2017

Object Oriented Modeling of secured E-learning system

Soumendu Banerjee,

Dr. Sunil Karforma

Publishing Partner: IJSRP Inc.

ISSN 2250-3153

9 772250 315302

Publication Partner:
International Journal of Scientific and Research Publications (ISSN: 2250-3153)

Object Oriented Modeling of secured E-learning system

Soumendu Banerjee[1]

Dr. Sunil Karforma[2]

[1] Research scholar, Dept. Computer Science, The University of Burdwan

[2] Associate Professor, Dept. of Computer Science, The University of Burdwan

Preface

In an e-learning environment, data security and secrecy is very essential, especially when data is transferred between the three main participants of e-learning like learners or students, teachers and developers or administrators. This type of data is related to information, admission, and registration, admit card, study material, question papers, answer scripts, mark sheets etc. In this competitive world, if data security cannot be provided appropriately, then hacker can easily reach to the data during transmission and may change or damage data before its arrival to the final destination, and make a bad impression for any particular e-learning institute. Architecture of secure e-learning system will be provided in our discussion. The four main security issues which should be considered to an e-learning organization are privacy, secrecy, non-repudiation and authentication (PINA). To achieve non-repudiation and authentication, we generally use symmetric key algorithms like Data Encryption Standard (DES), Triple DES, AES and public key algorithms like Digital Signature Algorithm, RSA digital signature, ElGamal digital signature, GOST digital signature. For security purpose, we can also apply Digital Watermarking and Digital Right Management (DRM) techniques. Here we will discuss about the object oriented implementation of secret key algorithms like DES, Triple DES and the public key cryptographic algorithms like DSA, RSA signature, ElGamal Signature and GOST digital signature.

Authors

Soumendu Banerjee

He has completed B.Sc. (H) in mathematics and MCA from the University of Burdwan. Now, he is acting as the Assistant Professor of St. Xavier's college, Burdwan. He is pursuing PhD in the Department of Computer Science, The University of Burdwan. He has 10 research publications in several national and international journals and conferences including one accepted book chapter.

Dr. Sunil Karforma

He has completed B.E and M.E in Computer Sc. And Engineering from Jadavpur University and completed his PhD in Computer Science from The university of Burdwan. He is currently serving as Associate Professor and Head of the Department of the Computer Science in The University of Burdwan. His research area includes Cryptography and Bio-informatics. He has published more than 100 research papers in many reputed national and international journal and conferences including 2 books and 2 book chapters in reputed publishing agencies. He has successfully supervised 4 PhD dissertations.

Contents:

1.E-learning:

1.1What is E-learning?

In general, e-learning refers to learning via Internet. Since, nowadays, Internet is available in most of the places, so, E-learning does not have any barrier of place and no need to move elsewhere. Learners, teachers and developers or administrators are the three main components of any e-learning system. In e-learning, all of the procedures regarding learning are done via Internet. The most accepted definition of e-learning[1] is according to the E-learners Glossary, "E-learning covers a wide set of applications and processes, such as Web-based learning, computer-based learning, virtual classrooms and digital collaboration. It includes the delivery of content via Internet, intranet/extranet (LAN/WAN), audio- and videotape, satellite broadcast, interactive TV and CD-ROM."

E-learning now-a-days is becoming a popular form of application of information and communication technology (ICT). In E-learning, all the procedures like searching of courses, checking course fee, paying course fee, distributing admit cards, study material, uploading documents, providing registration certificates and distribution of mark-sheets- all are done through Internet. With the progress of internet technology, the growing rate of e-learning also becomes high. According to a recent study on e-learning in a global level online program, India stand in the 2nd place in the number of enrollments in online courses, just behind the United States[2]. E-learning can be used in the field of a full learning course, any mandatory course in case of any business organizations etc. Sometimes learners face difficulties in reaching the learning institutes and adjust the timing span given by the institutions that means those who stay far away from the institution may not effort to come and stay and sometimes the working professionals, who are engaged in any kind of jobs, seem difficult to adjust the prescheduled timing assigned by the institutions[3]. In those cases, the e-learning is very helpful to give them the opportunity for studying further to learn more and more. Some of the advantages of e-learning are[4] as follows:

- **Cost effective**: Since in E-learning, it is possible to learn by staying far away from the associated institutions, which reduces the travelling cost and in most of the cases, there is no need of nay printed materials. So, e-learning is cost-effective.
- **Time saving:** Since learners can continue study without attending the regular classes, so they have no need to travel to corresponding learning institutions and which is most helpful for the working professionals, they can study other than their scheduled working hours, which saves their time.
- **Learning anytime and anywhere:** E-learning is especially so much helpful for the working professionals, those are already engaged in a job, without moving anywhere and without wasting time other than the scheduled job hour, can complete the necessary courses.
- **Discrete:** Sometimes, due to age, or any personal reason, some people do not feel comfort to study sitting in a group. E-learning seems to be helpful for them.

1.2 Architecture of e-learning:

The total e-learning system mainly has two parts: client and server. Generally students play the role of client and sometimes the teacher and/or developer also. Student, teacher and developer are connected via internet. Students send request for study material or other kind of services from the developer and the information generally stored at the database which is handled by the developer or sometimes by the teachers. The network administrator controls the access of data through firewall, which is not fully secure and to make the system better, we use various kinds of cryptographic algorithms[5].

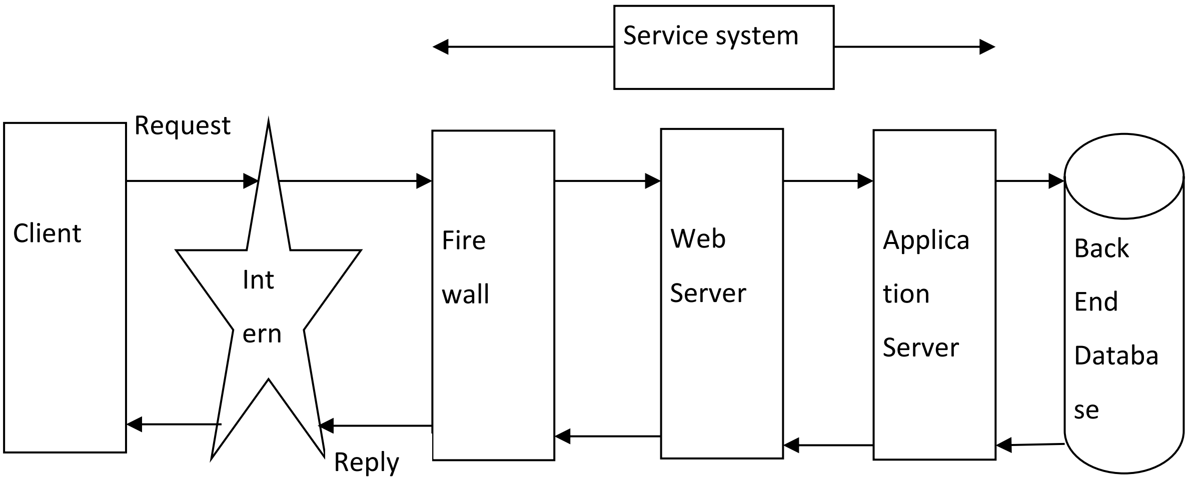


Fig 1: Architecture of a secured e-learning system

Web server gets request from client and give reply to client. Application server and backend database server may be one system or separate system. Database server may contain different database files related to e-learning resources. Multimedia database files can also be saved in database server. Here the application of firewall makes the architecture more prominent. In general firewall has two network interfaces[6]: one for internal side and the other for the external side, whose main function is to control the traffic from traversing one side to another and it also provide protection against different kind of attacks, more commonly Denial Of Service (DOS) attack.

