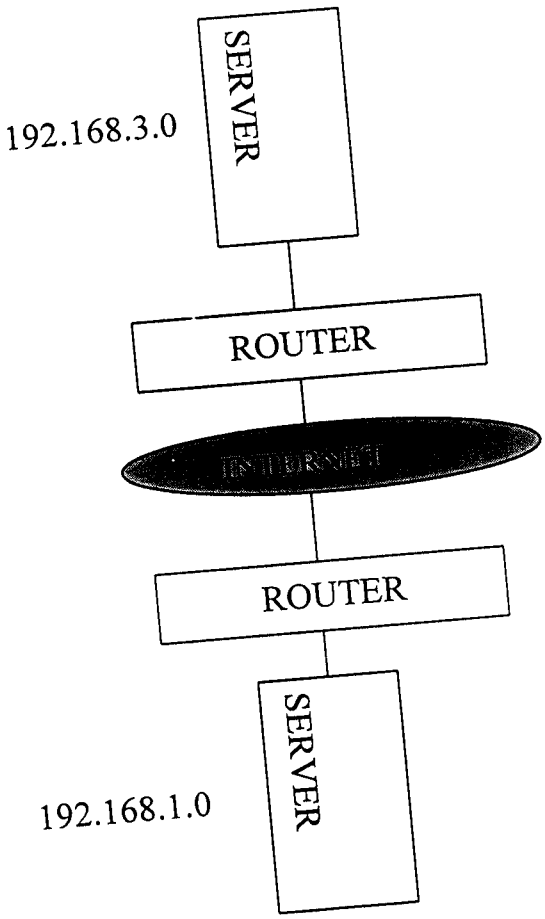
2.2 Tunneling:

When data is transmitted thru tunnel we do not get to see the IP address of the host that actually transmitted the data, nor the IP address of destination host. This information is encrypted along with the actual data within the original packet. Once the original packet is encrypted, the router will encapsulate the cipher text within a new IP packet using its own IP address as the source and a destination IP address of the remote router. This is called tunneling. Tunneling helps to ensure that a snooping attacker will not be able to guess which traffic causing the VPN worth trying to crack, since all packets use two routers IP addresses .Not all VPNs support this feature, but it is nice to use when it is available.

Since we have a virtual tunnel running between the two routers, there is added benefit of being able to use private address space across the Internet. For example, a host on Network A would be able to transmit data to a host on the 192.168.2.0 network without requiring network address translation. This is because the

routers encapsulate this header information as the data is delivered along the tunnel. When the router on network receives the packet, it simply strips of the encapsulating packet, decrypts the original packet ,and delivers the data to the destination host .

VPN also has the benefit of being platform and service independent .In order to carry on secure communications; workstations do not have to use software that supports encryption. This is done automatically as the traffic passes between the two routers. This means that services such as SMTP, which are transmitted in the clear, can be used in a secure fashion-provided the destination host is on the remote encryption domain



2.3 Cryptography:

Encryption can be regarded as a method for altering data into a form that is unusable by anyone other than the intended recipient, who has the means necessary to decrypt it. The input to an encryption algorithm is typically called clear text (plain text), while the output is referred to as cipher text or crypt text. The encryption process protects the data by making the assailant work too hard or too long to get at what's being hidden.

There are many algorithms available to convert from plain text to cipher text. All of them are fall into three basic categories. They are namely,

- Hash algorithms
- Private key crypto systems
- Public key crypto systems

Hash algorithms:

Hash algorithms, which are usually known as message digests or one-way hashes take an arbitrarily large and mathematically convert it into a fixed-length, one-way number. Hashes are typically used to check the validity of a particular message or password.

The process of hashing must be fast and reliable, and must produce a result that is fundamentally difficult to reverse. An example of a hash would be to take an input password, multiply it by PI(3.1417), divide by e(2.71828) , mod the result by 7654321,and take the middle eight bytes. It would be certainly be nasty to reverse this process without knowing anything about it.

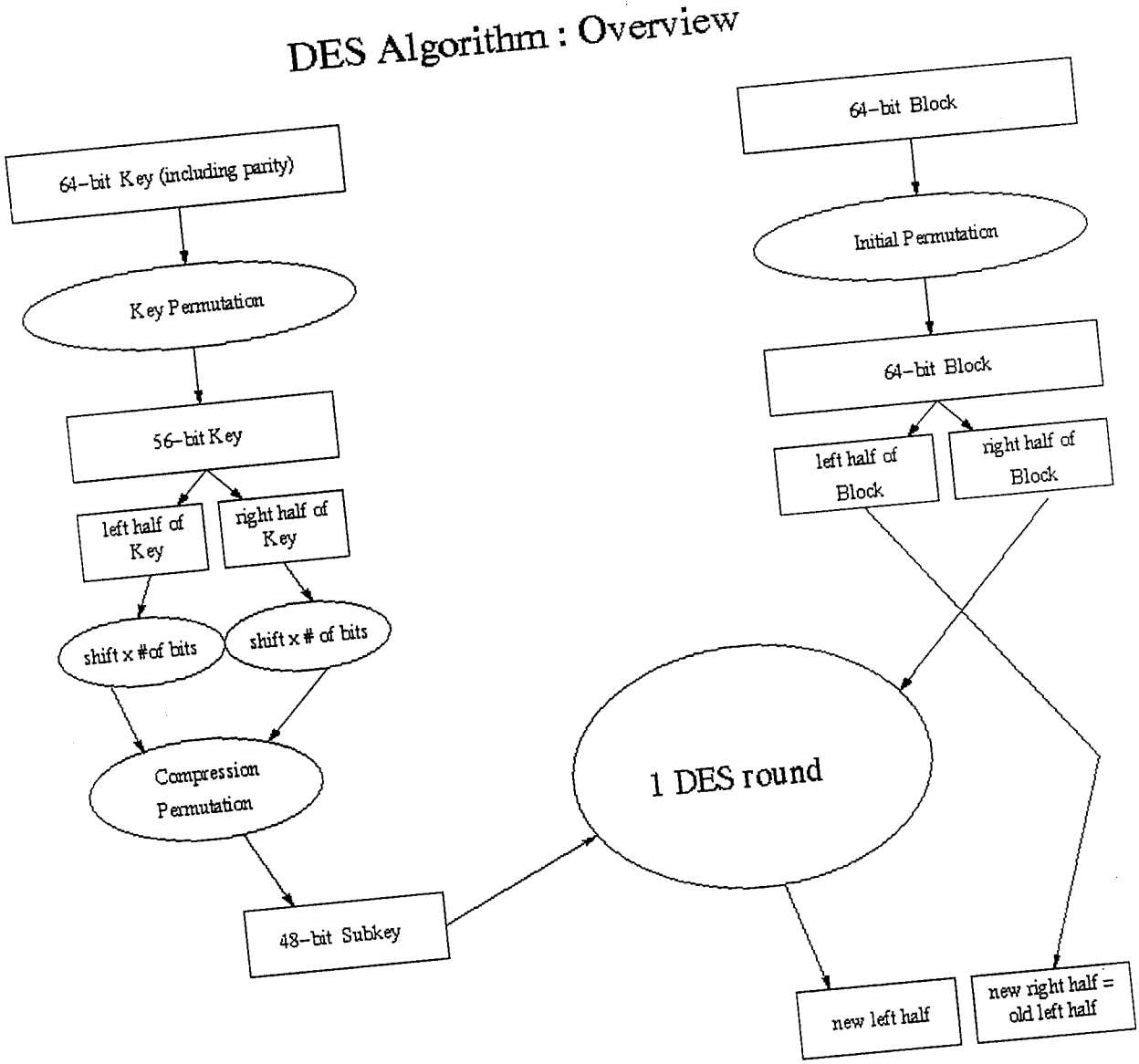
Some of the popular hashing algorithms are,

