A New Approach to Communicate Secret Message (Key) Among a Group using Chain Matrix Multiplication Based on Public Key Crypto System

Nageswara Rao Eluri, K. Venkata Rao, M. SomaSundara Rao, Mohammed Abazeed Bazeed

Abstract- Group key management is a fundamental building block for secure group communication systems. It is required for many applications such as teleconference, group meeting etc. Proposed System, Secure Group Communication in public key cryptography systems is proposed for dynamic groups which are secure. In this scheme a group is established and a master key is generated using the dynamic approach chain matrix multiplication and text messages are transmitted between users of group with help of Master key and also between sub groups. In our approach, group key will be updated when a user joins or leaves the group. Confidentiality can be achieved through changing re-keying when user joins or leaves the group.

Keywords: Key Distribution, Chain matrix Multiplication, Server/Client communication, RSA, Encryption and Decryption.

I. INTRODUCTION

Now a day's information security places a vital role, when two persons are communicating each other by sending messages then there is a chance of accessing the same message by unauthorized persons. So by providing the security services the unauthorized persons are denied access to these messages. To do this we have encryption algorithms, Symmetric encryption and asymmetric encryption (or) public key encryption.

The symmetric encryption will have single key where as the public-key encryption involves two keys, public and private keys. In the public-key encryption algorithm for sending the messages the sender will create the cipher text by encrypting the message by one key, the receiver will get the plain text by decrypting the cipher text with other key. If the sender is to send the message to group of members then the sender must send the messages individually one after another [1, 2].

To overcome this we go for the Secure Group communication in Public Key Cryptographic Systems (using chain matrix multiplication). A group is established and a master key is generated using the dynamic approach chain matrix multiplication and text messages are transmitted between users of group with help of Master key and also between sub groups. In our approach, group key will be updated when a user joins or leaves the group.

Manuscript received December, 2013.

Mr. Nageswara Rao Eluri, Lecturer, Information Systems, King Khalid University Abha, Kingdom Of Saudi Arabia.

Dr. K. Venkata Rao , HOD, Computer Science Engineering , Vignan's Institute of Information Technology, VisakhaPatnam, Andhra Pradesh, India.

Prof. SomaSundara Rao, HOD of MCA, Vignan IIT, Duvvada , Visakha Patnam, Andhra Pradesh, India .

Key Distributi3on

This section covers methods of distributing keys in ways that, without using public-key cryptography, reduce, without eliminating, the need to transport keys securely.

In practice, of course, a layer of public-key cryptography could be used as an additional safeguard for the secure transmission of keys for these methods. [2]

Simple Key Sharing

A set of cipher machines could each be given exactly half of the keys in a large set. As long as no cipher machine is made that has exactly the opposite set of keys as another machine, any two cipher machines would be able to communicate.

At least three cipher machines would need to be broken into to get the complete set of keys, but that means this protocol is not particularly resistant to collusion.

Note also that the set of keys shared between a pair of machines is not guaranteed to be unique, so some messages may be readable with the keys other machines have. In practice, this technique would also rely on the machines having tamperproof hardware, not only to protect the keys, but to restrict their use to decoding appropriately addressed messages.

The total number of keys in the system needs to be large enough, and the fraction given to each terminal small enough (but the number each terminal has large enough) that it is difficult for a number of colluding terminals to obtain enough keys to make smartcards that can fool other terminals.

The scheme can be made more elaborate by issuing the smartcards keys corresponding to block pairs held by the terminals as well. Because of the difference in resources, in this case each smartcard would be issued a very small fraction of a pool of possible keys that could be larger in size.

II. METHODOLOGY

The symmetric encryption will have single key where as the public-key encryption involves two keys, public and private keys. In the public-key encryption algorithm for sending the messages the sender will create the cipher text by encrypting the message by one key, the receiver will get the plain text by decrypting the cipher text with other key. If the sender is to send the message to group of members then the sender must send the messages individually one after another.

To overcome this we go for the Secure Group Communication in Public Key Cryptographic Systems (using chain matrix multiplication).

A group is established and a master key is generated using the dynamic approach chain matrix multiplication and text messages are transmitted between users of group with help of Master key and also between sub groups. In our approach, group key will be updated when a user joins or leaves the group.

This is to maintain confidentiality. Confidentiality can be achieved through changing the key material, known as ekeying every time a new member joins the group or existing member leaves from the group. The new group key is omputed guaranteeing forward and backward secrecy. whenever there is a membership change; group key must be changed to prevent a new user from reading past communication, called backward access control and a departed user from reading future communications, called forward access control.

