Secure Groups Communication for Mobile Agents Based On Public Key Infrastructure

1. Problem Definition :

The use of mobile agents based computing in this emerging world of electronic transaction is becoming increasingly prevalent due to the enormous benefits and services that can be derived from it. They are good for distributed applications and hence an excellent paradigm when group communications are involved. A mobile agent is a software program that self transports from one host to another and interacting with other resources and agents within the network.
Security has been identified as one of the prime factors to the acceptability of distributed computer system and group communication operation in general. In normal situation, two parties are needed to initiate any communication. In terms of cryptography, there are two keys involved ; public key that must be exchange between the two parties and share key that should be shared between them. Share key must be protected from being accessed by others on the network. Therefore, the strength of the communication lays on the method of passing the share key without others being able to look at it.
We consider the problem of group communication security where two parties or more involve in the communication. The objectives of the formed group are to complete a given task that must be accomplished in a secure environment by proposing a new method to achieve secure group communication without having intermediary that cause overhead as introduced by previous methods.

2. Solution:

2.1 Existing Methodology :

The key distribution protocol introduced by Diffie-Hellman in conference key distribution system method is based on discrete logarithm. The chairperson is responsible to select the conference key and distributes it to other participants in the group. In the system, each participant only communicates with the chairperson through secure channel created for each participant. Therefore no direct communication with others is allowed in this protocol. All messages must go through the chairperson before reaches the intended parties.

Another approach that utilizes Diffie-Hellman key exchange protocol is called Key Agreement Protocol (KAP). This method is useful for both two and multiple parties. The method is good for group communication because it provides forward secrecy. In forward secrecy, no communication takes place during construction of the sharing key. In this method, each participant is assumed to know others public key in advance.

2.2 Proposed Approach :

In the previously proposed systems the participants only communicate with chairperson. Proposed protocol still employs the concept of chairperson and participants. However, here the only communication with the chairperson is done at the beginning of the protocol. Each participant then could communicate with other participants in the group securely with a newly generated shared key for the group.

This solution is able to avoid bottleneck at the chairperson site, which can generate network congestion as introduced by previous solutions.

Chairperson is a trusted party that trusted by all participants in the group. The chairperson will gather shared key from each participant. After getting all the shared keys from the participants, the chairperson generate a random number, *IV*, and computes a combine key, *CK*, by XOR-ing all the shared keys and the *IV*, $KI \oplus K2 \oplus K3$ ...... $\oplus\ Kn \oplus IV = CK$. The chairperson then hash the value, *GK* = Hash *(CK)* before encrypting it, *Eh(GK)* with each participant's shared key and distribute them to the participants. Each participant will use the group secret key, *GK*, to communicate with each other in the group.

Centralized communication will take place since each participant needs to communicate with chairperson to establish his or her Shared Key, *Kx* . Assuming each participant & chairperson knows each other's public key in advance, which can be achieved by storing all public keys in a trusted central pool.

Elliptic Curve Cryptography (ECC) is used for key exchange protocol.

3. Implementation:

3.1 Pseudo code

```
Initialization process ( Both user & chairman ) :
STEP 1 :  Choose a prime number P to finite field GF(P)

STEP 2 :  Choose elliptic curve parameters a and b . Such that $4a^3 + 27b^2 \neq 0$
          mod P.

STEP 3 :  Generate set of points Ep(a,b) that satisfies $y^2 = x^3 + ax + b$

STEP 4 :  Choose a base point G that has the smallest (x,y) co-ordinates
          From points in set Ep

Each participant's task :
STEP 1 : Each participant will generate private key less than the value of P ,
         Private Key for each participant < prime number P

STEP 2 : Each participant will compute his or her public, key.
         Each participant's public key is equal to,
          participant's private key x base point, G.
         The public key is a point in Ep(a, b).
         Public Key of each participant = Private Key of each participant x
         base point, G.
```

STEP 3: Each participant already has his or her own private key and public key. Therefore, they need to get the chairperson's public key to generate the shared key. Once they get chairperson's public key, shared key for each channel between participants and chairperson can be computed.

Shared Key of each participant, *Kx* = Private Key of each participant x Chairperson's Public Key.

STEP 4 : All participants should get their shared key, *Kx,* that will be used instead of using their public key. Each participant will encrypt the shared key using chairperson's public key and send it to the chairperson.