- Secure Hash Algorithms (SHA)
- Message Digests (MD) Algorithms

Private key crypto Systems:

It is also otherwise called Secret key crypto systems. Data Encryption Standards (DES) is one of the best examples of this type.

National Bureau of Standards developed DES in 1977 for low-grade U.S. government work and commercial applications. It uses a 64-bit key, but trims the last bit of each eight bytes as a parity check, making the actual key size only 56 bits. The key is permutated via much iteration and finally 16 sub keys were obtained of size 48 bits.



The data block is of 64 bits are given to the permutation boxes as described in the diagram. The cipher text is obtained using the above-generated 16 sub keys combining with the permutated data.

In order to decrypt the data, reverse process is applied and the plain text is obtained.

Public key crypto systems:

The most popular algorithm for public key cryptography is the RSA algorithm.

The Rivest-Shamir-Adleman (RSA) algorithm is one of the most popular and secure public-key encryption methods. The algorithm capitalizes on the fact that there is no efficient way to factor very large (100-200 digit) numbers.

2.4 AUTHENTICATION:

- **Hashing techniques:**

Authentication techniques are essential to VPNs, as they ensure the communicating parties that they are exchanging data with the correct user or host. Authentication is analogous to "logging in" to a system with a user name and a password. VPNs, however, require more stringent authentication methods to validate identities.

Most VPN authentication systems are based on a shared key system. The keys are run through a hashing algorithm, which generates a hash value. The other party holding the keys will generate its own hash value and compare it to the one it received from the other end. The hash value sent across the Internet is meaningless to an observer, so someone sniffing the network wouldn't be able to glean a password.

Authentication typically performed at the beginning of a session, and then at random during the course of a session to ensure that an impostor didn't "slip into" the conversation. Any deviation in the checksum sent from one peer to the next means the data was corrupted during transmission, or intercepted and modified along the way.

Another way authenticating is using "DIGITAL SIGRATURES".

- **Digital Signatures:**

This digital signature provides proof that the message originated from the designated sender. In order to be effective, digital signature need to be both message-dependent as well as signer-dependent. This would prevent electronic "cutting and pasting" as well as modification of the original message by the recipient.

Suppose user A wanted to send a "digitally-signed" message, M, to user B:

- User A applies their decryption procedure to M. This results in cipher text C.
- User A applies the encryption procedure of user B to C. This results in message S.
- Cipher text message S is sent over some communication channel
- Upon receipt, user B applies their decryption procedure to S. This results in ciphertext message C.

• User B applies user A's encryption procedure to message C. This results in the original message, M.

User B cannot alter the original message or use the signature with any other message. To do so would require user B to know how to decrypt a message using A's decryption procedure.

2.5 Steganography

A completely different alternative technique to transfer archives securely over the Internet is Trojan like technique. Here the message is hidden in the image file and image is transferred. The logic behind the hiding technique is each pixel is represented by 32 bit of information.

One byte for RED value

One byte for GREEN value

One byte for BLUE value

One byte for INTENSITY

Of all the bytes INTESITY byte intensity byte has less significant and contributes for 20% of the clarity. When the pixel intensity is replaced by the message to be transformed

The pixel Intensity is distorted by probability of range 0.0 to 1.0, which leads to average probability of 0.5 for a byte. By considering the entire 32 bit for a pixel the distortion is

20*0.5=10 % or probability of 0.1;

But the perception of vision for human is only 60 % .By taking this advantage the average distortion of the pixel visible to human is

60* 0.1=06 % or probability of 0.06;

The image used for this technique is of PNG (Portable Network Graphics) format. PNG format is used because its

Compression technique is of loss-less type (Run Length Encoding). Lossy compression is not used because each character of the message has its importance

3. PROGRAMMING ENVIRONMENT

3.1. HARDWARE DESCRIPTION

a. FOUR PENTIUM MACHINES: -

- Two for Proxies
- One for Client
- One for Server

b. 64- MB RAM

c. 4 GB HARD DISK

d. NETWORK CARDS

NETWORK ENVIRONMENT:-

1.Four machines interconnected using cable.

2.The TCP/IP protocol for data transfer.

3.Host names for the machines.