Once a communication group is formed, the members in a group can send /receive messages from other members of same/different groups. To send a message a user needs to login, compose a message and send to user/users. The message is encrypted using RSA algorithm and is transmitted to the receiver user/users. The entire process of communication is done by establishing Client-Server environment using socket programming. [5]

The main objective of our proposed scheme is to establish the Client-Server Environment. When a new member is added or deleted from the group the server generates the new group keys and send them to the members. The server also generates the individual public and private keys for the members and these are constant. The message can be sent by the members within the organization either to a single user or to any group of users in the organization by encrypting the plain text by their public keys. The messages will be received successfully and they can view the messages by decrypting the cipher text with their private key. If the message is sent to any particular user then he can view the message by decrypting with his / her group private key. If the message is sent by a member to a group then the members within the group will view the message by decrypting it with their corresponding group private key.

The trusted authority is available, it is possible to use methods based on the principles examined above to allow members of a group to communicate with each other in pairs with a convenience similar to that afforded by public key cryptography. Initially, each member must receive keys from the trusted authority over a secure channel [6, 7].

Also, it is required to deal with the field giving the number of arguments; three common alternatives for doing what is required are:

i. The field may have a fixed length, such as one or two bytes;
ii. The field may begin with a fixed-length length indicator, such as a one or two byte field giving the number of bytes which contain the number of arguments (this, of course, provides for enormous, if finite, numbers of arguments);

The field may be expressed in a notation which includes a terminating character, such as being given in ASCII with a terminating null or space, or by being given in BCD with a terminating 1111 nibble [7, 8]. The first and second alternatives have the disadvantage of imposing a finite limit (although in the second case, one that is enormously large) on the numbers represented, the third involves a continuing inefficiency throughout the whole representation of the number of excluding at least the value of the terminating symbol from the possible digits used.

Chain Matrix Multiplication:

The chain matrix multiplication problem involves the question of determining the optimal sequence for performing a series of operations. Suppose, matrix A has p rows and q columns i.e., the dimension of matrix A is $p \times q$. You can multiply a matrix A of $p \times q$ dimensions *times* a matrix B of dimensions $q \times r$, and the result will be a matrix C with dimensions $p \times r$. That is, you can multiply two matrices if they are **compatible** the number of columns of A must equal the number of rows of B.

In particular, for

$1 \leq i \leq p$ and $1 \leq j \leq r$, we have

$$C[i, j] = \Sigma_{1 \leq k \leq q} A[i, k]\, B[k, j].$$

There are $p.\ r$ total entries in C and each takes $O(q)$ time to compute, thus the total time to multiply these two matrices is dominated by the number of scalar multiplication, which is $p\ .q\ .\ r$.

Problem Formulation

Note that although we can use any legal parenthesization, which will lead to a valid result. But, not all parenthesizations involve the same number of operations. To understand this point, consider the problem of a chain $A1$, $A2$, $A3$ of three matrices and suppose A1 be of dimension 10 × 100 A2 be of dimension 100 × 5.

A3 be of dimension 5 × 50, then

MultCost [((*A*1 *A*2) *A*3)] = (10×100×5) + (10×5×50) = 7,500 scalar multiplications.

MultCost [(*A*1 (*A*2 *A*3))] = (100×5×50) + (10×100×50) = 75,000 scalar multiplications. It is easy to see that even for this small example, computing the product according to first Parenthesization is 10 times faster.[9]

The Chain Matrix Multiplication Problem

Given a sequence of n matrices $A_1, A_2 \ldots A_n$, and their dimensions $p_0, p_1, p_2 \ldots p_n$, where $i = 1, 2 \ldots n$, matrix A_i has dimension $p_{i-1} \times p_i$, determine the order of multiplication that minimizes the number of scalar multiplications.

Dynamic Programming Approach

The first step of the dynamic programming paradigm is to characterize the structure of an optimal solution. For convenience, let us adopt the notation $A_{i..j}$, where $i \leq j$, for the result from evaluating the product $A_i A_{i+1} \ldots A_j$. That is, $A_{i..j} \equiv A_i A_{i+1} \ldots A_j$, where $i \leq j$.

It is easy to see that is a matrix $Ai \ldots j$ is of dimensions $pi \times pi+ 1$.In parenthesizing the expression, we can consider the highest level of parenthesization. At this level we are simply multiplying two matrices together. That is, for any k, $1 \leq k \leq n-1$, $A_{1..n} = A_{1..k}\ A_{k+1}..n$.[9]

The sub chain problems can be solved by recursively applying the same scheme. On the other hand, to determine the best value of k, we will consider all possible values of k, and pick the best of them. Notice that this problem satisfies the principle of optimality, because once we decide to break the sequence into the product, we should compute each subsequence optimally.