1.3 Security services and techniques:

E-learning is Information and Communication Technology (ICT) based education system. The total e-learning system is fully based on Internet. Again, Internet being a public network, security plays a vital role in e-learning. There are mainly four security issues, which we have to consider in case of transmission of documents in an e-learning system. They are Privacy, Integrity, Non-repudiation and Availability (PINA).Privacy and integrity, in generally, means only the authorized persons can change or modify the data. These security issues play an important role in an e-learning system. For example, suppose, the teacher is sending study material prepared by him/her, to the students as per their requirements and during the transmission if hacker can reach the documents and then modifies or destroys the documents. In this situation the privacy of the documents prepared by the teacher and integrity of the documents is in danger, which should be provided by the administrator of the e-learning institutions. Non-repudiation means that the sender can't deny after sending the documents. For example, suppose, during the transmission of mark sheet, hacker may be able to reach the document and change the data of the mark sheet. In these kinds of cases, if the learner claims for the resending of the same as it is modified during transmission, then the institution can't claim about the tampering of their previous documents. Availability means to avail the right things at right time. For example of availability, suppose an online exam is going on and internet connection is too much slow, then it will make a great trouble and exam may have to be postponed.

1.4: Benefits of Object Oriented approach in any system

The main benefits of the object oriented approach of any system, is the reduction of maintenance cost, improvement of reliability and flexibility and code reusability [7].

- **Reduction of maintenance cost**: Since most of the processes within the system are encapsulated in any object oriented approach of any system, the maintenance cost will be obviously reduced.
- **Real-world implementation**: Since the main aim of any object oriented design is to represent a system based on the real world features by using classes and objects along with their behaviors.
- **Reliability and Flexibility**: One of the main difference between the object oriented system and traditional system is reliability and flexibility because objects can be called dynamically and easily accessed. So, when we implement any system using object oriented approach, these two benefits are automatically achieved.
- **Code reusability**: One of the main advantages of the object oriented approach is inheritance, which gives the programmer freedom to reuse of codes in while designing any system using object oriented approach.

In modern software engineering, object oriented analysis (OOA) and object oriented design (OOD) mainly use the object oriented modeling (OOM) in modeling applications, system or business domains by using object oriented paradigm throughout the entire development life cycle[8]. The benefits of OOM are also includes:

i) Efficient and effective communication and

ii) Useful and stable abstraction.

Unified Modeling Language (UML) and SysML are the two most popular languages used to represent the object oriented modeling of any system. Here, we use the UML diagrams to represent the modeling of an e-learning system based on the secure transmission using some cryptographic algorithm based digital signatures and digital certificate. Along with the UML diagrams, we also use the Data Flow Diagram (DFD) for better understandability. A DFD is a graphical technique which is easy to recognize and understand for the technical and non-technical audience as well as it can provide a detailed representation of system components.

There are mainly nine types of UML diagrams, we use in software engineering[9], among them, we use the following diagrams to represent the object oriented modeling of the secret and public key cryptographies and digital certificate. Here we give brief information about our used UML diagrams:

- **Class diagram**: It is one of the most commonly used diagrams in UML and it represents the object oriented view of any system.
- **Use case diagram**: Use case diagram is another way to show the requirements of a system including internal and external influences. It is also a part of the Unified Modeling Language (UML). These requirements are generally related with the design requirements. So when a system is analyzed to gather its functionalities use cases are prepared and actors are identified[10].
- **Sequence diagram:** A sequence diagram[11] shows the interaction among objects as a two dimensional chart. The chart is read from top to bottom.
- **Activity diagram:** Activity Diagrams are represented graphically like a flowchart, to show the workflows of stepwise activities and actions with support for choice, iteration and concurrency[12].
- **Collaboration diagram:** Collaboration diagram is one kind of Unified Modeling Language (UML) interaction diagram. This diagram is used to emphasize on the structural organization of the objects that sends and receive messages[13].

To represent the object oriented modeling of the private and public key cryptographies and also for digital certificate, we use the above mentioned diagrams in this article to obtain the facilities of object oriented implementation in an e-learning system.

2. OOM of secure e-learning system using Secret Key Cryptography

In cryptographic system, there are mainly two kinds of cryptographies and one of them is secret key or symmetric key cryptography[14]. In secret key cryptography we use only one key to encrypt and decrypt the data. So the key should be kept very secret from the outside world. The recent trend of software development is to eliminate the redundant code and make reuse of codes and use data hiding[15]. Using data hiding in the e-learning system, we can hide the secret key from the outer world. There are so many models we can use in object oriented implementation like, class diagram, sequence diagram, use case diagram, collaboration diagram, activity diagram, etc. So, implementation of object oriented modeling is very essential for any e-learning system nowadays. It is not possible to draw all kinds of diagrams of each algorithm in a single chapter, so, here we just take any one or two of the models and implement them regarding the corresponding algorithms and give a brief description, which will help the reader to understand.

2.1 Modeling of DES algorithm:

In this section, we will discuss on some of the object oriented modeling along with data flow diagram (DFD), based on some diagrams such as class diagrams, use case diagrams and sequence diagrams regarding DES algorithms considering only the case where the teacher is sending the study material to the learner[16,17].

2.1.1 Data Flow Diagram (DFD):

The data flow diagram is a graphical representation of a system, which contains the input data to the system, processes which has been carried out on these data and also the output data generated by the system. Here we design two levels of DFD for the transmission of study material from the administrator to students based on the RSA algorithm. The level1 DFD is shown in Fig: 2, consists the study material transmission from teacher to learner. Level2 DFD consists of two parts, which has been shown in Fig: 3 and Fig: 4.

The first part of the level2 DFD, shown in fig.3, discusses about the study material encryption process and the second part of the level2 DFD, shown in the fig.4, shows the decryption[18] process of the study material. In the level2 DFD the Expansion and XOR function has been executed 16 times, which is difficult to present through the picture. This iteration has been done for 16 times in case of both the encryption and decryption (one iteration is shown here).