Description of Software & Packages Used :

3.2.1. Java 2.0:

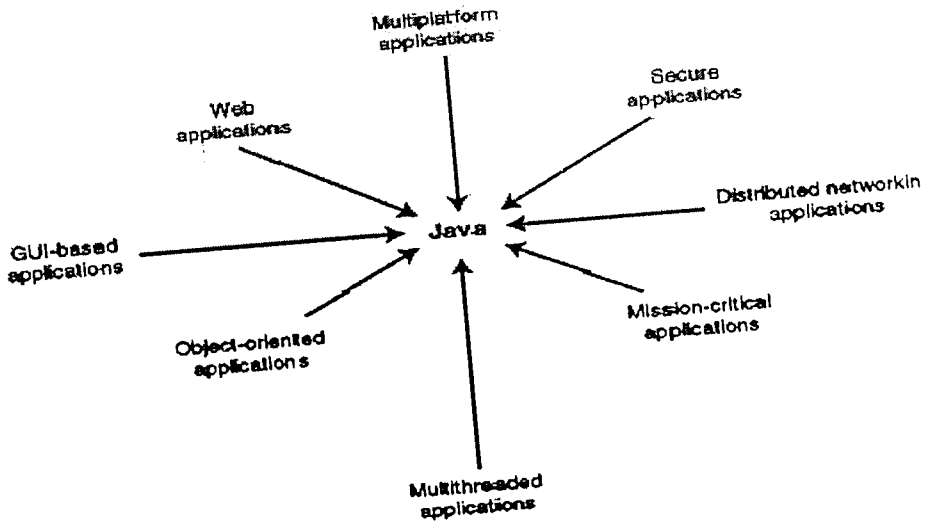
Java is a language for programming on the Internet developed by Sun Microsystems. It incorporates entire OOPS, multithreading and is platform independent. It is designed to be small, simple and portable across both platforms as well as operating systems at source as well as binary level. The popularity of java is due to its design mainly based on the combination of three key elements.

- Applets,
- Powerful Programming Language constructs (Application) and
- Significant object classes.

When the program is compiled, it is translated into machine code or processor instructions that are specific to the processor. In JDE, there are two parts.

- Java Compiler.
- Java Interpreter.

The power of Java language can be known through it's buzz words and it is diagrammatically represented as follows.



The former generates the byte code instead of machine code and the later executes the Java program. JDK provides system input and output capabilities and other utility functions in addition to classes that support networking, common Internet protocols and user interface toolkit functions.

3.2.2. Servlets:

The meaning of servlets is server side programming .The salient features of servlets are

- Multithreading - Since servlets are written in java they support multithreading.
- No GUI-Since they run on server side there is no need for GUI.So they do not support GUI and they run faster.

- Dynamic loading and downloading –Servlets are loaded dynamically into RAM and they are removed from RAM once their intended purpose is completed.
- HTTP Support –They provide well defined support for HTTP
- Advantages of servlets over CGI

CGI supports multiprocessing so there is overhead in context switching .But in case of servlets there is no overhead in context switching due to its multithreading environment.

3.2.3. JDBC:

The Java Database Connectivity Application Programming Interface (API) is an API currently being designed by Sun Microsystems that provides a Java language interface to the X/Open SQL Call Level Interface standard. This standard provides a DBMS-independent interface to relational databases that defines a generic SQL database access framework. The most visible implementation of the X/Open SQL CLI is Microsoft's ODBC (Open Database Connectivity). This API defines a common SQL syntax and function calls that can be used by developers to send SQL commands to and retrieve data from SQL databases. ODBC-enabled applications make use of database drivers (similar in concept to other device drivers) installed on the system that allow applications to talk to a vendor's database. Using this methodology, all of the DBMS-specific code is placed inside the ODBC driver and the application developer is

shielded from implementation-specific problems in theory. Practically speaking, it is sometimes difficult to completely remove vendor-specific syntax from all ODBC operations, but in most cases, it is a relatively simple task to port ODBC to run on a new database server.

3.2.4.Java script:

JavaScript is an Object Oriented language. This simply means that it can use objects. An object is a more complicated version of a variable. It can store multiple values and can also include actual JavaScript code. You can create your own objects to represent just about anything.

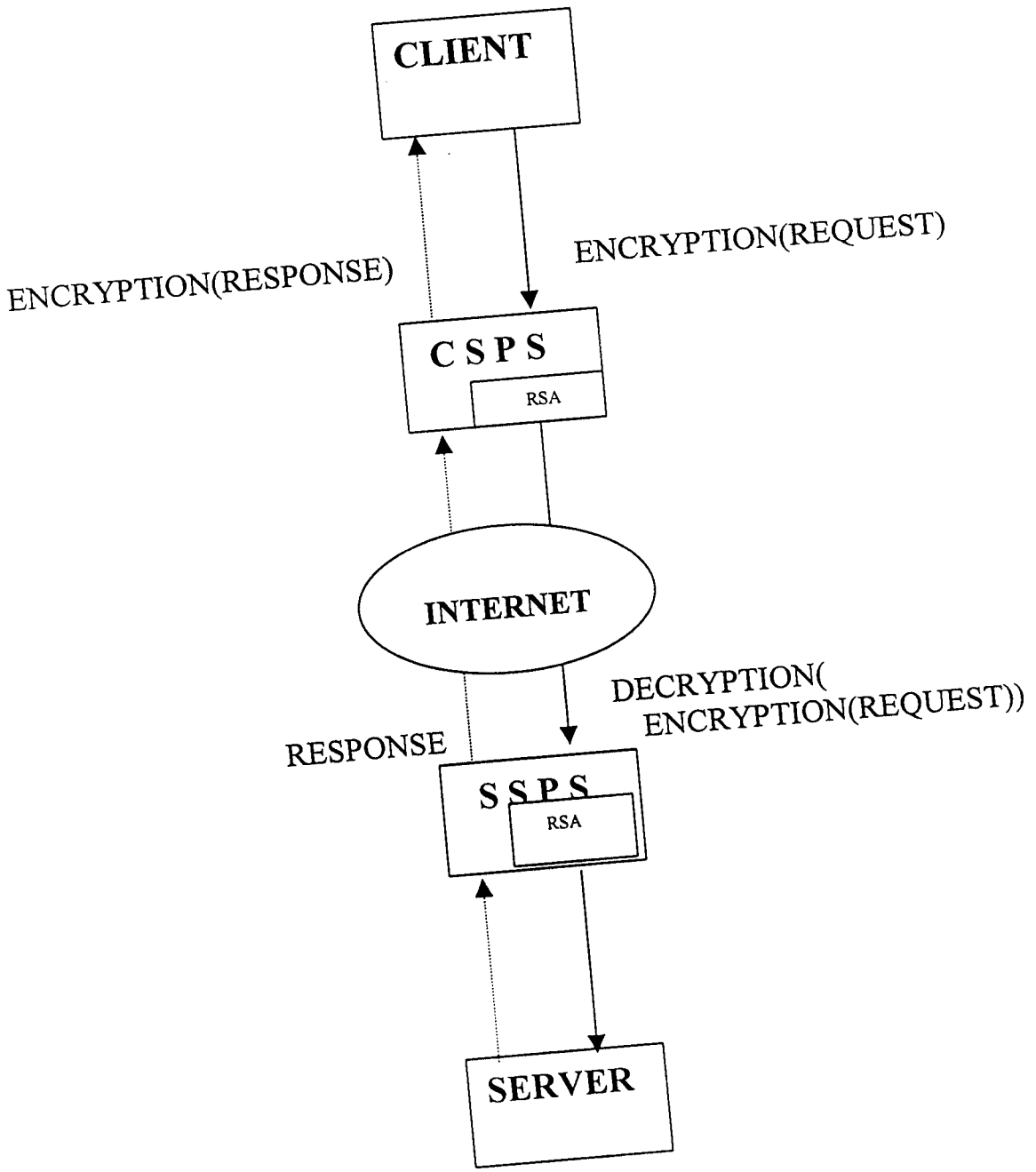
JavaScript also includes objects that enable you to access features of the browser directly. These objects represent actual elements of the browser and the Web page, such as windows, documents, frames, forms, links, and anchors.