That is, for the global problem to be solved optimally, the sub problems must be solved optimally as well.

The second step of the dynamic programming paradigm is to define the value of an optimal solution recursively in terms of the optimal solutions to sub problems. To help us keep track of solutions to sub problems, we will use a table, and build the table in a bottom up manner. For $1 \le i \le j \le n$, let $m[i, j]$ be the minimum number of scalar multiplications needed to compute the $A_{i..j}$. The optimum cost can be described by the following recursive formulation.

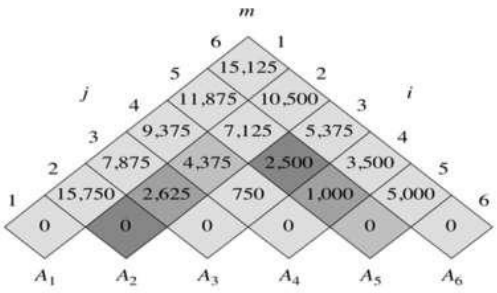
$$m[i,j] = \begin{cases} 0, & \text{if } i = j \\ \min_{i \le k \le j} \{ m[i,k] + m[k+1,j] + p_{i-1} p_k p_j \} & \text{if } i < j \end{cases}$$

The third step of the dynamic programming paradigm is to construct the value of an optimal solution in a bottom-up fashion.

For minimum scalar multiplication and splitting criteria

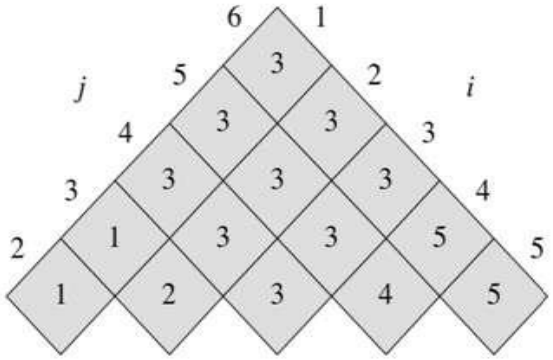
```
Matrix-Chain(array p[1.. n], int n)
{
Array s[1.. n −1,2.. n];
   FOR i =1 TO n DO   m[i, i]=0; //initialize
   FOR L=2 TO n DO {
    //L=lengthofsubchain
   FOR i  = 1 TO n −L+1 do
   {
      j = i +L−1;
    m[i, j] = infinity;
FOR k = i TO j −1 DO
{  //check all splits

q = m[i, k]+ m[k +1, j]+ p[i −1] p[k] p[j];

if (q <m [i,  j])
{
      m[ i,  j]= q;
      s[i,  j]= k;
}}}}
return m[1, n](finalcost)and s (splitting markers);
} }
```

The *m*-table computed by Matrix Chain procedure for $n = 6$ matrices $A1, A2, A3, A4, A5, A6$ and their dimensions 30, 35, 15, 5, 10, 20, 25



Minimum number of scalar multiplications. The running time of this procedure is O ($n3$) [2]. This is Step 4 of the dynamic programming paradigm in which we construct an optimal solution from computed information.

The array s[i, j] can be used.



Splitting criteria

By using chain matrix multiplication we can find out the optimal solution. By using splitting criteria we can find out where the optimal solution is obtained.

Multiplication of matrixes

```
Mult(i, j){
if (i == j)return A[i];       //Basis
else {
      k = s[i, j];
      X= Mult(i, k];         //X=A[i]…A[k]
      Y=Mult(k +1, j];       //Y=A[k+1]…A[j]
      return XY;
       //multiplymatrices  XandY
}
}
```

RSA Public-key Encryption Algorithm:

RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described it in 1978. RSA involves a public key and a private key**.** The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key.

The keys for the RSA algorithm are generated the following way:

1. Choose two distinct prime umbers p and q.

a. For security purposes, the integers p and q should be chosen at random, and should be of similar bit-length. Prime integers can be efficiently found using a primarily test.

2. Compute n = pq.
   a. n is used as the modulus for both the public and private keys
3. Compute $\varphi(n) = (p - 1)(q - 1)$, where φ is Euler's totient function.
4. Choose an integer e such that $1 < e < \varphi(n)$ and greatest common divisor of $(e, \varphi(n)) = 1$; i.e., e and $\varphi(n)$ are coprime.

a. e is released as the public key exponent.

b. e having a short bit-length and small Hamming weight results in more efficient encryption -most commonly 0x10001 = 65,537. However, small values of *e* (such as 3) have been shown to be less secure in some settings.