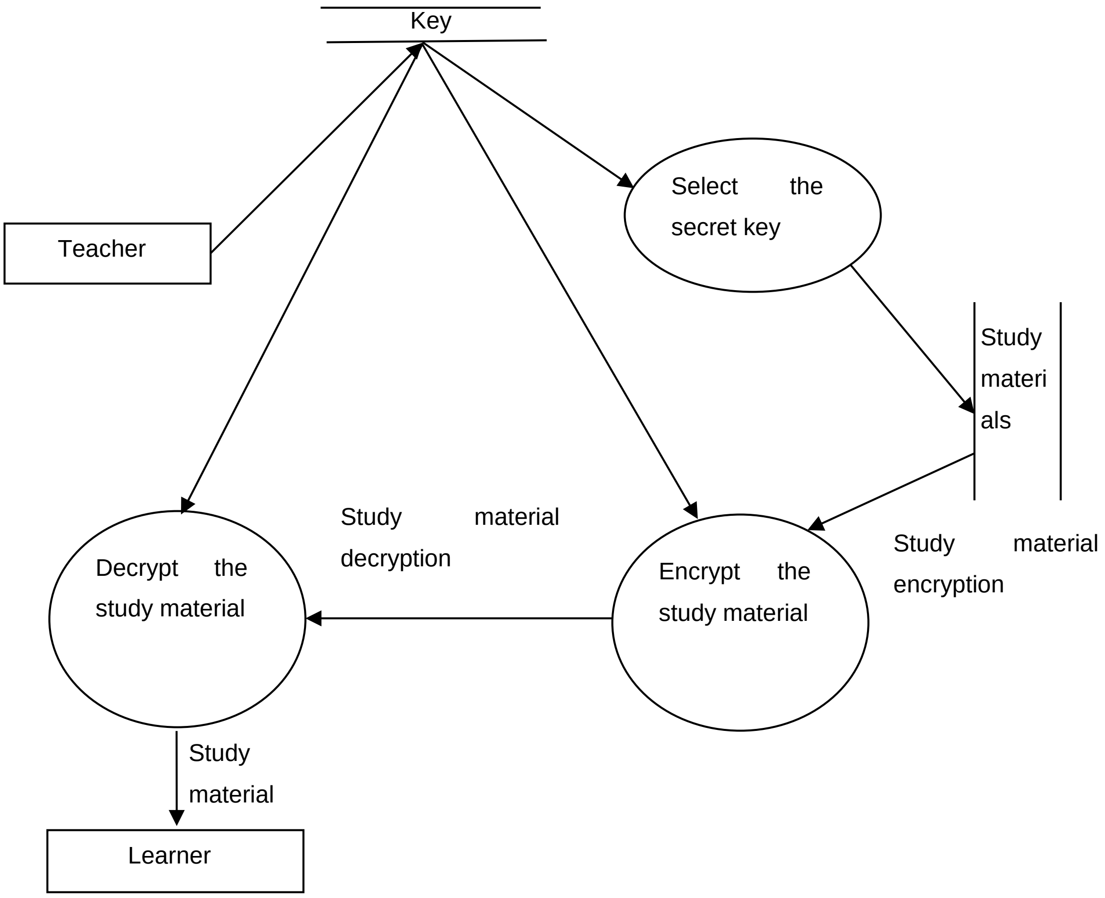

Key
Teacher
Select the secret key
Study materials
Study material encryption
Encrypt the study material
Study material decryption
Decrypt the study material
Study material
Learner

Fig: 2: Level1 DFDfor study material transmission

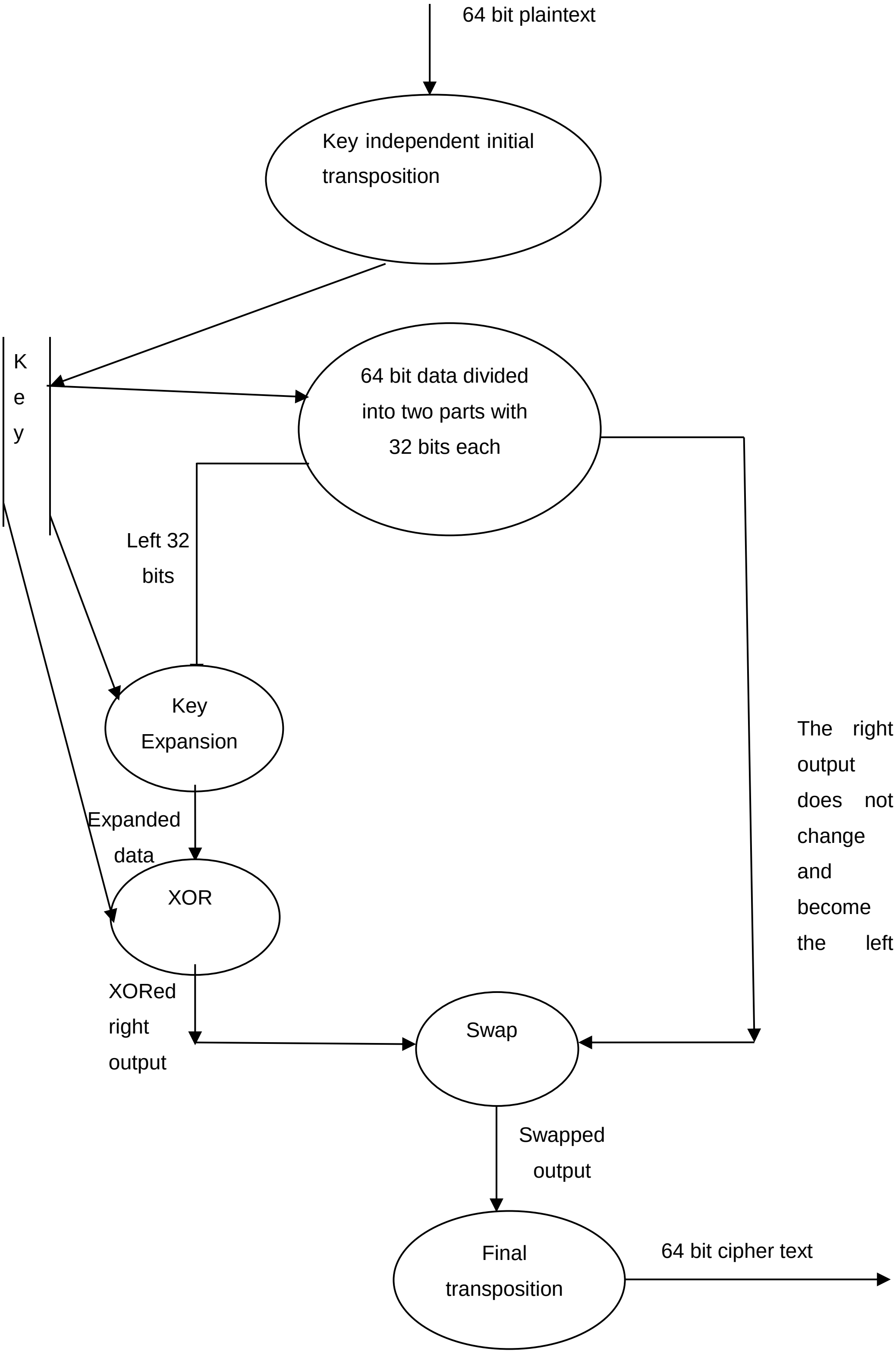

64 bit plaintext
Key independent initial transposition
K
e
y
64 bit data divided into two parts with 32 bits each
Left 32 bits
Key Expansion
The right output does not change and become the left
Expanded data
XOR
XORed right output
Swap
Swapped output
Final transposition
64 bit cipher text