Some of the benefits of using JavaScript are,

- The JavaScript language is interpreted rather than compiled. Changing a script is as simple as changing an HTML page.
- Rather than creating objects and classes, you can do quite a bit by simply accessing existing objects in JavaScript.
- Variables are loosely typed: You do not need to declare variables before their use, and most conversions (such as numeric to string) are handled automatically.

- Event handlers enable a JavaScript function to execute whenever an action is performed on part of the HTML document. For example, a form's input field can be checked for certain values whenever it is modified.

4. DATA FLOW DIAGRAM



SSPS – SERVER SIDE PROXY SERVER
CSPS – CLIENT SIDE PROXY SERVER
RSA -- ENCRYPTION ALGORITHM

5.IMPLEMENTATION

In this part of the project work VPN is developed for "CENTWIN AUTOMOBILES" company, which is located in three places. The company details are given below.

Centwin has a HeadOffice (HO) located in Chennai. It has production Centers located in Hosur and Calicut.

The Managing Director (MD) is based in Chennai and he is the only person authorized to accept orders and confirm prices. An order will have the following elements:

The MD also specifies whether the factory in Hosur or Calicut has to execute the order. Each factory has a manager who deals with order execution and shipment.

The Manager fills in information about the current status of the order, Actual Date of shipment actual quantity shipped, comments for any delay/problem.

The MD needs to be able to view all date in terms of current order status, completed orders, factory wise production details and actual completion dates. Each factory Manager views only data applicable to his job, which includes Order No, Spare Part Required, Place of Shipment, Expected Data Delivery.

An administrator placed in Chennai should be capable of maintaining over all user details which includes creating new users, updating the existing user database, deleting a user.

The design will incorporate a browser interface. So appearance must be tested with different browsers. The Data transfer must take place securely without any corruption by external agents.

AUTHENTICATION:

Here one of the security mechanisms called "AUTHENTICATION" is achieved using the hashing algorithms.

The hashing algorithm generates a hash key value. When ever, the user gets "logging in" to the site, user enters the password. Hash key is generated using the above said alogrithm. The key is sent through the tunnel via the Internet. The key value is not useful for an intruder, while the data packets are on the way. So the key value is received at the destination end. The same algorithm is made to run in the server side also. If both the keys are matched we confirm that the communicating parties are true.

There may be chance for an intruder to attack the network while the session is on the way. To avoid this, the same hashing algorithm is made to run during the random period of the session.This confirms that no intruder has attacked the system and insures that both the people are same.

The mechanism ensures that only the company employees namely Managing Director (MD) and Factory Managers (FMs) can only "log in" to the company site. It is necessary to maintain the privacy of each employee.i.e., Factory Managers shouldn't be able to access the details of Managing Director and among them self. Our Authentication technique maintains the privacy policy to achive the purpose.

Tunneling:

The type of Tunneling developed here is referred as Pseudo-tunneling and it is done at the application layer. The header from the browser contains the following information

- Destination IP address
- Destination port thru which communication occur
- Protocol type with version
- Method used for data transfer
- Data type major/minor
- Content type which the browser can accept
- Content length

The data that that are actually transferred are Order No, Date, Buyer Name, Address, Phone, Mail, Spare part required, Quantity, Place of Shipment and Date of delivery.

A tunnel is laid between the client side proxy server and the server side proxy server by cryptographic techniques through which the application layer header is encrypted along with the data, in client side proxy server and transferred to the server side proxy and vice-versa. The header information, which is encrypted, is from the browser. The server side proxy decrypts the message and performs some firewall checks and passed to the server. The server processes the request and sends the response to the Server side proxy, which in turn encrypts the message and pass to the client side proxy. The client side proxy decrypts the message and passed to the client.

Here any Hacker who capture's the stream in the Internet can do nothing with the encrypted message because the public key crypto

system used in encryption is world wide accepted standard. The data stream appears to be from the client side proxy server and the server side proxy server not from the server and the client

Firewall:

Firewall here is used to ensure that the data from the Internet to the Proxies are only from the companies' client and the server. Placing characters at random positions and placing information of their position before encryption and checking for their occurrence at the destination after decryption does the purpose of the firewall. The purpose of the firewall is to implement the access control policy that only the request from the peer proxy server will be processed and hence the request which out of VPN are filtered

Encryption :

RSA Algorithm's are implemented for encryption purpose. RSA is of type public key cryptography. Encryption is done by means of public key and decryption is done by means of private key so there is no need of some secure way of key exchange as in case of private key algorithm's. RSA is 10-100 times slower than the secret key crypto systems.

✓ **The RSA Algorithm**

The Rivest-Shamir-Adleman (RSA) algorithm is one of the most popular and secure public-key encryption methods. The algorithm capitalizes on the fact that there is no efficient way to factor very large (100-200 digit) numbers.

Using an encryption key (e,n), the algorithm is as follows:

1. Represent the message as an integer between 0 and $(n\text{-}1)$. Large messages can be broken up into a number of blocks. Each block would then be represented by an integer in the same range.

2. Encrypt the message by raising it to the eth power modulo n. The result is a ciphertext message C.

3. To decrypt ciphertext message C, raise it to another power d modulo n

The encryption key (e,n) is made public. The decryption key (d,n) is kept private by the user.

How to Determine Appropriate Values for *e*, *d*, and *n*

1. Choose two very large (100+ digit) prime numbers. Denote these numbers as p and q.

2. Set n equal to $p * q$.

3. Choose any large integer, d, such that GCD(d, ((p-1) * (q-1))) = 1

4. Find e such that $e * d = 1$ **(mod** ((p-1) * (q-1)))

Here key size used are of 64 bit and the encryption is done character by character. The header mentioned above and the data specified are encrypted and decrypted using this algorithm.