5. Determined as:

$d \equiv e^{-1} \pmod{\varphi(n)}$

i.e., d is the multiplicative inverse of e mod φ(n).

a. This is more clearly stated as solve for d given $(de) \bmod \varphi(n) = 1$

b. This is often computed using the extended Euclidean algorithm.d is kept as the private key exponent.

The public key consists of the modulus n and the public (or encryption) exponent e. The private key consists of the modulus n and the private (or decryption) exponent d which must be kept secret.

Encryption:

Sender transmits her public key (n,e) to receiver and keeps the private key secret. Receiver then wishes to send message M to sender. He first turns M into an integer m, such that 0<m<n by using an agreed upon reversible protocol known as a padding scheme. He then computes the cipher text C corresponding to $C = m^e \pmod n$.

This can be done quickly using the method of exponentiation by squaring. Receiver then transmits C to sender.

III. DECRYPTION:

Sender can recover M from C by using her private key exponent d via computing $M=C^d \pmod n$ given m, she can recover the original message M by reversing the padding scheme [6].

IV. CONCLUSION

For the messages delivered between the members of the group, the paper ensures confidentiality, authenticity, integrity. As there is a very important need for Secure Group Communications by many networking applications also on the internet, the paper has many network applications such as teleconferencing, information services, distributed interactive simulation, collaborative work, group meetings. Information Services is a system most commonly used on the internet these days where information on any subject is updated by the server to the peers registered to it .Distributed Interactive Simulation (DIS) is an open standard for conducting real time platform level war across multiple host computers and is used worldwide, especially by military organizations but also by other agencies such as those involved in space exploration and medicine.

FUTURE WORK

This work can be extend to group among group can be extend in Data mining and Data ware housing, Image processing by using this domain. We can increase the performance and reduce the time complexity of the process.

As the security aspects are increasing day by day, this factor helps in the group messaging in a broad manner. Hence privacy increases and this work is highly implemented in all the domains.

REFERENCES

1. http://www.conference.org
2. www.algorithmist.com/index.php/Chain_Matrix_Multiplication
3. www.oracle.com/technetwork/java/socket-140484.html
4. S Rafaeli- ACM Computing Surveys (CSUR), 2003 -dl.acm.org
5. L Dondeti - US Patent App. 12/804,216, 2010 – Google Patents
6. "NETWORK SECURITY ESSENTIALS" by William Stallings
7. Computer Networks by Fourazen
8. Network Programming by William Stallings
9. en.wikibooks.org/wiki/Java Programming/Client-server
10. http://www.waset.org/journals/waset/v34/v34-63.pdf
11. www.cse.ust.hk/dekai/271/notes/L12/L12.pdf
12. www.cs.sunysb.edu/jgao/CSE548-fall07/Davidmount- DP.pdf.
13. www.cs.umd.edu/meesh/351/mount/.../lect26-chainmx-mult.pdf
14. http://www.cs.tau.ac.il/ohadrode/papers/thesis/phd.pdf
15. en.wikibooks.org/wiki/Java Programming Version7
16. www.cs.umd.edu/NetBeans.pdf
17. www.cs.umd.edu/uml.pdf

AUTHORS PROFILE

Mr. Nageswara Rao Eluri Received M.Tech in Information Technology from Punjab University, M.Sc Computer Science from Bharatidasan University, 2003, 2000 respectively. Currently Working as a Lecturer in Information Systems, King Khalid University, Abha, Saudi Arabia. Previously worked as Assistant Professor in SASTRA University and Affiliated Engineering Colleges, Hyderabad, INDIA. My Research Interests includes Wireless Sensor Networks, Network security, Computer Networks.

Koduganti Venkata Rao Received Phd in Computer Science and engineering from andhra University, M.Tech in Computer Science and Technology from Andhra University and M.Sc computer Science from Nagarjuna University, 2008,1999,1994 respectively. Currently Working as Head of the Department and Professor in Computer Science Engineering , Vignan Institute of Information Technology, Visakhapatnam, Andhra Pradesh, India.

Mr. M. Soma Sundara Rao Pursuing phd from Jawaharlal Nehru University of Technology, Kakinada. Currently Working as Head of the Department and Associate Professor in Master of computer Applications , Vignan Institute of Information Technology, Visakhapatnam, Andhra Pradesh, India.

Mohammed Abazeed Bazeed pursuing PhD from University, Malaysia. Currently working as a Head of the Department and Lecturer in Information systems department, Khammis Mushait Community College, King Khalid University, Abha, Kingdom of Saudi Arabia.