FACULTY OF ENGINEERING AND

TECHNOLOGY SRM INSTITUTE OF SCIENCE

AND TECHNOLOGY

Kattankulathur, Chengalpattu District

NOVEMBER 2022

In partial fulfilment for the Course

of

18CSC381T- CRYPTOGRAPHY
MINI PROJECT REPORT

Submitted by

Adhin Jibil (RA2011030010031)
Shanthosh Sivan S(RA2011030010044)

Under the Guidance of

J.Prabakaran

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

(Under Section 3 of UGC Act, 1956)

BONAFIDE CERTIFICATE

Certified that this mini project report "**ACCESS CONTROL LIST**" is the bonafide work of **Gokul MK (RA2011030010023), Adhin Jibil (RA2011030010031) and Shanthosh Sivan (RA2011030010044)** who carried outthe project work under my supervision.

SIGNATURE

J PRABAKARAN
ASSISTANT PROFESSOR
NWC
SRM Institute of Science and Technology

ACKNOWLEDGEMENT

We express our heartfelt thanks to our honorable **Vice Chancellor Dr. C. MUTHAMIZHCHELVAN**, for being the beacon in all our endeavors.

We would like to express my warmth of gratitude to our **Registrar Dr. S. Ponnusamy,** for his encouragement

We express our profound gratitude to our **Dean (College of Engineering and Technology) Dr. T. V.Gopal,** for bringing out novelty in all executions.

We would like to express my heartfelt thanks to Chairperson, School of Computing **Dr. Revathi Venkataraman,** for imparting confidence to complete my course project

We wish to express my sincere thanks to **Course Audit Professor Dr.Annapurani Panaiyappan, Professor and Head, Department of Networking and Communications** and **Course Coordinators** for their constant encouragement and support.

We are highly thankful to our my Course project Faculty **J PRABAKARAN , ASSISTANT PROFESSOR**, **NWC,** for his/her assistance, timely suggestion and guidance throughout the duration of this course project.

Finally, we thank our parents and friends near and dear ones who directly and indirectly contributed to the successful completion of our project. Above all, I thank the almighty for showering his blessings on me to complete my Course project.

TABLE OF CONTENTS

INTRODUCTION
ACL

Access Control Lists (ACL) are very powerful security feature of Cisco IOS. By using Access Control Lists (ACL), we can deny unwanted access to the network while allowing internal users appropriate access to necessary services. Access Control Lists (ACL) are a set of commands, grouped together (by a number or name), that are used to filter traffic entering or leaving an interface. Access Control Lists (ACL) commands define which traffic is permitted and which is denied.

We have already discussed that an Access Control Lists (ACL) is a group of statements that define whether packets are accepted or rejected coming into an interface or leaving an interface. Access Control Lists (ACL) statements operate in sequential, logical order. If a condition match is true, the packet is permitted or denied and the rest of the Access Control Lists (ACL) statements are not checked. If all the Access Control Lists (ACL) statements are unmatched, an implicit "deny any" statement is placed at the end of the list by default. Access list statements operate in sequential, logical order and they evaluate packets from the top down. Once there is an access list statement match, the packet skips the rest of the statements. If a condition match is true, the packet is permitted or denied. You should remember that there is an implicit "deny any" at the end of every Access Control Lists (ACL).