6. CONCLUSION

Virtual Private Networks reduces the cost associated with the installation and maintenance of Intranet over geographically dispersed areas drastically. The project is successfully implemented between the Head Office and two branch Offices located at three different places, which are far apart.

The project incorporates various security mechanisms such as Authentication, Encryption, Firewalls and Tunneling which makes it quite difficult for the Hacker to break.

One of the lucrative aspects of this project is its encryption mechanism whose basis are of world standards.

In this project we made a trade-off between time and security in order to increase the efficiency of the latter.

7. SCOPE FOR FEATURE DEVELOPMENT

This project successfully works for this particular application and this can be extended to nay sort of similar organization which are geographically far apart.

In order to transfer the data via the Internet faster, the code for this application can be migrated into firmware.

This project adopts TCP/IP protocol suite, as it's basic means of data transfer. It can be made to adapt to similar sort of protocols with subtle changes.

This project may be enhanced to involve the customers along with the employees of the company.

8.BIBLIOGRAPHY

1. Charlie Scott, Paul Wolfe, and Mike Erwin
Virtual Private Networks.
O'Reilly & Associates Inc., 1999.

2. Tannenbeum S. Andrew, ***Computer Networks***
McGraw-Hill International Edition, 1990.

3. Chris Brenton, ***Mastering Network Security***
BPB Publications, 1999.

4. Hunter, ***Java Servlet Programming***
O'Reilly & Associates Inc., 1999.

5. Patrick Naughton & Herbert Schildt
Java2: The Complete Reference, Third Edition
Tata McGraw-Hill Publications,1999

URL'S

1. www.shiva.com

Commercial implementer of VPN.

2. www.oakland.edu

Describes the RFCs details.

3. www.rsa.com/rsalabs

Describes the RFCs details.

4. www.abisoft.com

Describes the DES algorithm.

```
/*
CLIENT SIDE PROXY SERVER
-DECRYPTS THE ENCRYPTED REQUEST
(i.e) From client side proxy server
AND PASS TO THE SERVER
-ENCRYPTS THE RESPONSE
(i.e) From server
AND PASS TO CLIENTSIDEPROXYSERVER
*/


import java.net.*;
import java.io.*;
public class cspsme
{
ServerSocket server;  //LISTENS FOR THE REQUEST
Socket arrived;
public cspsme()         //STARTS THE SERVER SOCKET
{
try{ server=new ServerSocket(8085);}
catch(Exception e)
{System.out.println("EXCEPTION \n"+e.getMessage());}
}
public void listen()//LISTENS FOR THE REQUEST  DIRECT THE
        {               //REQUEST  TO  A SEPARATE  THREAD  FOR
```

```
while(true)          //ENCRYPTION
try{
arrived=server.accept();
new requestc(arrived);
}catch(Exception e){System.out.println(e.getMessage());}
}

public static void main(String a[])
{
cspsm c=new cspsm();
c.listen();
}

}

/*
THE CLASS THAT  DECRYPTS THE ENCRYPTED RESPONSE
AND  PASS TO THE CLIENT
*/

class responsec implements Runnable
{
Socket sendreq,arrived;
Thread resthread;
```

```
public responsec(Socket arrival, Socket reply) //INITIATION
{
arrived=arrival;
sendreq=reply;
resthread=new Thread(this);
resthread.start();
}

public void stopThread()
{
resthread=null;
}
/* RSA ALGORITHM FOR DECRYPTION */
public int dec(int C)
{
int n2 = 4331,   // public modulus,
e2 = 83,     // public exponent,
d2 = 3947;   // private exponent
int r = 1;
while (d2 > 0)
{
if (d2 % 2 == 1)     // Is the exponent odd?
r = (r * C) % n2;
C = (C * C) % n2;
d2 = d2 / 2;
}
```

```
int P = r;
return P;
}
public void run()
{
BufferedReader br=null;
BufferedWriter bw=null;
ObjectInputStream ois=null;
try{
br=new BufferedReader(new

        InputStreamReader(sendreq.getInputStream()));
 bw=new BufferedWriter(new

        OutputStreamWriter(arrived.getOutputStream()));
 ois=new ObjectInputStream(sendreq.getInputStream());
 } catch(IOException ioe){System.out.println(ioe.getMessage());}
 try{
 while(!br.ready());      // WAITS FOR THE  RESPONSE
 char c;
 int i=0;
 while(true)
 {
 //DO DECRYPTION
 c=(char)dec(i=ois.readInt());
 //DISPLAY FOR USER VIEW
```

```
System.out.print(i);
//PASS TO CLIENT
bw.write(c);
bw.flush();
}
}
catch(Exception e){ System.out.println(e.getMessage()); }
finally
{
try{
bw.write("\n");   //CLOSE ALL CONNECTIONS
bw.flush();  //AND STREAMS
br.close();
bw.close();
ois.close();
stopThread();
arrived.close();
sendreq.close();
}
catch(IOException ioe){ioe.printStackTrace();}
}
}

}
```

```
/*
THE CLASS THAT  ENCRYPTS THE REQUEST
AND  PASS TO THE  SERVER SIDE PROXY SERVER
*/

class requestc implements Runnable
{
Socket accept,sendreq;
Thread acceptreq;
/*      RSA ALGORITHM FOR ENCRYPTION    */
public int enc(int C)
{
int M=C;
int n=4331, e=83;
int r=1;
while (e2 > 0)
{
if (e % 2 == 1)   // Is the exponent odd?
r = (r * M) % n;
M = (M * M) % n;
e = e / 2;
}
C = r;
return C;
}
```