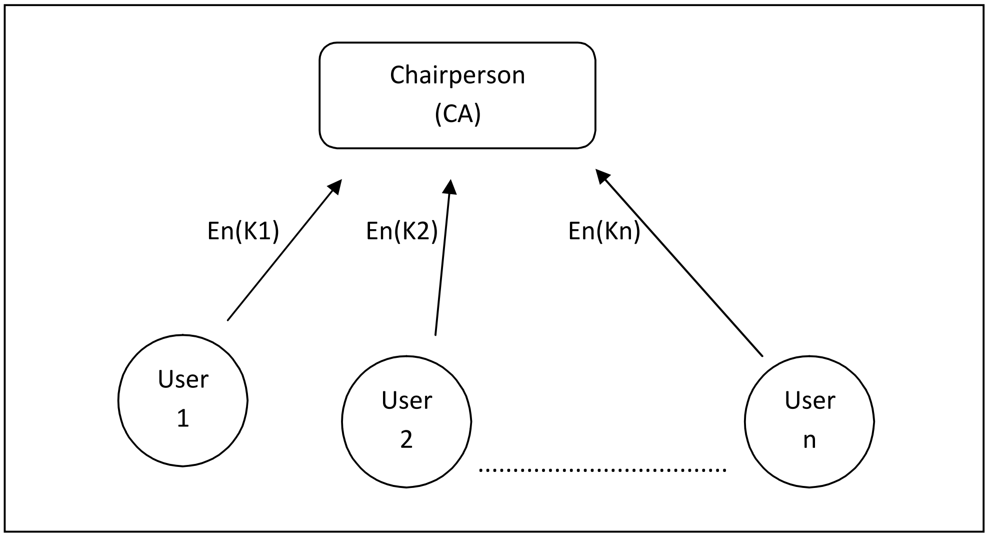


Figure 1. *Chairperson receives encrypted Shared Key of each participant*

Figure shows how participants and chairperson generate a shared key by exchanging their public key. Each participant and chairperson's connection will have a different Shared Key.

<u>Chairperson's tasks:</u>

STEP 1 : The chairperson should receive encrypted message from each participant that contains their shared key.

STEP 2 : Decrypt that message using the chairperson's private key.

STEP 3 : Generate *IV*, a random number.

STEP 4 : Compute Combine Key, *CK.* All participant's shared keys and IV will be XOR-ed together to produce the CK.

$CK = K1 \oplus K2 \oplus K3 \ldots\ldots\ldots \oplus Kn \oplus IV$

STEP 5 : Hashing the combine key value, CK with hash function to produce the group key, GK.

GK = Hash (CK)

STEP 6 : When Group Key, *GK* is ready, the chairperson will encrypt the group key with shared key of each participant and send it to all participants in the group.

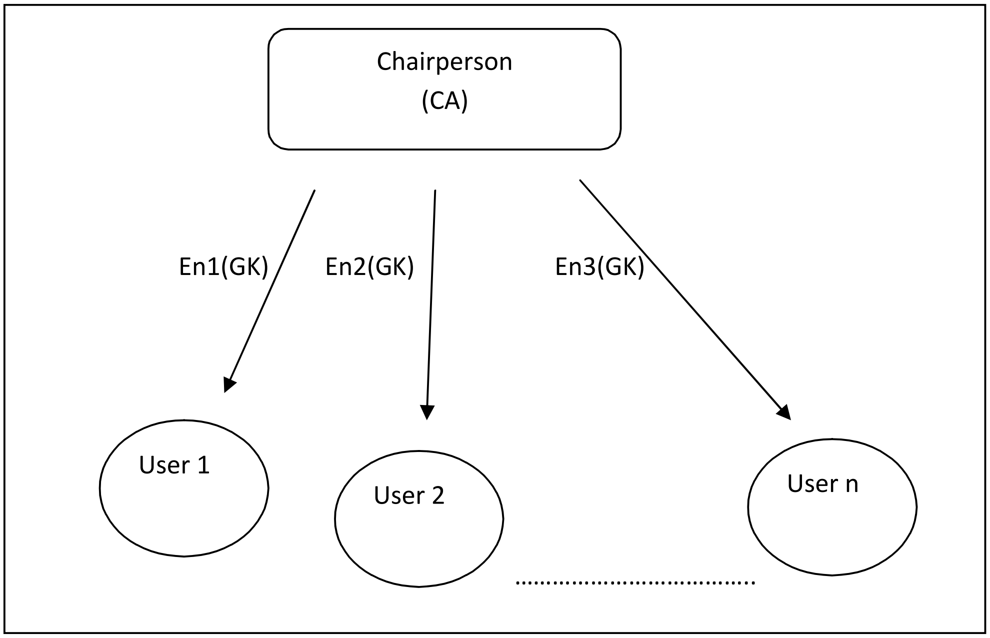


Figure 2. *The chairperson will send Group Key once he or she gets the entire shared key from all participants & compute GK*