Fig: 3: Level2 DFD for study material encryption

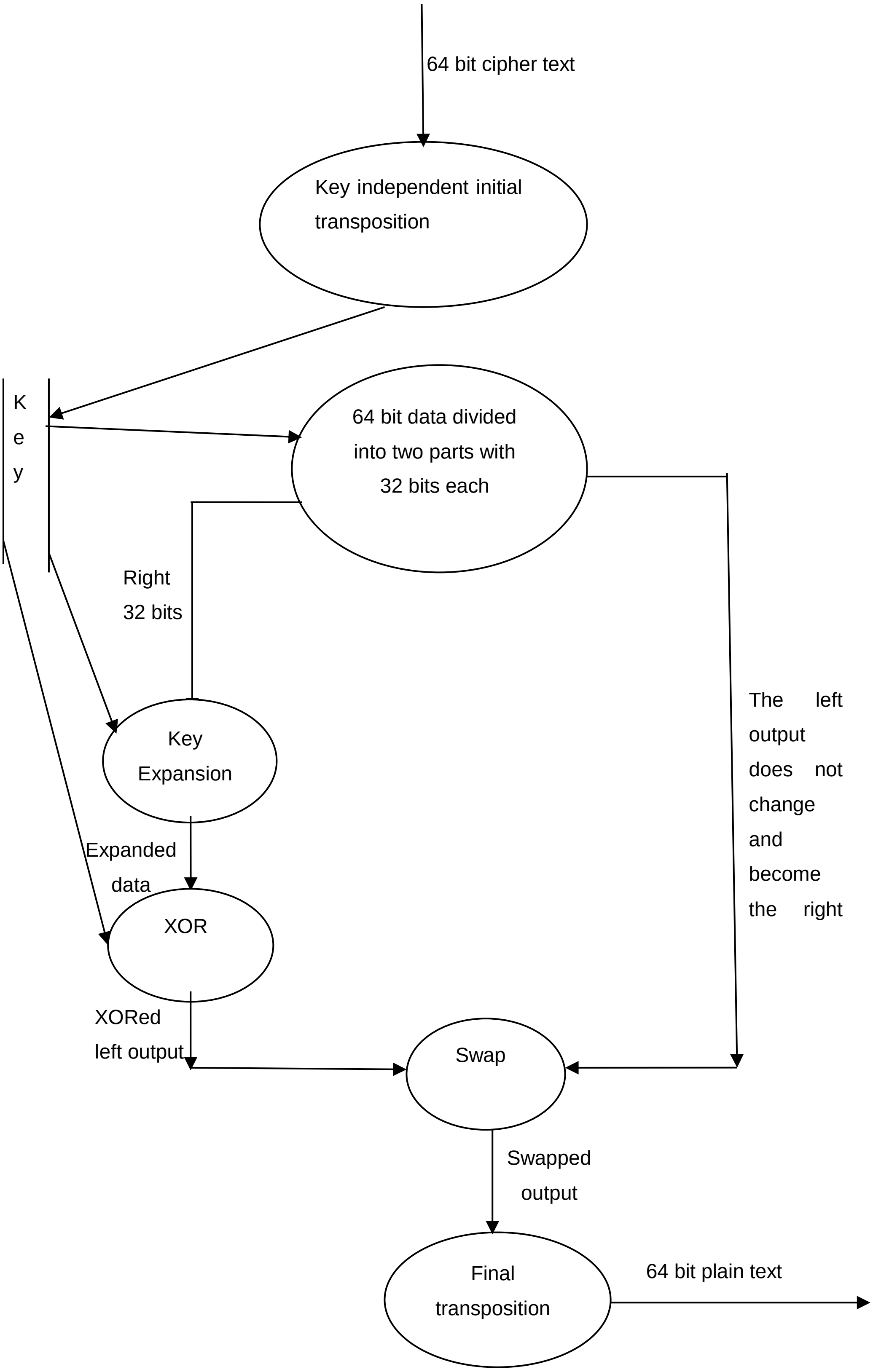
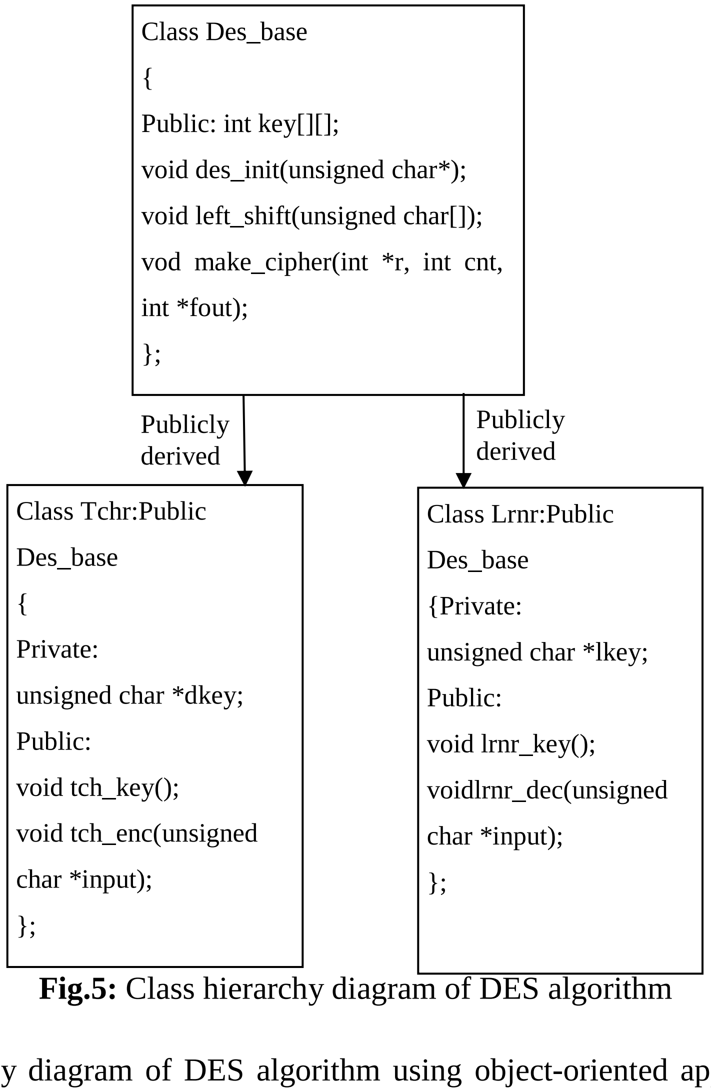

64 bit cipher text
Key independent initial transposition
K e y
64 bit data divided into two parts with 32 bits each
Right 32 bits
The left output does not change and become the right
Key Expansion
Expanded data
XOR
XORed left output
Swap
Swapped output
Final transposition
64 bit plain text

Fig: 4: Level2 DFD for study material decryption

2.1.2Class hierarchy diagram of DES algorithm:

The figure of the class hierarchy diagram, shown in the figure below (fig.5), demonstrates the organization of classes showing how the teacher can securely send the study material to the learners using a combination of DES algorithm in object oriented approach.



```
Class Des_base
{
Public: int key[][];
void des_init(unsigned char*);
void left_shift(unsigned char[]);
vod make_cipher(int *r, int cnt,
int *fout);
};
```

```
Class Tchr:Public
Des_base
{
Private:
unsigned char *dkey;
Public:
void tch_key();
void tch_enc(unsigned
char *input);
};
```

```
Class Lrnr:Public
Des_base
{Private:
unsigned char *lkey;
Public:
void lrnr_key();
voidlrnr_dec(unsigned
char *input);
};
```

Fig.5: Class hierarchy diagram of DES algorithm

The class hierarchy diagram of DES algorithm using object-oriented approach is shown in Fig:5 along with the associated data members (data parts) and member functions (function part).

Both the Tchr and Lrnr classes are publicly inherited from the Des_base class and thereby all the public member functions of Des_base class such as des_init(unsigned char *), left_shift(unsigned char[]) and make_cipher(int *r, int cnt, int *fout) will be added and reused in Tchr and Lrnr classes in addition to those special functions which are explicitly defined with in the class Tchr and the class Lrnr. The use of functions tch_key() andtch_enc(unsigned char *input) are defined in the Developer.

Class Tchr uses a tch_key() function of its own to get its secret key and class Lrnr use a lrnr_key() function of its own to get its secret key.

void tch_enc(unsigned char *input):

This function is used to encrypt the study material sent by the object of the clas tchr to an object of the Lrnr class.

void lrnr_dec(unsigned char *input):

An object of Lrnr class will use this function to decrypt the received study material using the same secret key which was used by the object of Tchr class for encryption of the study material. Tchr cannot decrypt the original study material if other secret key is used during decryption.

2.1.3 Use case Model:

Here we use the two main components of any e-learning system: Teacher and Learner. Here we use two use case models. In fig.6.1, we show the use case of encryption of study material, which will be done at teacher’s end and fig.6.2contains the use case of study material decryption, which will be done at learner’s end. In fig.6.1, teacher selects the secret key, which includes the initialization of the key and also requires some left shifts of the 28 bit data. Also the encryption of the study material is done at the teacher’s end which includes the make cipher process, which is used to process 64 bit data block. In the other use case, shown in fig.6.2, learner gets the secret key from the teacher, which includes initialization of the key and required number of left shifts of the 28 bit data. Also, the decryption of the study material is done at the learner’s end which includes the process make cipher.

