OORJA

ISSN - 0974-7869 (Print)
ISSN - 2395-6771 (Online)

Using Hybrid Approach Secure Data Transmission over Medium

Ajeet Kumar Vishwakarma
Assistant Professor
Institute of Management & Computer Science
NIMS University, Jaipur

Ruchir Saxena
Head of Department
Institute of Management & Computer Science
NIMS University
Jaipur

Abstract

In this era's of the privacy and security concerns prevailing in the environment, users are more likely to require privacy; that is traceable. There should be an authentication mechanism for the client using services needed in various real-world applications. The security of computer is related to the whole world and individual. Secure data transmission is the technique of achieving security used by decoding or encoding message to make them non-readable to encrypted so that secure data or information transmits over the internet work. In this paper, we are introducing an approach based on multiple public keys and 'n' prime number. Hybrid algorithm is mostly used in implementation of public key and symmetric key cryptography. This paper uses public key cryptography with two different keys and DES. In public key Cryptography, one key is used in encryption data and other key used for decryption of keys. Second key does not decrypt the data to find out readable form. Even if it is useful algorithm it is vulnerable to other person. In this research paper we are trying to develop new approach by using prime number and multiple public keys and triple DES.

Keywords: Asymmetric key cryptography, 'n' prime number, Cryptography, RSA algorithm, Triple DES.

Introduction

In this proposed work the network security and network infrastructure is investigated. According to the recent research trends, the major issues on the available security architecture is recognized. Additionally for providing optimum solution, new security architecture is designed and implemented in this work. In order to provide security for the network data centers, previously available security mechanism is improved in terms of efficiency. For that purpose one time password, DES encryption algorithm and the third party authentication mechanism is incorporated with the system design. The proposed security architecture is responsible for secure file transfer and sharing.

ISSN - 0974-7869 (Print)
ISSN - 2395-6771 (Online)

It is an ancient methodology to hide private messages from others, but these methods are significantly improved in modern days. In various application confidential data is involved and it is transmitted over internet, but the data is not much secure. Therefore to protect data in these applications, it is highly recommended to use the cryptographic methods.

In a Secure network, data cryptography became important part of secure communication. There are three types of cryptography algorithm:

1. Symmetric Key Cryptography
2. Hashing
3. Asymmetric Key Cryptography.

Symmetric key cryptography uses an algorithm that uses the same keys for both encryption of normal text as well as for decryption for cipher text. The concept of public key cryptography to solve the key distribution problem was developed by Whitfield Diffie and Martin Hellman, Network platform usually refers to application host that offers computational power, storage and web access. Amazon Elastic Network Computing (EC2) and Google App Engine (GAE) are two well-known network platforms based on virtualization, where each EC2 instance is a virtual machine. Users can choose different Operating Systems and hardware architectures to run on their VMs.

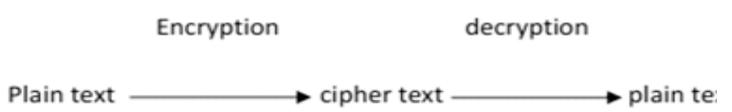
Through Hybrid Approach data can be transferred over the network, where public key is used for encryption and because it is well known to everyone, so with the help of public key, an attacker can apply brute force method to find private key which is to be used further for message decryption.

This algorithm is similar to RSA and DES with few modifications. Algorithm is also known by public key cryptography. In this algorithm we are using two public keys and very large number that has few prime factors in addition.

Related work

Cryptanalysis is a process, which is associated with encoding readable into cipher text (encryption process) then back again readable i.e. decryption. There are two different keys public key and private key which are being used in asymmetric key cryptography, where private key cannot obtain by public key.

This is the key difference between asymmetric and symmetric key cryptography, and that major difference changes the whole mechanism. Mostly it has implication throughout the security. As compared, symmetric key cryptography is faster, more easy and better suited for application while the drawback of symmetric key cryptography over asymmetric key cryptography is it's less secure and more open to wider areas of attacks.



ISSN - 0974-7869 (Print)
ISSN - 2395-6771 (Online)

Literature review

Hybrid methodology is used for confidentiality and authentication. This research paper uses secure transmission over the computer and network to increase the efficiency and security.

This is new way to deliver services while reducing ownership, improving responsiveness and allowing the decision makers to focus their attention on the business rather than their IT infrastructure. There is no organization that has not thought about moving to the Network. It was proposed by IBM Corporation in 2007. Since then many leading companies like Google, Microsoft, Amazon etc. are working on the network computing. Network computing is different for the different people; no exact definition can be given to network. Generally there are three types of computer users that are end users, web developers and businessmen.

Ravi Shankar suggested that the Security of Hybrid algorithm depends on prime number because it is difficult to track large prime number. Here we are proposing a hybrid algorithm that provides security against brute force attack.

Problem Definition

Security is the key for the data success. The security in the network is now the main challenge of network computing. Till few years ago all the business processes of organisations were on their private infrastructure and, they were outsourcing services. Now with network computing, the story is changed. Organization feels they have lost control over their data. The traditional network perimeter is broken, and the benefit of being accessible from anywhere becomes a big threat.