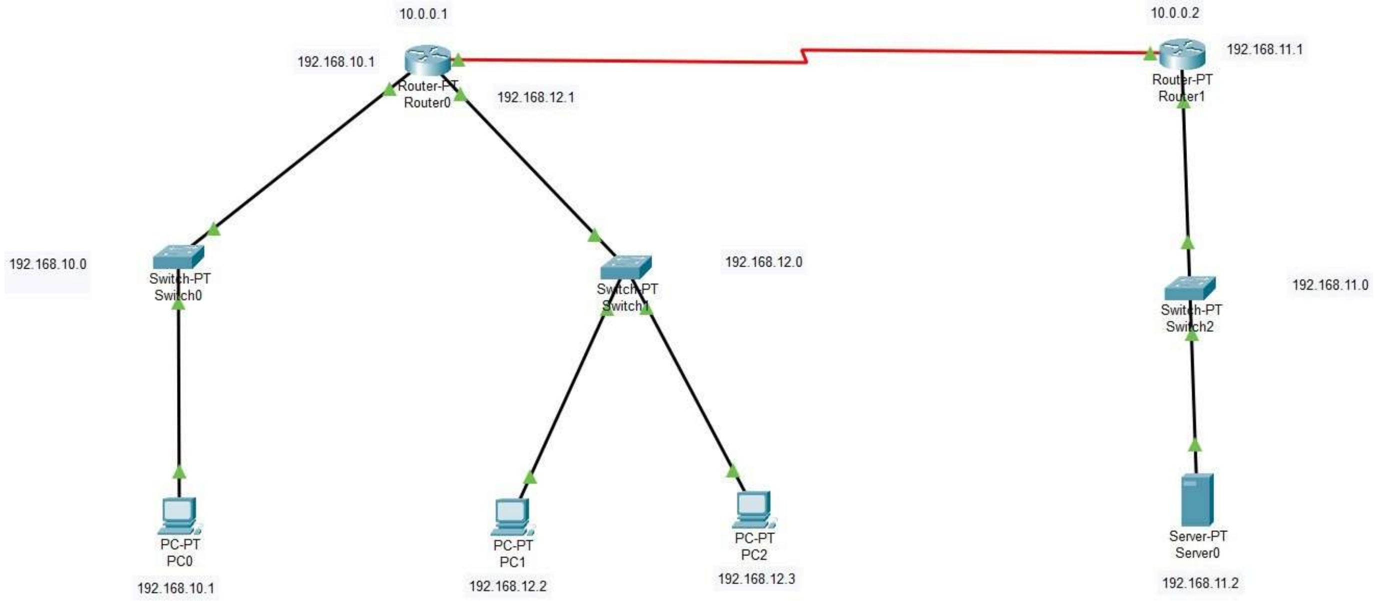
We can classify Access Control Lists (ACL) as

- Numbered and Named Access Control Lists (ACL): A Numbered ACL is assigned a unique number among all Access Control Lists (ACL), but a Named Access Control Lists (ACL) is identified by a unique name.

- Standard and Extended Access Control Lists (ACL): Standard IP Access Control Lists (ACL) can be used filter traffic only based on the source IP address of the IP datagram packet. An extended Access Control Lists (ACL) can be used to filter traffic based on Source IP address, Destination IP address, Protocol (TCP, UDP etc),Port Numbers etc.

NETWORK DESIGN

The following is the network design.



It consists of 4 networks:

First network: 192.168.10.0

Second Network: 10.0.0.0

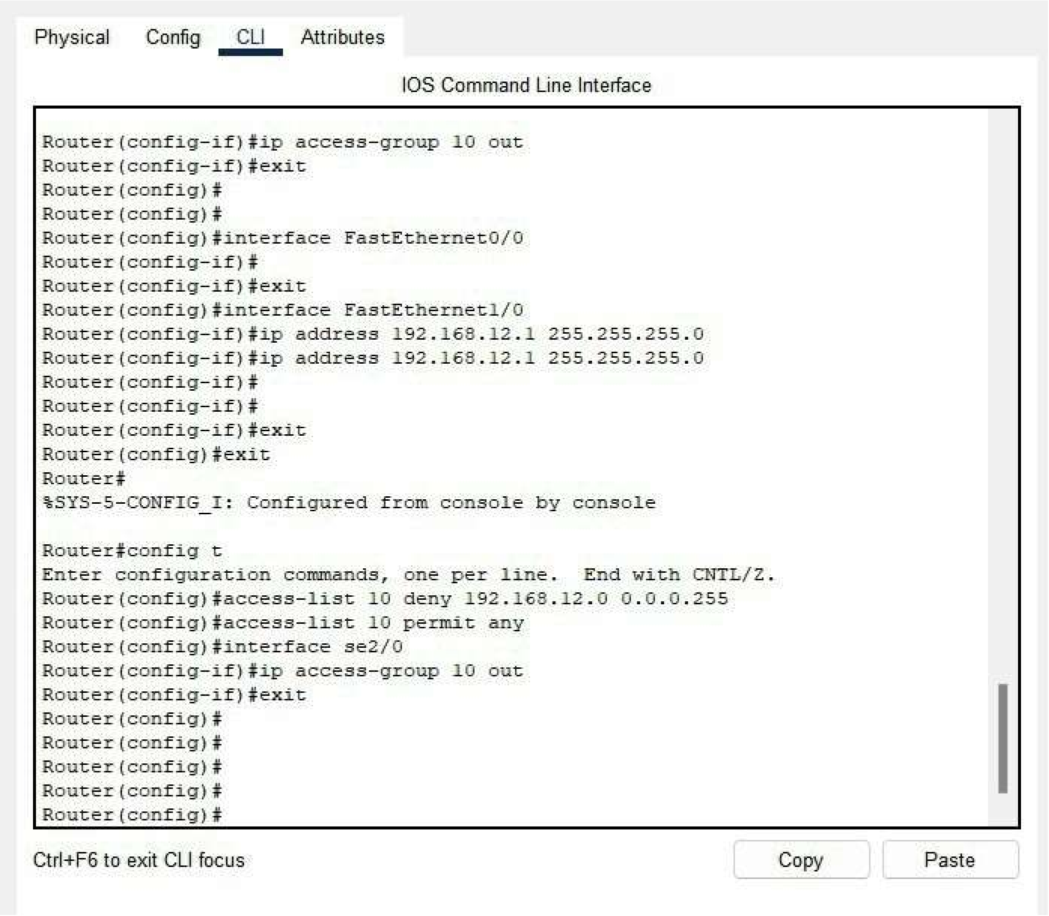
Third Network: 192.168.11.0

Fourth Network: 192.168.12.0

Device	Interface	Ip Address
PC0	Fa0/0	192.168.10.2
PC1	Fa0/0	192.168.11.2
PC2	Fa0/0	192.168.11.3
Server0	Fa0/0	192.168.12.2
Router 3	FastEthernet 0/0	192.168.10.1
Router 3	Serial0/0/0	10.0.0.1

Router 3	FastEthernet	192.168.11.1
Router 2	FastEthernet 0/0	192.168.12.1
Router 2	Serial0/0/0	10.0.0.2

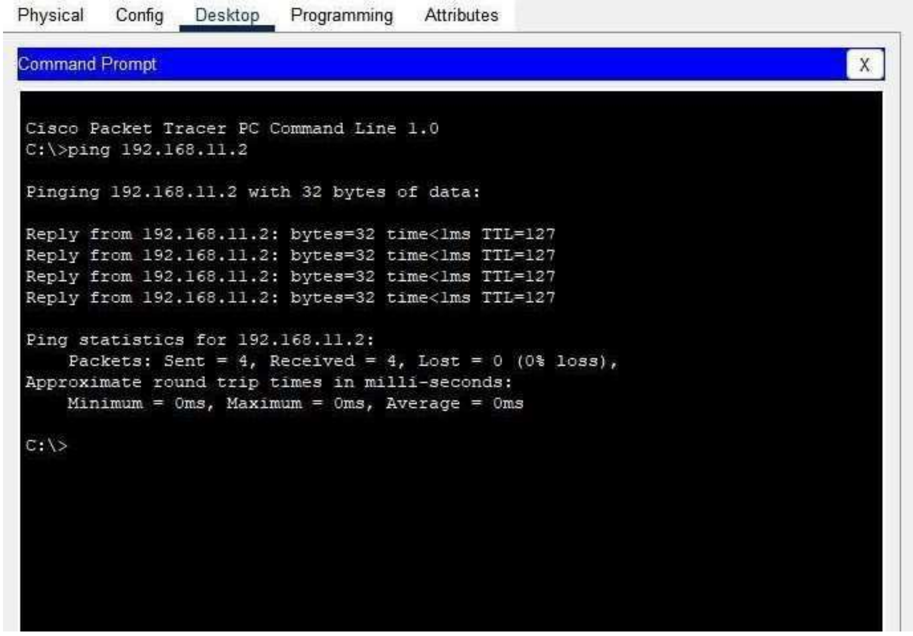
ACL COMMANDS



```
Router(config-if)#ip access-group 10 out
Router(config-if)#exit
Router(config)#
Router(config)#
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet1/0
Router(config-if)#ip address 192.168.12.1 255.255.255.0
Router(config-if)#ip address 192.168.12.1 255.255.255.0
Router(config-if)#
Router(config-if)#
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 10 deny 192.168.12.0 0.0.0.255
Router(config)#access-list 10 permit any
Router(config)#interface se2/0
Router(config-if)#ip access-group 10 out
Router(config-if)#exit
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
```