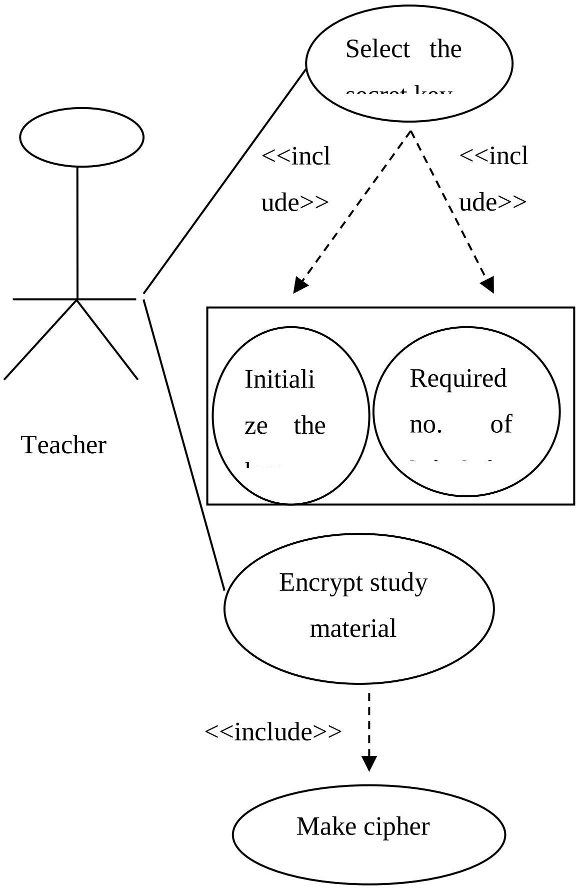


Fig. 6.1: Use case diagram for study material encryption

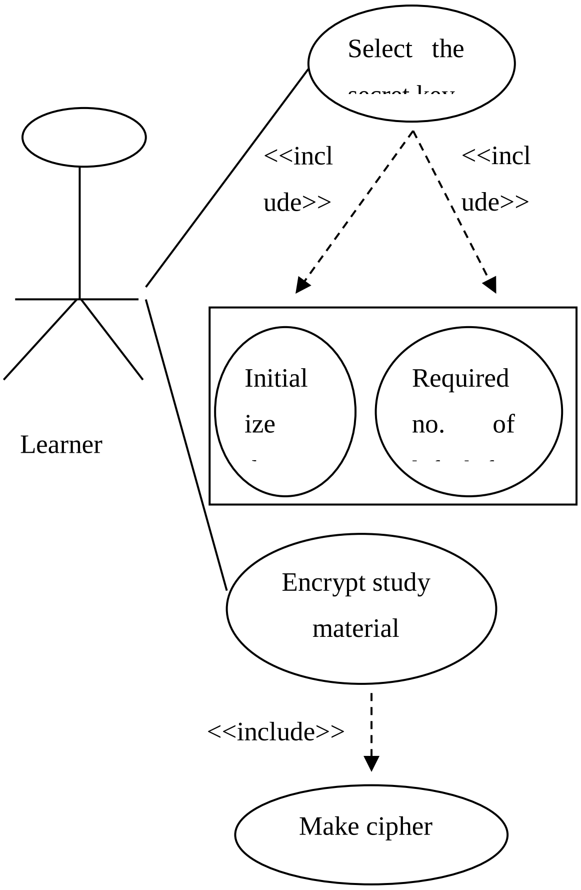


Fig.6.2: Use case diagram for study material decryption

2.1.4Sequence Diagram:

The sequence diagram of study material encryption has shown in the Fig: 7. Here we only sketch the diagram for study material encryption. For this purpose, we have taken two classes Tchr an Lrnr. The interaction between teacher and learner regarding study material is shown here. In this sequence diagram shown below, we cannot represent the 16 iteration steps of the expansion and XOR. In this diagram, we have shown only single iteration. In this diagram, student will login to the system by giving valid user-id and password. If the id or password does not match, then an error message will be displayed. After login by placing the correct user id and password, provided by the system administrator, learner will request for study material. The teacher will encrypt this study material using the steps of DES algorithm and send the encrypted study material and the secret key to the learner.

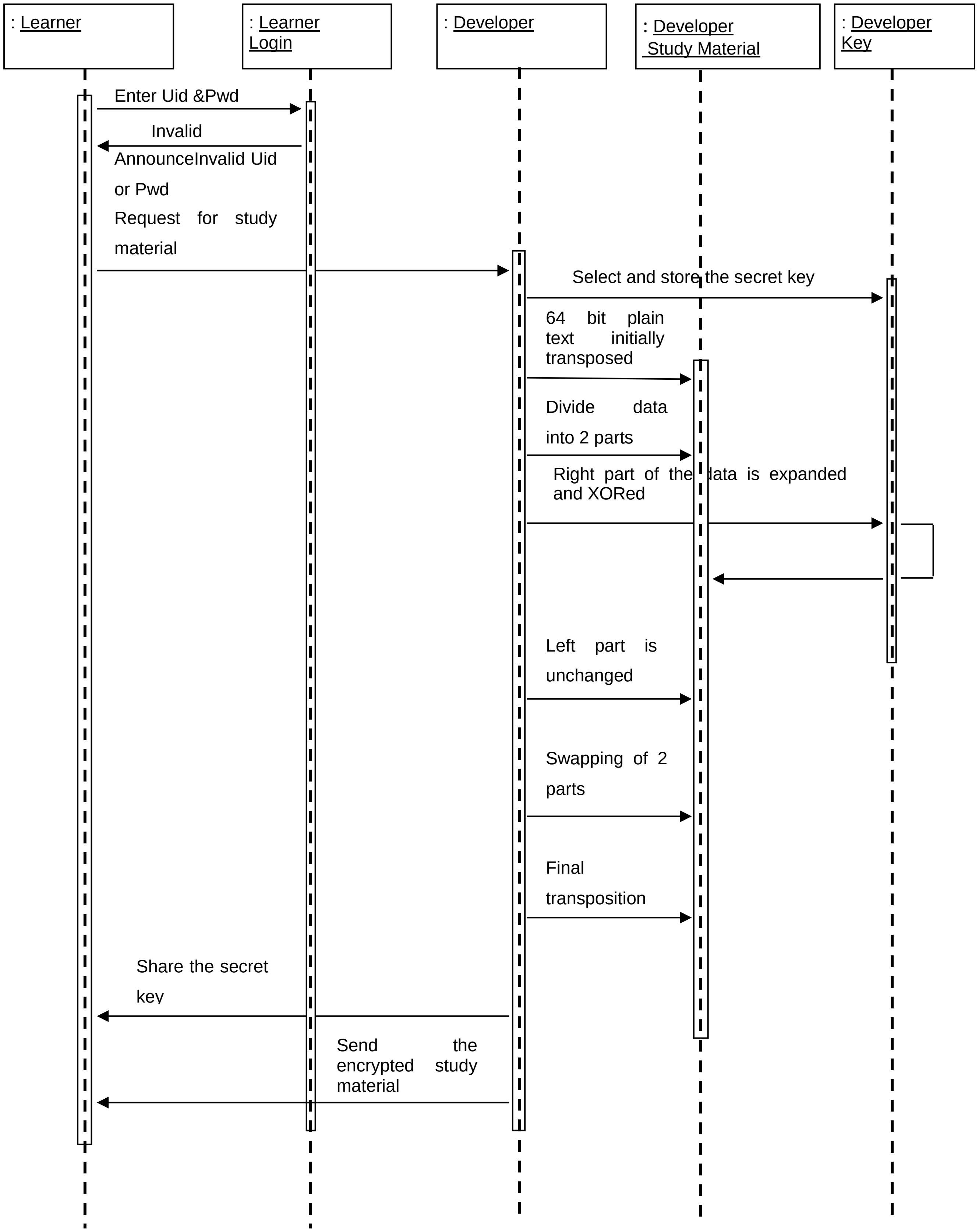

: Learner
: Learner Login
: Developer
: Developer Study Material
: Developer Key
Enter Uid &Pwd
Invalid AnnounceInvalid Uid or Pwd
Request for study material
Select and store the secret key
64 bit plain text initially transposed
Divide data into 2 parts
Right part of the data is expanded and XORed
Left part is unchanged
Swapping of 2 parts
Final transposition
Share the secret key
Send the encrypted study material