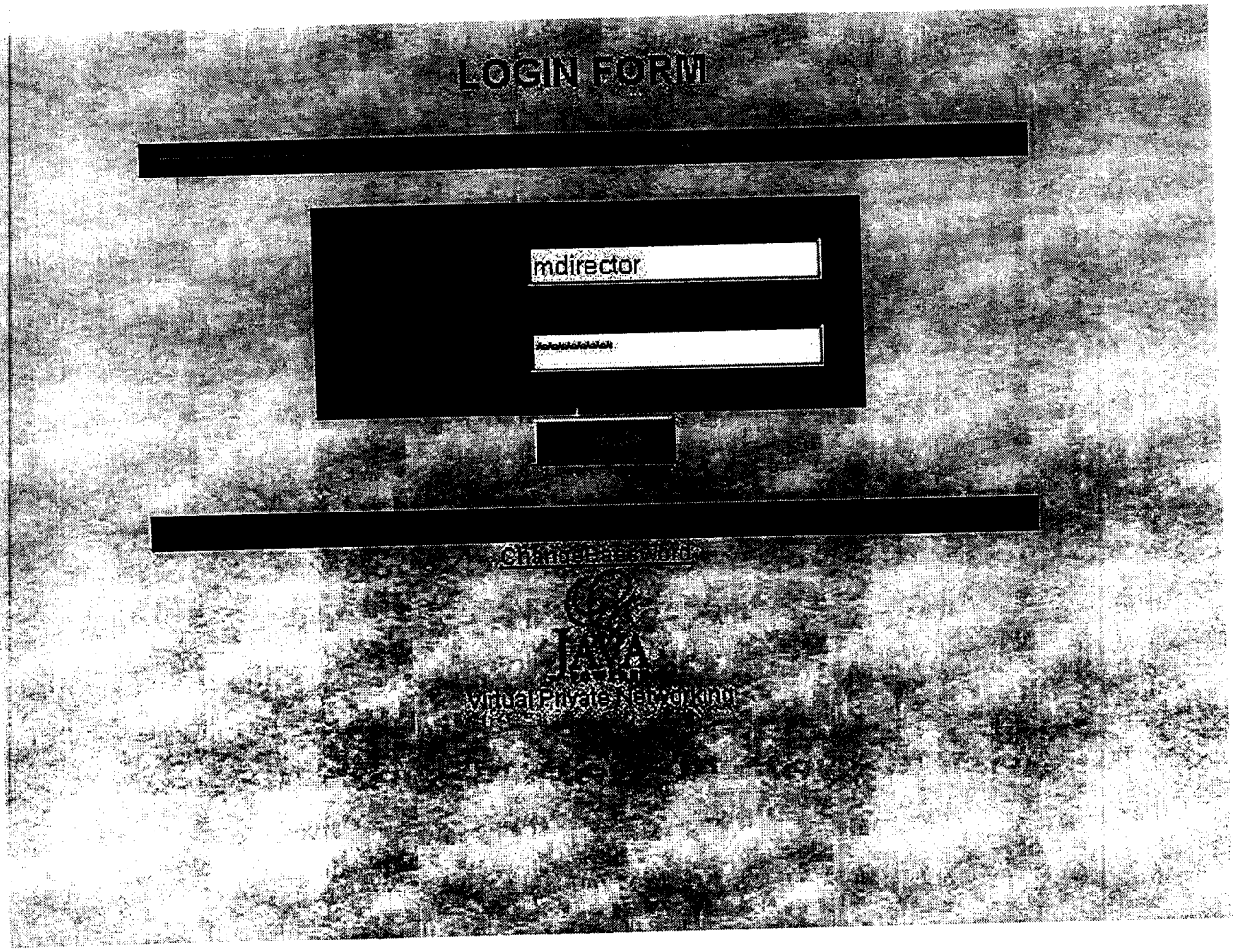
```
public requestc(Socket arrival) // INITIATION
{
accept=arrival;
acceptreq=new Thread(this);
acceptreq.start();
 }

 private void stopThread()
 {
 acceptreq=null;
 }

  public void run()
  {
  BufferedReader  br=null;
  ObjectOutputStream oos=null;

   try{
   br=new BufferedReader(new
                              InputStreamReader(accept.getInputStream()));
    sendreq=new Socket("localhost",8086);
    new responsec(accept,sendreq);
    oos=new ObjectOutputStream(sendreq.getOutputStream());
    char c;
    // READ A CHARACTER FROM  CLIENT
    while((c=(char)br.read())!=(char)-1)
```

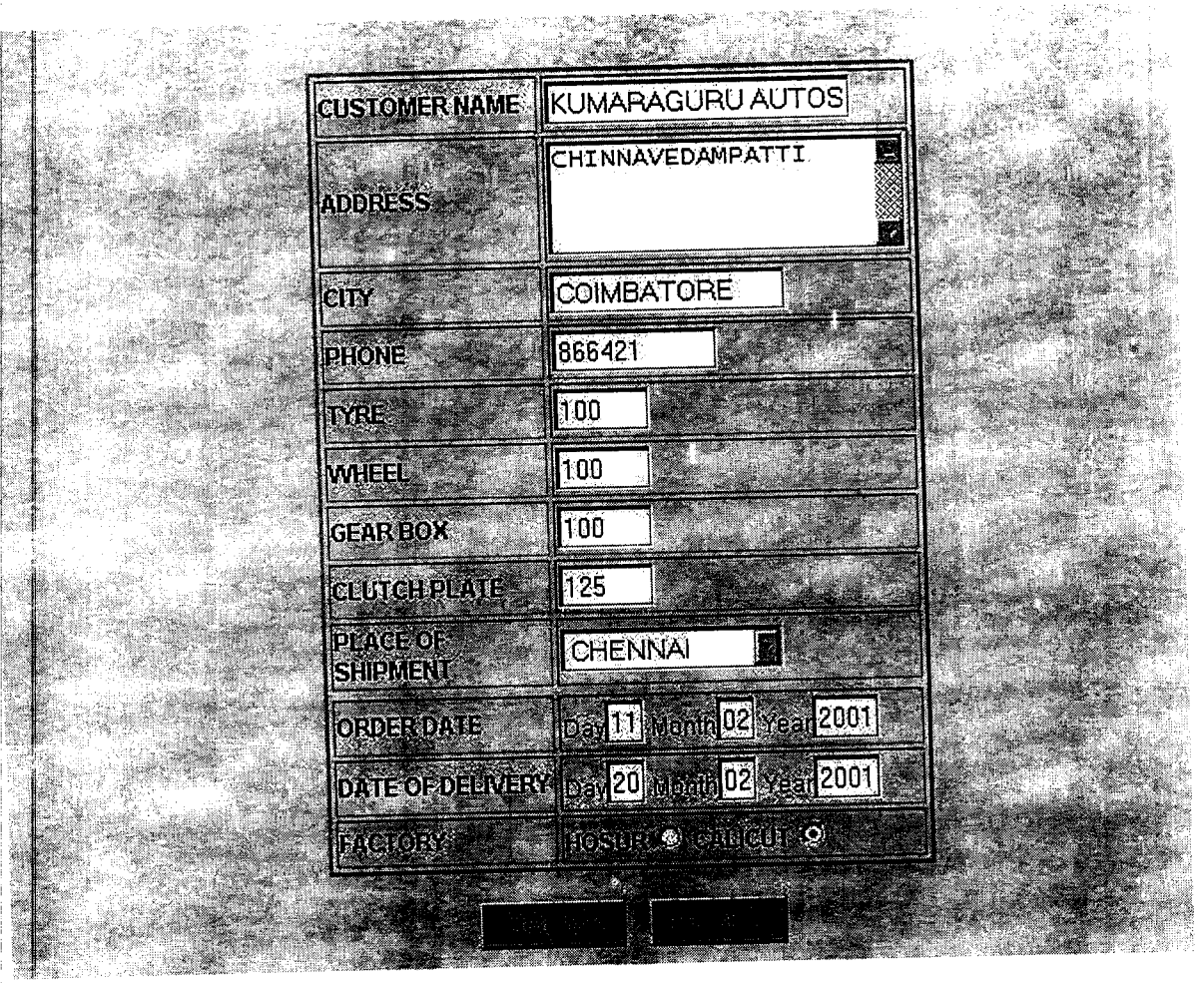
```
{
int i=enc(c);          //ENCRYPT
System.out.print(i);
oos.writeInt(i);        //PASS THE ENCRYPTED
oos.flush();           // VALUE TO  SERVER SIDE
// PROXY SERVER
}
}catch(Exception e){}
finally
{
try{          /* CLOSE THE STREAMS AND SOCKET */
br.close();
oos.close();
stopThread();
}catch(IOException e){e.printStackTrace();}
System.out.println("CONNECTION CLOSED");
}
}
}
```