It uses combination of asymmetric key and symmetric key crypto systems to provide provable secure and effective manageable systems. All parties can communicate with each other directly using Group Key, GK, without going through the chairperson. This protocol can avoid bottleneck and reduce network congestion.

<u>HASHING *TECHNIQUE :*</u>

One way to make the protocol more secure is by using hash function. Hash function produce fingerprint of a message or block of data. Usually, hash functions are used in message authentication. Use the hash function to enhance the group key computation.

MEMBER OPERATIONS :

ADDING A NEW MEMBER INTO GROUP :

New member :

STEP 1 : New member request to join the group.

STEP 2 : Gets the chairperson's public key and computes the shared key.

STEP 3 : Encrypts the shared key with the chairperson's public key and sends it to the chairperson.

STEP 4 : Receives the group key from the chairperson. Decrypt back using shared key.

Chairperson :

STEP 1 : Receives a shared key from new member, user $(n + 1)$.

STEP 2 : Update the shared keys list. Generate a new random number, *IV.*

STEP 3 : Compute new Combine Key, *CK.*

$$CK = K1 \oplus K2 \oplus K3 \ldots\ldots\ldots \oplus Kn \oplus K(n+1) \oplus IV$$

STEP 4 : Hashing the combine key value, *CK*, with hash function to get the group key. Group Key, *GK* = Hash *(CK).*

STEP 5 : When Group Key, *GK* is ready, the chairperson will encrypt the group key with shared key of each participant and send it to all participants in the group.

Current participant :

STEP 1 : Receives message from the chairperson informing that the group has a new member and the current group key is not valid anymore.

STEP 2 : Receives a new group key from the chairperson.

REMOVED A MEMBER FROM GROUP :

Leaving member :

STEP 1 : Leaving member broadcasts message indicating the intention of leaving the group.

STEP 2 : Leaves the group.

Chairperson :

STEP 1: Removes the public key of the member who is leaving or inactive after timeout.

STEP 2: Updates the list of participant public keys.

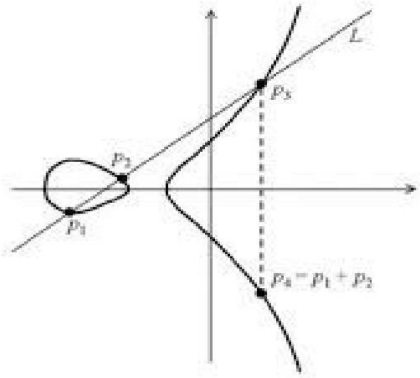
STEP 3: Computes a new group key, *GK.*

STEP 4: Distributes a new group key to each participant.

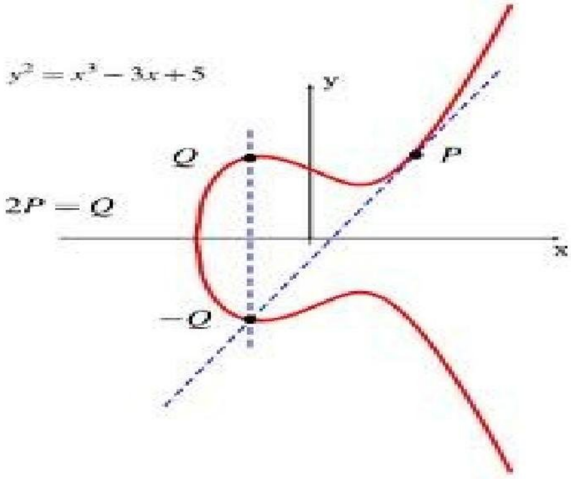
Current participant :

STEP 1: Receives a new group key from the chairperson.