Fig: 8: Sequence diagram for study material encryption

- In the above section, we have shown the object oriented modeling of the DES algorithm based on the transmission of the study material from the teacher to the learner in an e-learning environment. To make understand of the modeling, we have used the four UML diagrams: use case diagram, data flow diagram, class hierarchy diagram and sequence diagram. The other UML diagrams like state chart diagram, timing diagram etc. can also be implemented.

2.2 OOM of triple DES:

Triple DES or 3DES is an up gradation of the DES algorithm. In triple DES, the steps of DES algorithm are applied for 3 times to each block of data. Here, generally 3 keys are used to encrypt and 3 keys to decrypt. At first teacher will encrypt the study material using the key k1, then decrypt it using key k2 and again encrypt the material using key k3. Similarly, learner has to decrypt the study material after receiving from the teacher in encrypted form along with the three keys in reverse way. First, learner will decrypt the study material using k3, and then encrypt the material using k2 and again decrypt using the key k1[19,20]. We can explain it simply as:

Cipher text=$E_{k3}(D_{k2}(E_{k1}(\text{plaintext})))$

Plain text=$D_{k1}(E_{k2}(D_{k3}(\text{cipher text})))$

2.3 Comparison between Symmetric key algorithms:

Here we will discuss on the three main symmetric key algorithms: DES, triple DES and AES(Advance Encryption Standard) based on 4 issues[21,22,23]:

Issues	DES	3DES	AES
Developed	1977	1979	1997
Key length	56 bits	168 bits (3keys are different) 112 bits (2keys are same) 56 bits (3keys are same)	128, 192 or 256
Data block size	128 bits	64 bits	64 bits
Efficiency	Proven Inadequate	Better than DES	Secure

Table 2.1: Comparison between 3 secret key algorithms

3. OOM of secure e-learning system using Public Key Cryptography:

Another way to secure data transmission among the participants of e-learning system is to apply public key cryptography. Here generally two types of keys are used: one key is publicly known and the other is kept secret. Digital signatures are one kind of public key cryptography and some of the important signature algorithms are Digital Signature Algorithm(DSA), RSA digital signature, ElGamal digital signature etc. Digital Signature algorithms are also used to implement authenticity regarding sending any material through online, which issue is known as non-repudiation. If we can achieve non-repudiation, then the sender can never deny about sending of the mail.

This unit contains some signature algorithms wrapped with some object oriented model for implementation of authenticity of the study material to utilize the benefits of objects oriented analysis and design.

3.1 OOM of DSA:

Here we will discuss only on the activity diagram (fig.9) regarding registration of a student in an e-learning system[24] to get the study material. Here, learner will enter into the system by putting his/her id & password. To check the authenticity of the learner, he/she will generate digital signature using DSA and developer must verify it, after that learner can finally upload the personal information details in the registration form.

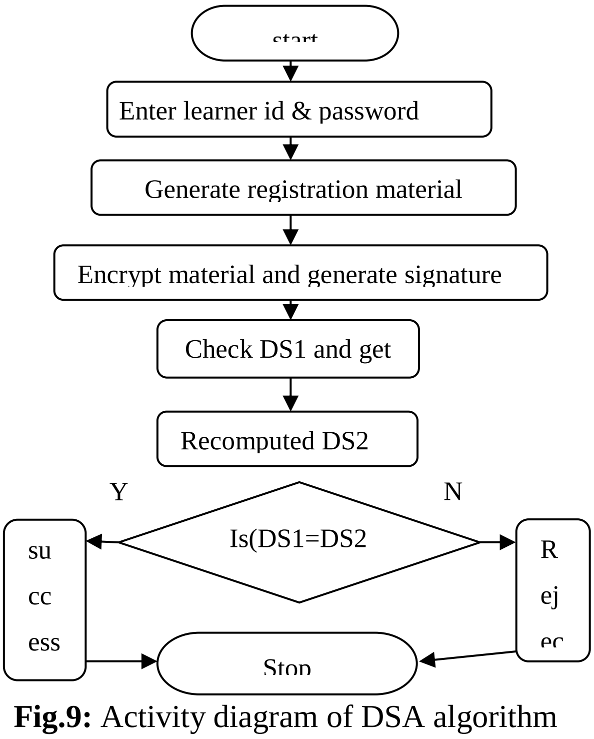
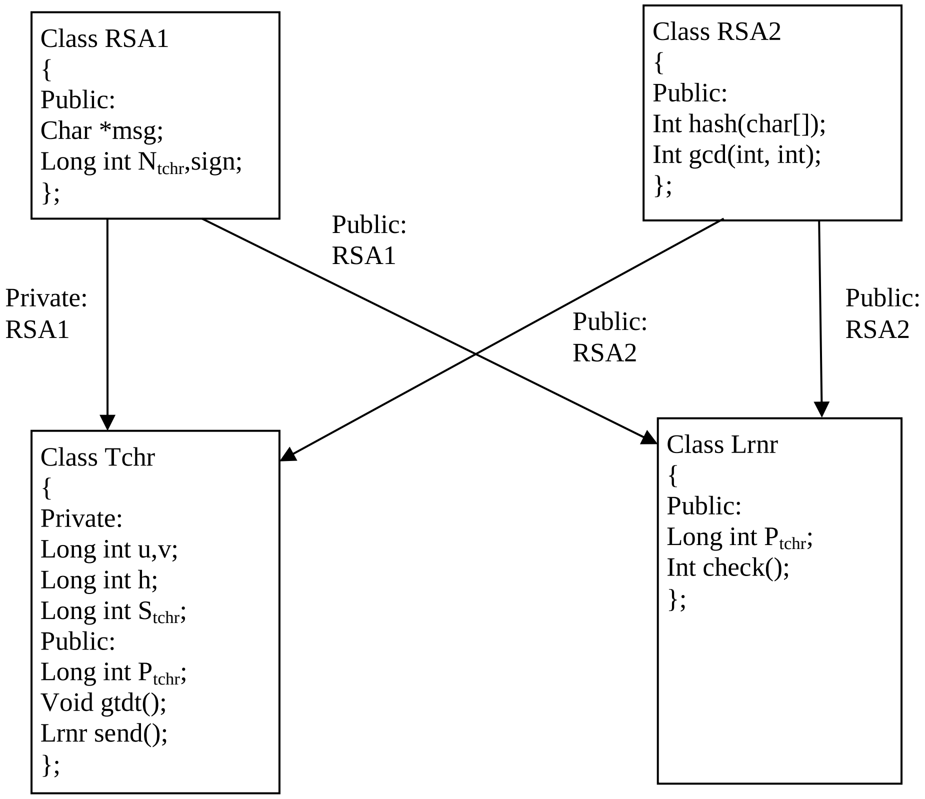

start
Enter learner id & password
Generate registration material
Encrypt material and generate signature
Check DS1 and get
Recomputed DS2
Y
N
Is(DS1=DS2
su
cc
ess
R
ej
ec
Stop

Fig.9: Activity diagram of DSA algorithm

3.2 Object Oriented Modeling of RSA digital signature:

RSA digital signature is one of the most important digital signatures. In this context, we are going to implement object oriented analysis and design (class diagram) of RSA digital signature algorithm[25] to secure the transmission of study material from teacher to learner in an e-learning system.