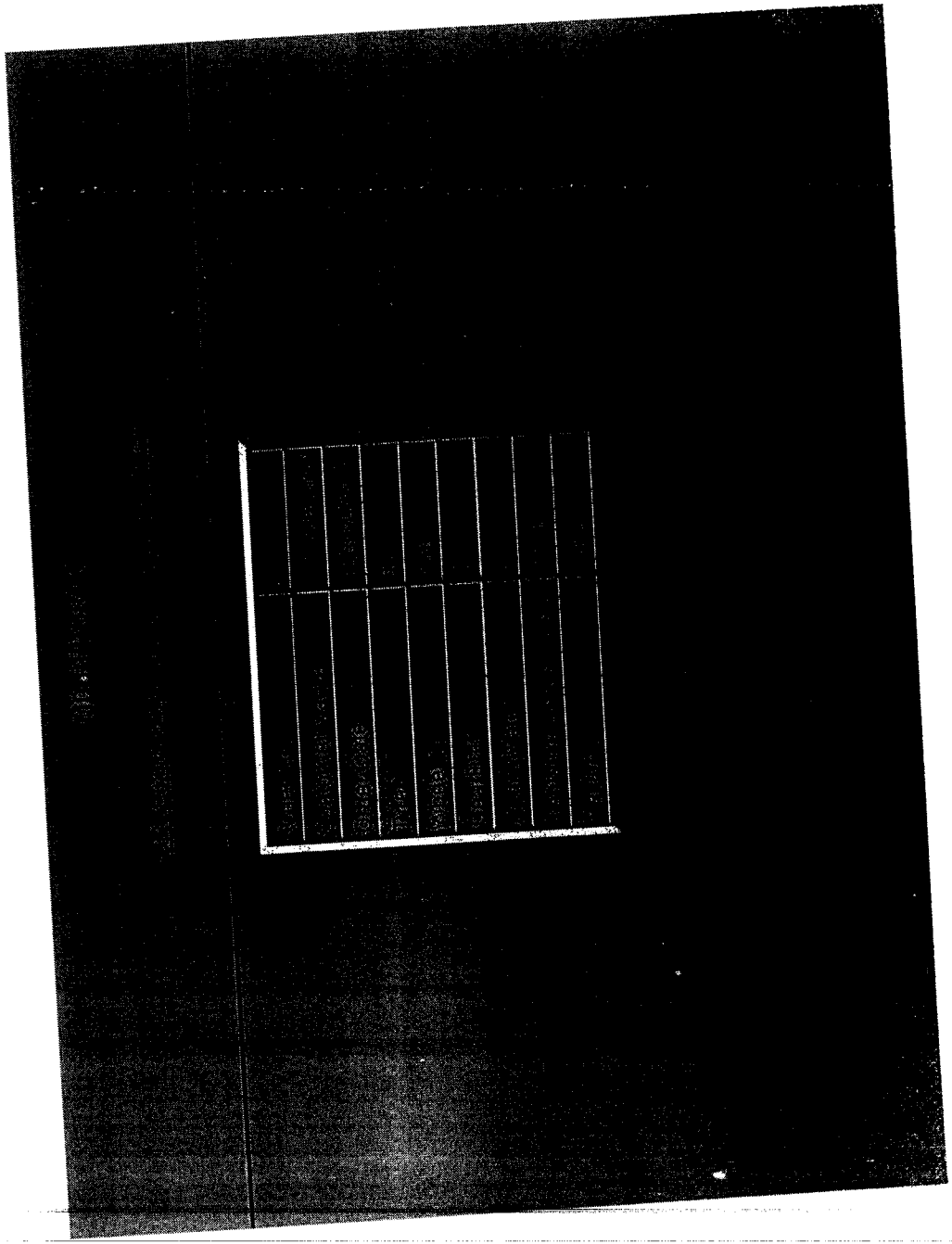
```
/*
GENERATES AND DISPLAYS THE RSA
PUBLIC AND PRIVATE KEY PAIRS
*/
public class RSAKeyGen
{
private long p,q,n; / / TWO PRIME NO,MODULIE
private long e;          / /  PUBLIC EXPONENT
public long d;           / /  PRIVATE EXPONENT
/*  GENERATES  p AND Q */
private long primeGen()
{
double d=Math.random();
long l=(long)(d*1000000000L);
if(l%2==0)
l++;
long o=1;
while(true)
{
for(int i=0;i<l;i++)
o=o*2%l;
if(o==2)
break
else
{  l+=2;   o=1;  }
}
```