3.2 Mathematical Backgrounds :

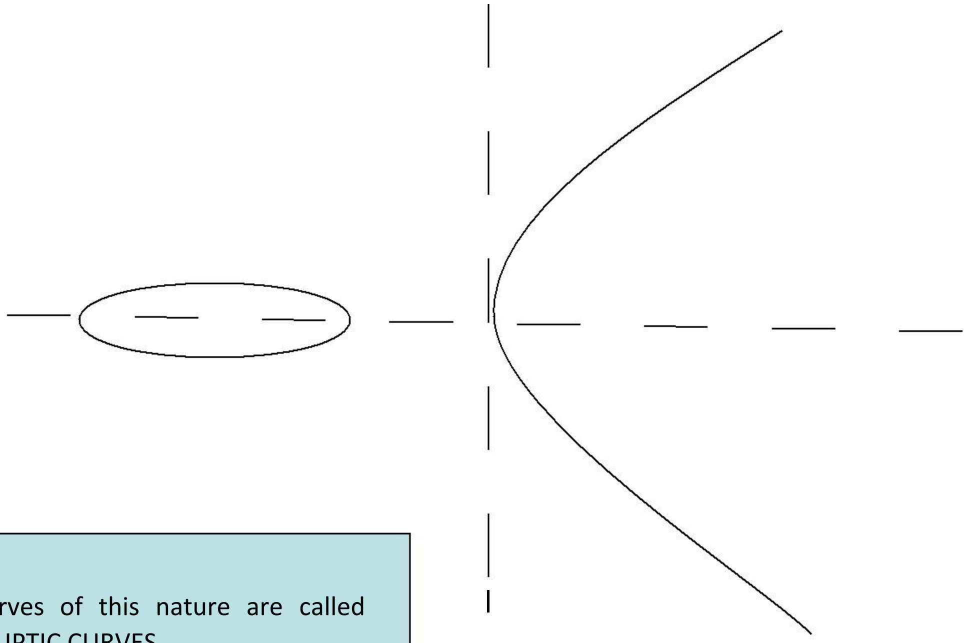


Case 1



Case 2

ELLIPTIC CURVES



Curves of this nature are called ELLIPTIC CURVES

Consider the puzzle given below:

What is the number of balls that may be piled as a square pyramid and also rearranged into a square array?

Solution: Let x be the height of the pyramid.

Thus, $1^2+2^2+. . . +x^2=(x(x+1)(2x+1))/6$

If y be the side length of the square then, $y^2=(x(x+1)(2x+1))/6$.

This equation represents a simple form of elliptic curve as shown above.

Definition of Elliptic curves

An elliptic curve over a field *K* is a nonsingular cubic curve in two variables, *f(x,y) =0* with a rational point (which may be a point at infinity).

The field *K* is usually taken to be the complex numbers, reals, rationals, algebraic extensions of rationals, p-adic numbers, or a finite field.

Elliptic curves groups for cryptography are examined with the underlying fields of F_p(where p>3 is a prime) and $F_2{}^m$ (a binary representation with 2^m elements).

General form of a EC

An *elliptic curve* is a plane curve defined by an equation of the form:

$$y^2=x^3+Ax+B \text{ ....} \qquad (1)$$

Points on the Elliptic Curve (EC)

Elliptic curve over a field L is composed of the points:

$E(L)=\{\infty\}\cup\{(x,y) \in L \times L \mid y^2+...=x^3+...\}$

The point infinity(∞) is added to the above list for a special reason.
Consider a line passing vertically through the curve.In such a case the line shall intersect the curve at only two points .However as the curve is cubic in x, there should be three points on the curve satisfying the line .We consider the point at infinity(usually denoted by O) to be that third point.
O is considered to lie both at the top and bottom of the curve.

PROPERTIES OF ELLIPTIC CURVES

One important property of elliptic curves that follows from the property of fields is that of Abelian Groups.Considering an elliptic curve E(Fp) with points P and Q we can say :

1. R=P+Q belongs to E(Fp) ..... (closure property)
2. P+Q=Q+P ..... (commutativity)
3. P+(Q+R)=(P+Q)+R ..... (associativity)
4. P+O=O+P=P ..... (existense of identity)
5. P+(-P)=O ..... (existense of inverses)

SUM OF TWO ELLIPTIC POINTS (P(x1,y1) and Q(x2,y2))

Let R(x 3,y3) denote the sum of P and Q. We
can have two cases:
1.P and Q are distinct
2.P=Q