3.2.1 Class Diagram of RSA digital signature:



```
Class RSA1
{
Public:
Char *msg;
Long int Ntchr,sign;
};
```

```
Class RSA2
{
Public:
Int hash(char[]);
Int gcd(int, int);
};
```

```
Class Tchr
{
Private:
Long int u,v;
Long int h;
Long int Stchr;
Public:
Long int Ptchr;
Void gtdt();
Lrnr send();
};
```

```
Class Lrnr
{
Public:
Long int Ptchr;
Int check();
};
```

Fig: 9: Class diagram of RSA digital signature

The class diagram is shown in fig.9 below. Here four classes are used: RSA1, RSA2, Tchr and Lrnr. RSA1 and RSA2 are used as base classes. First, we are giving a brief description on the data members and member functions of the class hierarchy diagram:

Class RSA1: Char *msg;//Here msg is the study material to be sent by an object of the class Tchr

Long int N_{tchr}; //it is the product of two prime numbers

Long int sign;// it represents the digital signature

Class RSA2: Int hash(char[]); //this is used to create hash value

Int gcd(); //used to find the gcd of two numbers

Class Tchr: Long int u,v; //u and v are two prime numbers

Long int h; //h is used to store hash value

Long int S_{tchr}; //it stores the secret key of class Tchr

Long int P_{tchr}; //it stores the public key of class Tchr

Void gtdt(); //it is used to receive study material and signature from Tchr

Lrnr(send);// it is used to send the study material along with the signature to the learner from the teacher

Class Lrnr: long int P_{tchr}; //it also used to store public key of class Tchr

Int check(); //it is used to verify digital signature

3.2.2: Use Case Model

In this use case model, we take two types of objects teacher and learner. Here teacher is generating the study material along with the signature and sends these to the learners. After receiving these, learners will compute the hash values and verifies if the material original or not. To implement these, we use two use case models, one for the teacher and the other for the learner.

The first use case model is shown in the fig. 10. Through this diagram, we discuss about the signature generation, which is done by the teacher. Here, teacher generates the signature, computes the private key, computes the secret key and after that send the study material along with the signature to the administrator. The last step also include two other functions getdata() and hash().

In the second use case model, shown in the fig.11, we discuss about the signature verification, which has been done by the learner. That means the learner after receiving the study material along with the signature, check for the similarity. Here the learner gets the public key of teacher, receive the study material and signature from the teacher and compares the two hash values. The last step includes two other processes, one is the first hash value sent by the teacher and the other hash value, generated by the learner.

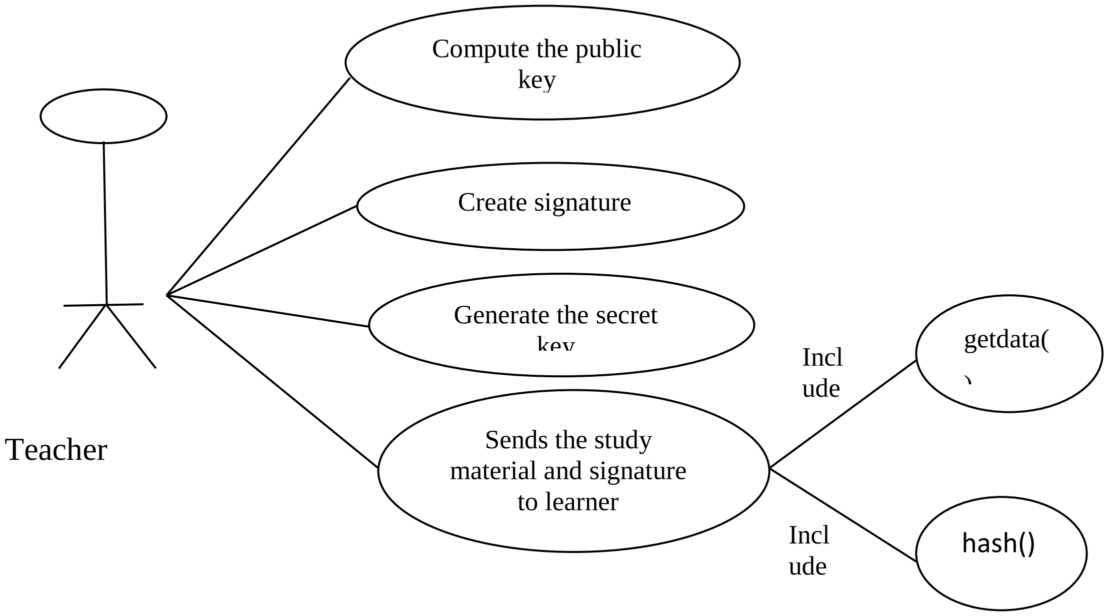


Fig.10: Use case diagram for teacher in RSA digital signature

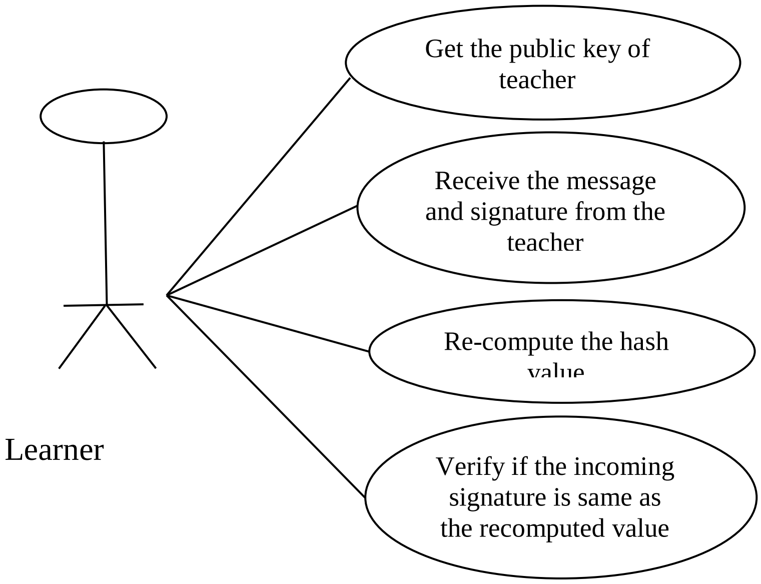

Get the public key of teacher
Receive the message and signature from the teacher
Re-compute the hash value
Verify if the incoming signature is same as the recomputed value
Learner

Fig.11: Use case diagram for learner in RSA digital signature

3.2.3: Data Flow Diagram

The data flow diagram contains the input data to the system and processes which has been carried out on these data and also the output data generated by the system. The data flow diagram of transmission of study material from teacher to learners is shown in the fig.12. Here teacher is sending the study material and compute the hash value from the using the hash() function. The public key and the teacher's private keys are stored in the data store. Using this private key teacher generates the signature and sends it along with the study material and the public key to the learners. After receiving these documents, learners compute the hash value from the public key of teacher and compare the hash values with the received hash value. If they are same, then the learners accept the study material, otherwise request the teacher to resend it.