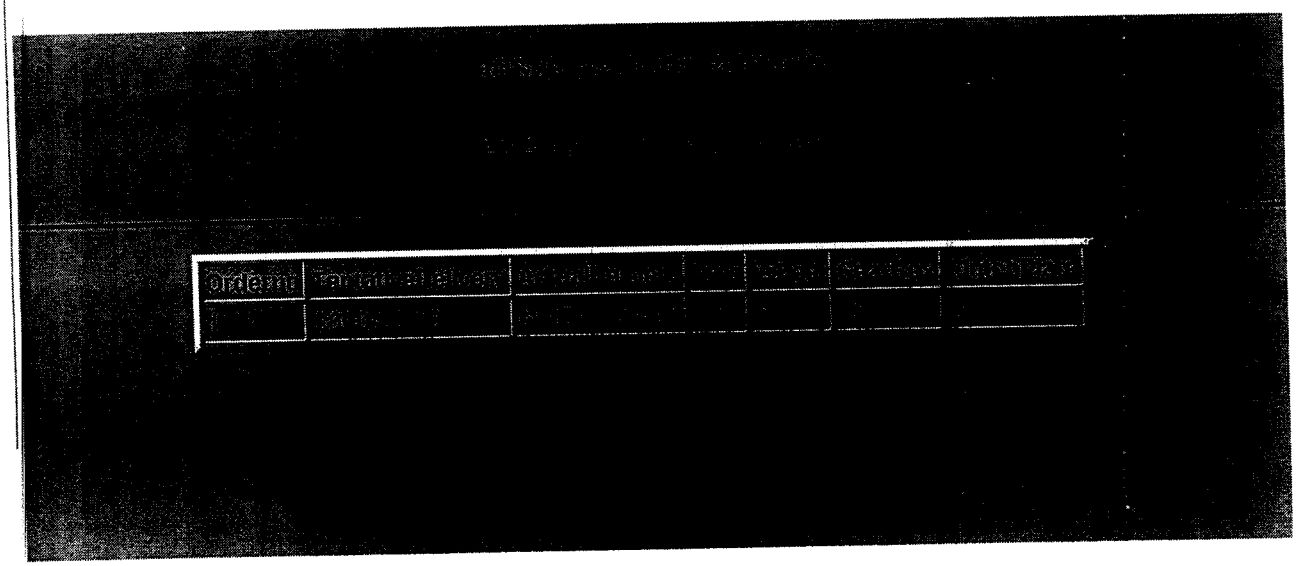
```
return l;
}
/* GENERATES e  */
private long relativelyPrimeGen()
{
long x ;
while(true)
{
x=primeGen();
if((x<p)&&(x<q))
break;
}
return x;
}

public void keyGen()
{
p=primeGen();
q=primeGen();
e=relativelyPrimeGen();
computePublicKey();
n=p*q;
}
/* GENERATES d */
public void computePublicKey()
{
```

```
long k=0,x=((p-1)*(q-1))%e;
System.out.println("x  ="+x);
int i=1;
while(true)
if(((x*i++ + 1)%e)==0)
{
k=i-1;
break;
}
d=(k*(p-1)*(q-1)+1)/e;
}

public static void main(String a[])
{
RSAKeyGen kg=new RSAKeyGen();
kg.keyGen();
System.out.println("p  ="+kg.p);
System.out.println("q  ="+kg.q);
System.out.println("e  ="+kg.e);
System.out.println("d  ="+kg.d);
System.out.println("n  ="+kg.n);
}
}
```

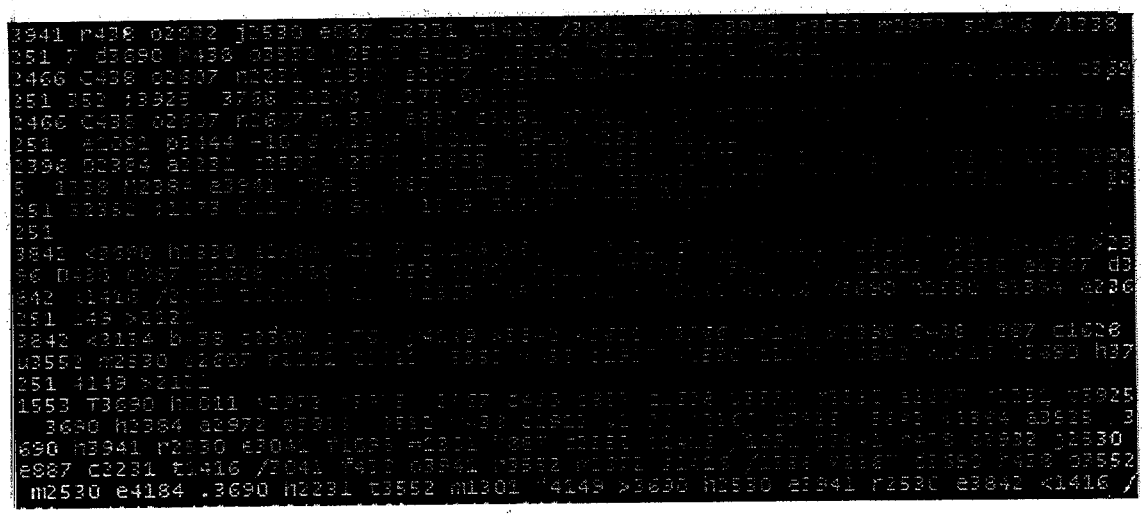

LOGIN FORM
mdirector
Change Password
JAVA
Virtual Private Network


CUSTOMER NAME
KUMARAGURU AUTOS
ADDRESS
CHINNAVEDAMPATTI
CITY
COIMBATORE
PHONE
866421
TYRE
100
WHEEL
100
GEAR BOX
100
CLUTCH PLATE
125
PLACE OF SHIPMENT
CHENNAI
ORDER DATE
Day 11 Month 02 Year 2001
DATE OF DELIVERY
Day 20 Month 02 Year 2001
FACTORY
HOSUR CALICUT





SAMPLE ENCRYPTED MESSAGE



1. MD [MANAGING DIRECTOR] : -

Field	Type	Size
Ono	Number	Integer
Cname	Text	25
Odate	Date	
Addr	Text	50
City	Text	15
Phone	Text	10
Tyre	Number	Integer
Wheel	Number	Integer
Gbox	Number	Integer
Cplate	Number	Integer
Pship	Text	25
Ddate	Date	
Adate	Date	
Status	Text	25
Factory	Text	10

2.USER: -

Field	Type	Size
Sno	Number	Integer
Userid	Text	25
Pass	Text	25