If P and Q are distinct then any line passing through them will have the slope
m1=(y2-y1)/(x2-x1) .
However if P=Q then we cannot take the above form of m to find slope In this case slope will be given by the differentiation of eq(1) which gives,

$m2=(dy/dx)=(3x1^2+A)/2y1.$

Taking these values of m for respective cases we arrive at the following conclusion:
x3=λ -x1-x2
y3=λ(x3-x1)+y1.

where λ={m1 when P!=Q and m2 when
P=Q }

SINGULARITY

An elliptic curve $y^2=f(x)$ should be non singular(i,e it should not have singular points)
Singular Points:A point (x0,y0) is said to be singular if for $F(x,y)=y^2-f(x)$

$(\delta F/\delta x)(x0,y0)=(\delta F/\delta y)(x0,y0)=0 => 2y0=-f\,'(x0)=0$

$=>f(x0)=f'(x0)$
=>f has double roots. Consider $y^2=x^3+Ax+B$ then, $x^3+Ax+B = 3x^2+A = 0$
$=>x^2=-A/3$ Also,$x^4+Ax^2+Bx=0$

3.3 S/W & H/W requirements :

3.2.1 S/W : C program used for implementation.

3.2.2 H/W : Communication channel & required H/W support for practical implementation.

4. Solution Analysis:

Advantage :

- Bottleneck at Chairperson’s site is resolved.
- Secure communication among all members using GK without involving Chairperson.
- Elliptic curve is a better way for key exchange.
- ECC results in smaller key sizes , faster computations, reduction of storage space and processing power.
- A combination of asymmetric key and symmetric key crypto systems to provide provable secure and effective manageable systems.
- Design architecture promoted to Complete graph from Star graph.
- Highly secured as Discrete logarithm involved.
- Management of large number of members become easier.
- Because of same GK for all members intra group transparency is much more.
- Chairman has total authority over adding & removing group members.

Disadvantage :

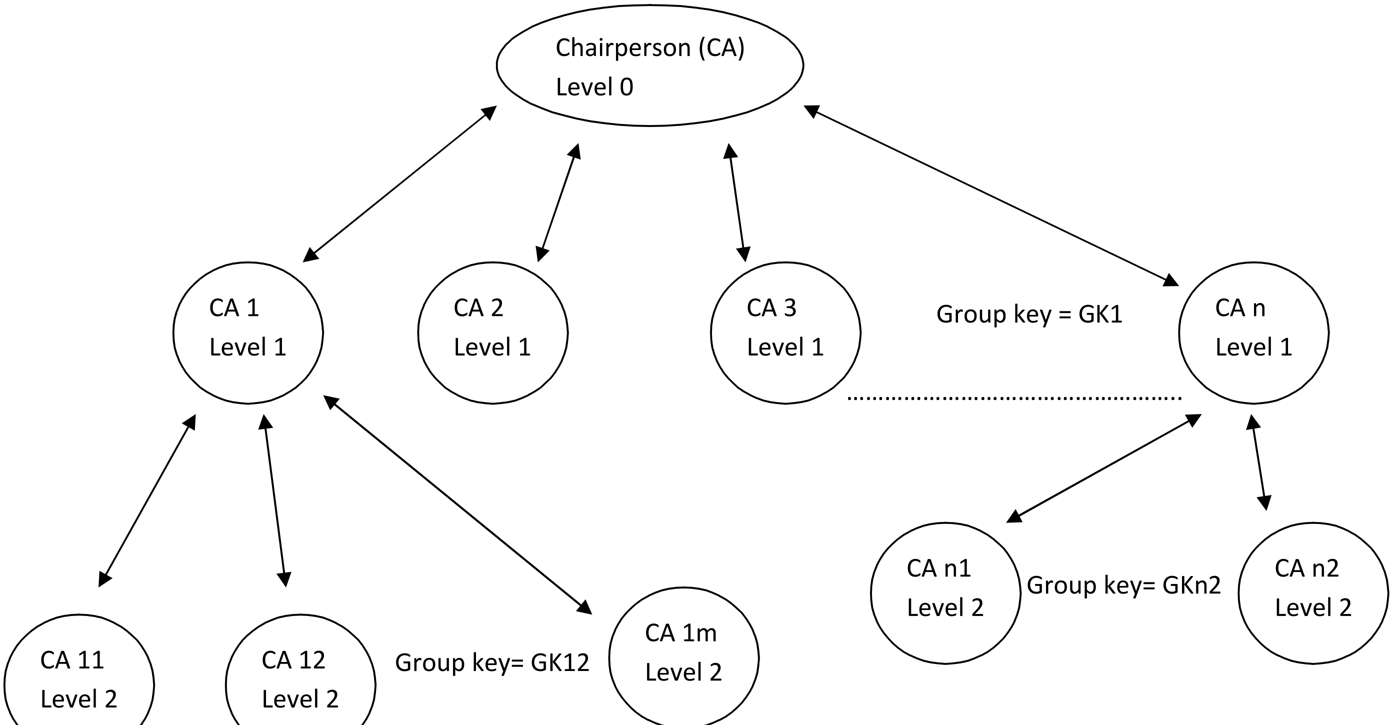
- Chairperson depended on all users for generating Group Key.
- One member can’t secretly communicate with any other member, all members can decrypt the communication.