Solution

In this research paper we are proposing an algorithm based on RSA algorithm using two public key with a 'n' prime number and DES.This algorithm provides high security over the network and secure data is transfered on the transmission medium.

Computational steps for Mathematical foundation and key generation in RSA of algorithm

A: -The RSA digital signature has appropriate mathematical foundation, which is as follow

Theorem 1:

a positive Integer a can be denoted by AI where

$$A_i=p_1\ p_2\ p_3\text{----------}p_n,\quad \forall p_n\ ,\ \mathbf{A_i>0}$$

Where $p_1,\ p_2,\ p_3$…….are prime numbers

Theorem 2

The greatest common divisor (gcd) of the positive integer a and b can be represented as a liner sum of original two number a and b (Euclid theorem). In other world, it is always possible to integer s and t such that-

ISSN - 0974-7869 (Print)
ISSN - 2395-6771 (Online)

g =s*a+t*b [6]

Theorem 3

If p is a large prime number, then for any positive integer a, then a^p=a mod (p) or a^{p-1}=1 (mod p) : Fermatlittle theorem

Theorem 4:

If p and q are two prime numbers such that p is not equal to q then

$$\Phi(p\ q) = \Phi(p) * \Phi(q) = (p-1)(q-1)$$

B: RSA key generation algorithm-

1. Find p and q two different large random prime number.

2. Calculate n=p*q and xΦ(n) = (p-1)*(q-1) [theorem 4]

3. Where Φ is an Euler's function

4. Choose an integer e,such that 1<e< Φ (n) and gcd (e, Φ (n)) =1 [theorem 2] where Φ (n) and e are co-prime.

5. Compute d which is multiplication inverse of e mod(Φ (n))

i.e. e *d mod Φ(n) =1

6. The public key is (e, n) and private key is (d, n).

Encryption:-

Sender A knows the following

1. Receive the receiver B's public key.

2. The plaintext message as a positive Integer m.

3. Find the cipher text C=m^e mod n

4. calculated C sends to B

Decryption:-

Receiver B does the following

1- Compute m=c^d mod n by using private key.

2-Get original plain text m

Hybrid algorithm:

In 1024 bit block RSA cipher, the plain text and cipher text integer value lie between 0 to n-1, in which four prime number are being used to generate get public key and private key and also uses two public keys and one private key for encryption and decryption

ISSN - 0974-7869 (Print)
ISSN - 2395-6771 (Online)

RSA key generation

1. Computational steps for selecting the largest prime number p,q,r and s in RSA cryptography.

a. Firstly, we decide upon the size of integer and implementation if RSA of size B Bits.

b. Generate the prime integer p, q, r and s;

c. Using the high quality random number generator. We first generate a B/2 bits size random number.

d. Set the lowest bit of integer generated by the above step which ensures that the number will be odd.

e. We also set the two highest bits of the integer: this ensures that the highest bits of null are set.

2. Compute n= p*q*r* s and $\Phi(n) = (p-1)(q-1)(r-1)(s-1)$

3. Where is Euler's function.

4. Select an integer value e, where e lies between 1 to $\Phi(n)$ and gcd $(e, \Phi(n)) = 1$.

5. Find two number a and b such that b=a*e and using this number two public keys {b, e}, {a}.

6. Finally compute d as multiplication inverse of e mod $(\Phi(n))$

Encryption:

During the process of sending encrypted information, the random number generator uses triplets DES session key only once. It encrypt the plaintext to output cipher text. On the other hand, the originator get public key from public key management centre, and then uses Hybrid to encrypt session key. Finally, the mixture of the session generated.

Decryption:

Decryption of the cipher text by A and user A decrypt message $m= c^d \bmod n= (m^{b/a})^d \bmod n = m^{b/ad} \bmod n$.

Both sender and receiver must know about the values of n, b and a. Only receiver knows the secret value of d. In asymmetric key cryptography with public key K.U={b,n},{a} and private key of K.R ={d,n}. These keys are being generated dynamically over the network and stored on database corresponding to data item sent or received by the clients.

Comparison among RSA, Hybrid public key algorithm and MRSA using n prime number

A general comparison among RSA, Hybrid algorithm and Modified RSA using n prime number, we found that by increasing module length this algorithm decreases the speed and increases the security.

ISSN - 0974-7869 (Print)
ISSN - 2395-6771 (Online)

In the context of Key generation, Hybrid RSA with n prime number is faster than MRSA, while in encryption all are working almost same. There is only one additional multiplication operation is for each divided calculation in the algorithm.

For decryption point of view, Hybrid algorithm and RSA have almost same overall performance. MRSA with n prime number is better in security but less in speed and throughput.