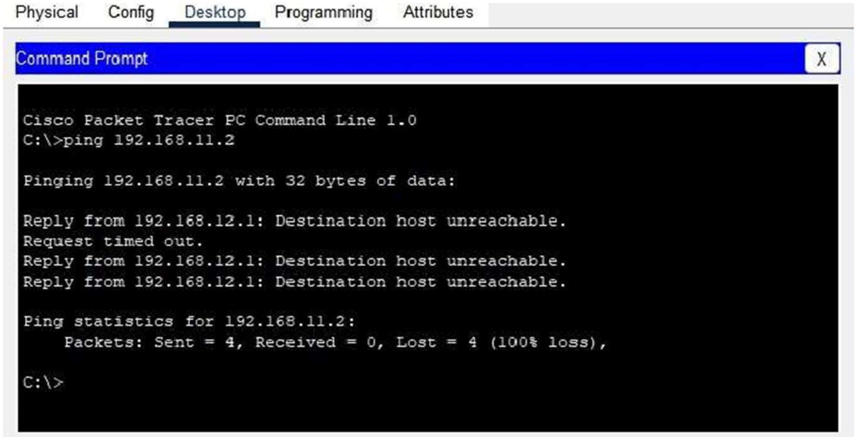
OUTPUT:

Pinging server from Permitted Network (192.168.10.0):