- Chairperson needs to be trusted to all.
- Any change in total members involves recalculation of GK.

5. Application Areas
   - Military intelligence to communicate among agents.
   - S/W industry , communication among group of users of a particular s/w
   - Mobile phone technology .
   - AGAPE (Allocation and Group Aware Pervasive Environment) middleware for the support of group membership management in MANET scenarios. No predefined knowledge on group member names is necessary in AGAPE to enable communication.
   - The multicasting communications model can facilitate effective and collaborative communication among groups. Flooding and tree-based routing represent two ends of the multicasting spectrum
   - Mobile ad hoc network (manet) comprises a set of wireless devices that can move around freely and cooperate in relaying packets on behalf of one another.
   - The communication among clients in client-server architecture.

6. Future Enhancements :

   This method can be enhanced to make an secured hierarchal communication system where each member will act as a chairperson for his/her subordinates by issuing a GK for them that involves GK for his/her level of communication during its calculation.



Here, $GK12 = K11 \oplus K12 \oplus K13 \ldots\ldots \oplus K1m \oplus GK1$

& $GKn2 = Kn1 \oplus Kn2 \oplus GK1$

7. Conclusion

Proposed a new protocol for secure group communication based on public key infrastructure. The proposed protocol addresses the bottleneck problem faced by the existing protocol. The proposed protocol uses chairperson to form a group communication only at the beginning of the protocol. Once a group has been established, secure communication between each participant can be done directly without going through the chairperson. This will help reduce the traffic compared to the previous approach where all traffic needs to *go* through the chairperson.

8. References

[1 J *William M Farmer, Joshua D. Guttman and Vipin Swamp, Securiry for Mobile Agents: Issues and Requirements. In Proceedings of the Igh National Information System Securiry Conference, pp. 591 - 597, Baltimore, 1998.*

[2] *Wayne Jansen, A Privelege Management Scheme for Mobile Agent Systems, First International Workshop on Securitv of Mobile Multiagent*

[3] Hirose, s. *andlkeda, K.. A conference key distribution system for the star configuration based on the discrete logarithm problem. Information Processing Letters, vol. 62, no. 4, 1997.05, pp. 189 - 192.*

[4] *D@e, W., and Hellman. M. "New Directions in Ctyptography." IEEE Transactions on Information Theory, Nov. 1976.*

[5] Secure Groups Communication For Mobile Agents by,
Muhammad Aiman Mazlan, Azman Samsudin and Rahmat Budiarto *School of Computer Science, University Science Malaysia I800 Penang, Malaysia Email: (aiman, azman, rahmat) @ cs.usm.my*

[6] Implementation of Text based Cryptosystem using Elliptic Curve Cryptography by, S. Maria Celestin Vigila1, K. Muneeswaran' *1 Asst. pro! , Department ofInformation Technology, Noorul Islam College ofEngg., Kumaracoil 2 Prof., Department ofComputer Science and Engg., MEPCO Schlenk Engg. College, Sivakasi.* celesleon@yahoo.com,kmuni@mepcoeng.ac.in

---

A Report By,

Sujay Kumar Mandal	*(M120361CA)*
Rakesh Patni	*(M120364CA)*
Vishwash Sharma	*(M120372CA)*
Suresh Patidar	*(M120357CA)*
Shashak Mishra	*(M120363CA)*
Puit Singh	*(M120527CA)*
Manu G Krishnan	*(M120353CA)*