Table No. 1 : Comparison among RSA, Hybrid public key algorithm and MRSA with n prime number

S.No.	RSA	Hybrid algorithm	MRSA with n prime number
1.	Use only one public key	Use 2 public key	Use 2 public key
2.	Less communication overhead	Medium communication overhead	High communication overhead
3.	Process speed is fast	Process speed is slow	Process speed is very low
4.	It has less security	It is increasing security	It is provide more security
5.	More permeable to brute force attack	Less permeable to brute force attack	Little permeable to brute force attack
6.	Using encryption and decryption required time is more.	Using encryption and decryption required time is less.	Using encryption and decryption required time is more less.

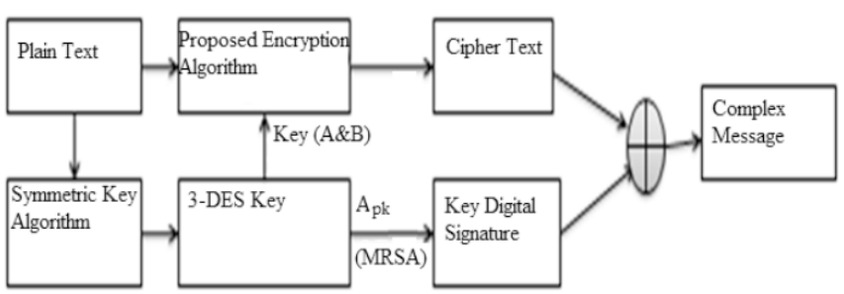


Figure I : System Overview

With the recent medium of data transmission and sharing on network systems such as online social networks or distributed network, these demands and concerns have been increasing for distributed data security to improving security and efficiency in data sharing over the transmission medium and network.

In three levels of Authentication are provided with a dedicated architecture.

First Level: It is the User, who is having all the privileges to add clients, for sharing specific node or to all the workstations members.

ISSN - 0974-7869 (Print)
ISSN - 2395-6771 (Online)

Second Level: Here only authentication nodes access network.

Third Level: After second level verification, client access network then this permission granted by Data Access Control level.

Conclusion and Future work

In this proposed algorithm we are implementing a public key cryptography (RSA) using two public and four prime number and DES symmetric key Approach for same mathematical equations. Using two public keys and n prime number, provides the security over the network where the attacker cannot get keys therefore it prevents the decryption of the message. The Discovered Hybrid approach is used for system that provides more security though it decreases the speed comparatively with other algorithms but improves security and efficiency in data sharing over the network. This would be inspiring for advance research in the context of secure transmission of file, image file, network computing etc. This may perhaps be our future research topic using hybrid data encryption and decryption approach.

References

- AtulKahate, Cryptography and Network Security, Tata McGraw-Hill Publication Company Limited page no. 32.
- XiaowenKang; Inst. of Electron. Technol., PLA Inf. Eng. Univ., Beijing; Yingjie Yang; Xin Du,"ADisaster-Oriented Strong Secure File System"Innovative ComputingInformation and Control, 2008.ICICIC '08. Pages 557.
- XinZhou, Xiaofei Tang,"Reasearch and Implementation of RSA algorithm for Encryption and Decryption "IEEE 6th International Forum on strategic Technology pp 1118-1121.
- Rajan.S.Jamgekar, Geeta Shantanu Joshi "File Encryption and Decryption using secure RSA" International Journal of Emerging Science and Engineering (IJESE) ISSN: 2319–6378, Volume-1, Issue-4, February 2013.
- Maheswari Losetti, Kanaka Raju Gariga "An Enhanced RSA Algorithm for Low Computational Devices" International Journal of AdvancedResearch and Innovations Vol.1, Issue .2, pp 114-118.
- en.wikipedia.org/wiki/Euclidean algorithm
- B.Persis Urbana Ivy, Purshotam Mandiwa. Mukesh Kumar "A modified RSA cryptosystem based on 'n' prime numbers"International Journal of Engineering and Computer Science ISSN: 2319-7242 Volume1 Issue 2 Nov 2012 Page No. 63-66
- en.wikipedia.org/wiki/Random_number_generation
- Avinash kak, Purdue University LectureNotes on "Computer and Network Security"June20, 2013

ISSN - 0974-7869 (Print)
ISSN - 2395-6771 (Online)

· Amare Anagaw Ayele ,Dr. Vuda Sreenivasarao "A Modified RSA Encryption Technique Based on Multiple public keys"International Journal of Innovative Research in Computer and Communication Engineering Vol. 1, Issue 4, June 2013.

· Rangarajan A. Vasudevan,Sugata Sanyal"Jigsaw-based Secure Data Transfer over Computer Networks"

· Wuling Ren, Zhiqian Miao, College of Computer and Information Engineering, Zhejiang Gongshang University, "A Hybrid Encryption Algorithm Based on DES and RSA" in Bluetooth Communication Second International Conference on Modeling, Simulation and Visualization Methods2010.

· A.Shukla, V.Kapoor, IET DAVV University, Indore, "Data Encryption and Decryption using Modified RSA Cryptography Based on Multiple Public Keys and 'n' Prime Number" international journal of engineering sciences &research technology 2014.