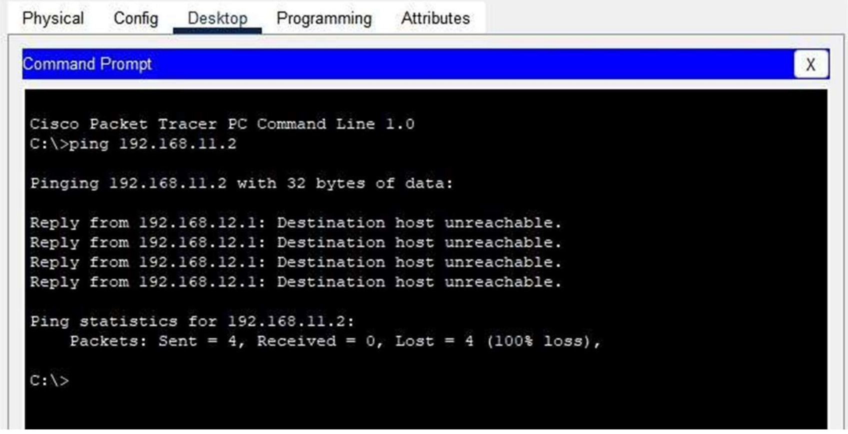


```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.11.2

Pinging 192.168.11.2 with 32 bytes of data:

Reply from 192.168.11.2: bytes=32 time<1ms TTL=127
Reply from 192.168.11.2: bytes=32 time<1ms TTL=127
Reply from 192.168.11.2: bytes=32 time<1ms TTL=127
Reply from 192.168.11.2: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.11.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Pinging server from Denied Network (192.168.12.0):



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.11.2

Pinging 192.168.11.2 with 32 bytes of data:

Reply from 192.168.12.1: Destination host unreachable.
Request timed out.
Reply from 192.168.12.1: Destination host unreachable.
Reply from 192.168.12.1: Destination host unreachable.

Ping statistics for 192.168.11.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.11.2

Pinging 192.168.11.2 with 32 bytes of data:

Reply from 192.168.12.1: Destination host unreachable.
Reply from 192.168.12.1: Destination host unreachable.
Reply from 192.168.12.1: Destination host unreachable.
Reply from 192.168.12.1: Destination host unreachable.

Ping statistics for 192.168.11.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

RESULT

Numbered Access Control List has been implemented on PC0.

CONCLUSION

Access control lists are used for controlling permissions to a computer system or computer network. They are used to filter traffic in and out of a specific device. Those devices can be network devices that act as network gateways or endpoint devices that users access directly.

After implementing Access control on Router for PC0 we can see that PC0 is not being able to connect to the server. The permission is being denied by the gateway router which is not passing any packets that are sent by PC0. On the other hand, all the other PCs are able to communicate with server because they have been allowed on the network.

Access Control List is a great way to filter out traffic in and out of a device or a network. This method provides security by filtering out unwanted traffic and devices from the network.

RSA ALGORITHM

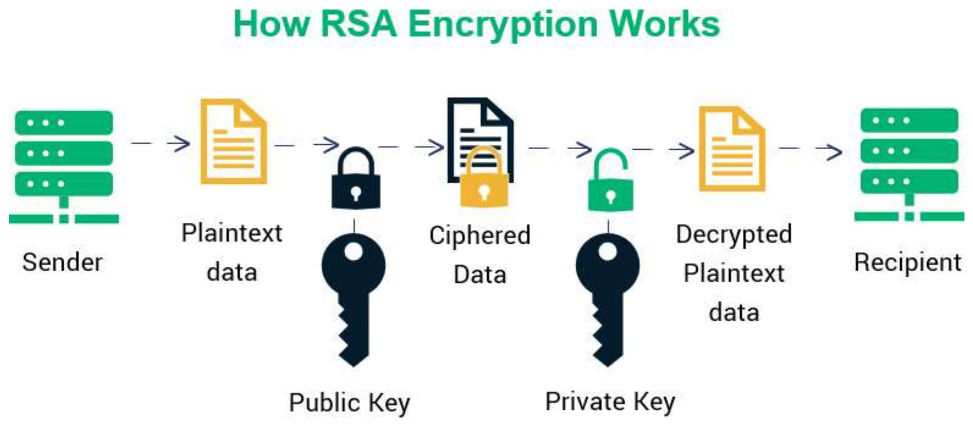
AIM:

To perform RSA (Rivest–Shamir–Adleman cryptographic algorithm.

THEORY:

Cryptography is playing a major role in data protection in applications running in a network environment. It allows people to do business electronically without worries of deceit and deception in addition to ensuring the integrity of the message and authenticity of the sender. It has become more critical to our day-to-day life because thousands of people interact electronically every day; through e-mail, e-commerce, ATM machines, cellular phones, etc. This geometric increase of information transmitted electronically has made increased reliance on cryptography and authentication by users. Despite the fact that secured communication has existed for centuries, the key management problem has prevented it from commonplace application. The development of public-key cryptography has enabled large-scale network of users that can communicate securely with one another even if they had never communicated before.

This paper considers a Public Key encryption method using RSA algorithm that will convert the information to a form not understandable by the intruder therefore protecting unauthorized users from having access to the information even if they are able to break into the system.



ALGORITHM:

Begin

1. Choose two prime numbers p and q.
2. Compute n = p*q.
3. Calculate phi = (p-1) * (q-1).
4. Choose an integer e such that 1 < e < phi(n) and gcd(e, phi(n)) = 1; i.e., e and phi(n) are coprime.
5. Calculate d as d ≡ e−1 (mod phi(n)); here, d is the modular multiplicative inverse of e modulo phi(n).
6. For encryption, c = me mod n, where m = original message.
7. For decryption, m = c d mod n.

End

PROGRAM:

```
#include<iostream>
#include<math.h>
using namespace std;
// find gcd
int gcd(int a, int b)
{
   int t;
   while(1) {
      t= a%b;
      if(t==0)
      return b;
      a =  b;
      b= t;
   }
}
int main()
{
   //2 random prime numbers
   double p ;
   double q ;
   cout<<"Enter prime p->";
   cin>>p;
   cout<<"Enter prime q->";
   cin>>q;
```

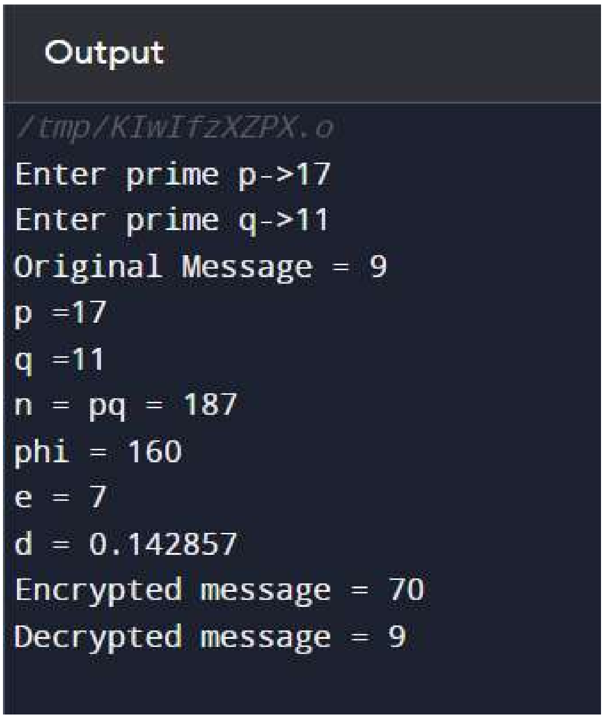
```
    double n=p*q;//calculate n
    double track;
    double phi= (p-1)*(q-1);//calculate phi
    //public key
    //e stands for encrypt
    double e=7;
    //for checking that 1 < e < phi(n) and gcd(e, phi(n)) = 1; i.e., e and phi(n)
are coprime.
    while(e<phi)
    {
        track = gcd(e,phi);
        if(track==1)
            break;
        else
            e++;
    }//private key
    //d stands for decrypt
    //choosing d such that it satisfies d*e = 1 mod phi
    double d1=1/e;
    double d=fmod(d1,phi);
    double message = 9;
    double c = pow(message,e); //encrypt the message
    double m = pow(c,d);
    c=fmod(c,n);
    m=fmod(m,n);
    cout<<"Original Message = "<<message;
    cout<<"\n"<<"p ="<<p;
    cout<<"\n"<<"q ="<<q;
    cout<<"\n"<<"n = pq = "<<n;
    cout<<"\n"<<"phi = "<<phi;
    cout<<"\n"<<"e = "<<e;
    cout<<"\n"<<"d = "<<d;
    cout<<"\n"<<"Encrypted message = "<<c;
    cout<<"\n"<<"Decrypted message = "<<m;
    return 0;
}
```

Sample Input:

p-> 17

q-> 11

Sample Output:



```
/tmp/KIwIfzXZPX.o
Enter prime p->17
Enter prime q->11
Original Message = 9
p =17
q =11
n = pq = 187
phi = 160
e = 7
d = 0.142857
Encrypted message = 70
Decrypted message = 9
```

ADVANTAGES AND DISADVANTAGES OF RSA:

Advantages

- It is very easy to implement RSA algorithm.
- RSA algorithm is safe and secure for transmitting confidential data.
- Cracking RSA algorithm is very difficult as it involves complex mathematics.
- Sharing public key to users is easy.
- The use of Digital Signature makes it safe from repudiation.
- It may be used with Secret Key Cryptography.

Disadvantages

- It may fail sometimes because for complete encryption both symmetric and asymmetric encryption is required and RSA uses asymmetric encryption only.
- It has slow data transfer rate due to large numbers involved.
- It requires third party to verify the reliability of public keys sometimes.
- High processing is required at receiver's end for decryption.
- RSA can't be used for public data encryption like election voting.
- Key generation is very slow.
- Speed of encrypting of text is slow.
- Message length should be less than the bit length otherwise algorithm will be failed.
- RSA is factorization-based algorithm so that every time RSA initialization takes two large prime number p and q.
- If private keys of users are not available, it is vulnerable to impersonation.

Result:

Hence the implementation of RSA asymmetric algorithm has been successfully Implemented.