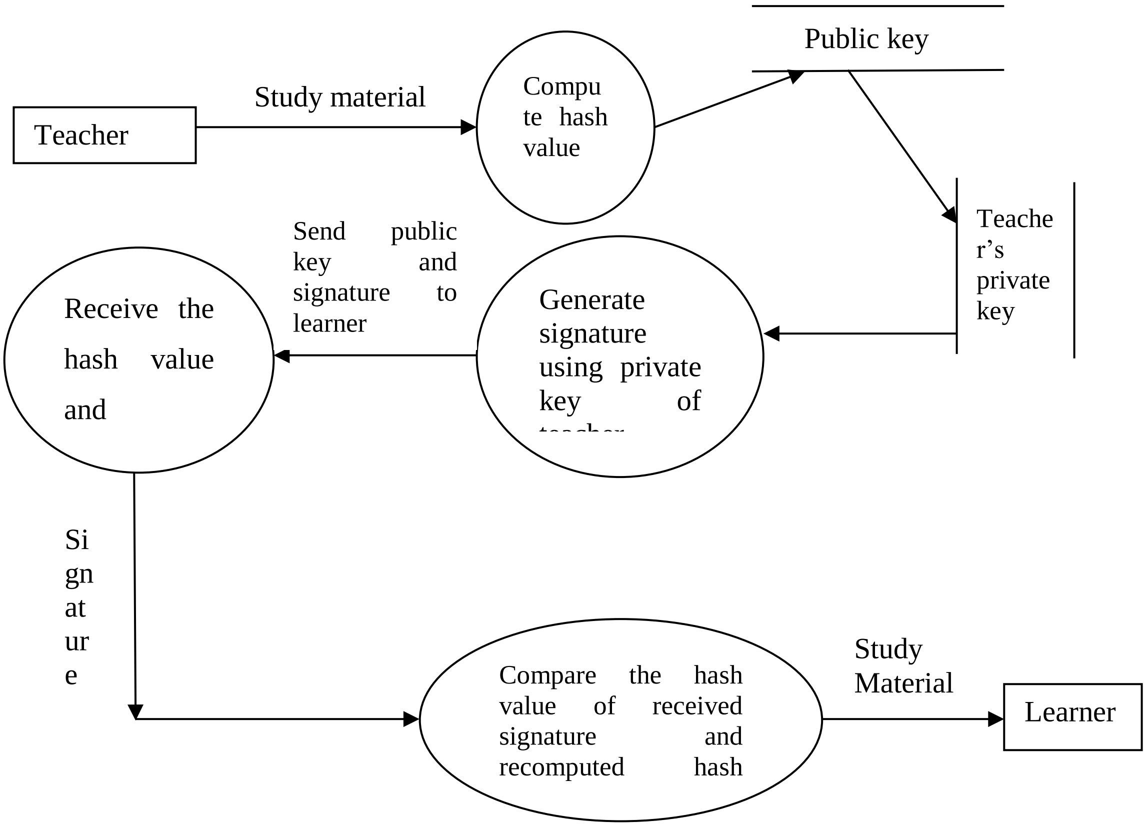

Public key
Study material
Teacher
Compute hash value
Teacher's private key
Send public key and signature to learner
Receive the hash value and
Generate signature using private key of teacher
Signature
Study Material
Compare the hash value of received signature and recomputed hash
Learner

Fig.12: DFD of RSA digital signature of transmission of study material from teacher to learner

3.3 Object oriented modeling of ElGamal digital signature:

In this unit, we will also consider the same model like sending study material from teacher to student and to implement security regarding sending material, we will apply ElGamal digital signature[26]. This digital signature is quite better than the others, because of the application of its discrete logarithm problem. The discrete logarithm problem required for ElGamal Digital Signature is quite tedious and it is not so easy to calculate sender's (here developer) private key from the digital signature. The hardness of solving the logarithm problem in any cyclic group makes this algorithm better than RSA. In this unit, we will implement here the use case diagram, class hierarchy diagram, activity diagram, collaboration diagram and also sequence diagram based on the above context of an e-learning system.

3.3.1 Use Case Diagram:

A use case diagram is a graphical representation of the interactions among the elements of a system. Here the system is an e-learning system. A use case diagram is a part of Unified Modeling Language (UML), which is used in system analysis to identify, clarify, and organize system requirements.[27]

In this Use case diagram, shown in fig.13 and fig.14, shown below, we use two objects: Teacher and Learner. First of all, two universally known numbers, a generator and a modulus, and a universally known hash function are selected. From these two numbers, the teacher calculates an ephemeral public key and a static public key. Then the learner receives the study material from the teacher and uses the hash function combined with the ephemeral public key. After that, the teacher creates the ElGamal signature and sends the static public key, ephemeral public key, study material and signature to learner. These all things are shown in the fig.13. In the fig.14, we have discussed about the ElGamal digital signature verification. Signature verification occurs at the learner end. After receiving all the public keys and signature and study material, student first compute the hash function and then verify the signature for the authentication. If the received signature is authentic, then the study material is accepted otherwise it is rejected.

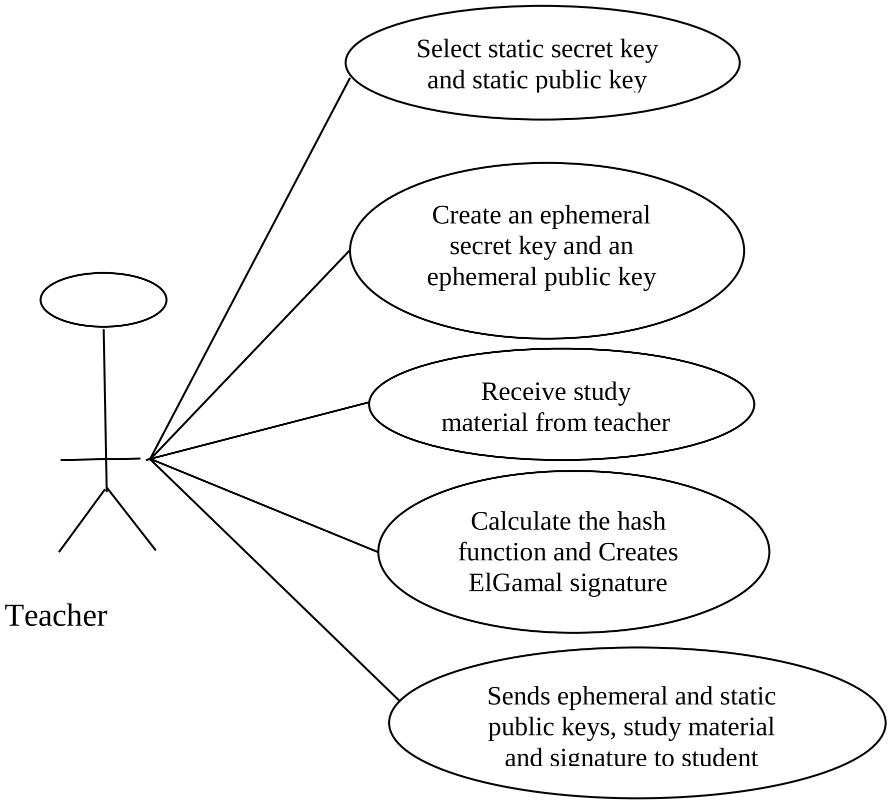

Select static secret key and static public key
Create an ephemeral secret key and an ephemeral public key
Receive study material from teacher
Calculate the hash function and Creates ElGamal signature
Sends ephemeral and static public keys, study material and signature to student
Teacher

Fig.13: Use case diagram for ElGamal signature generation

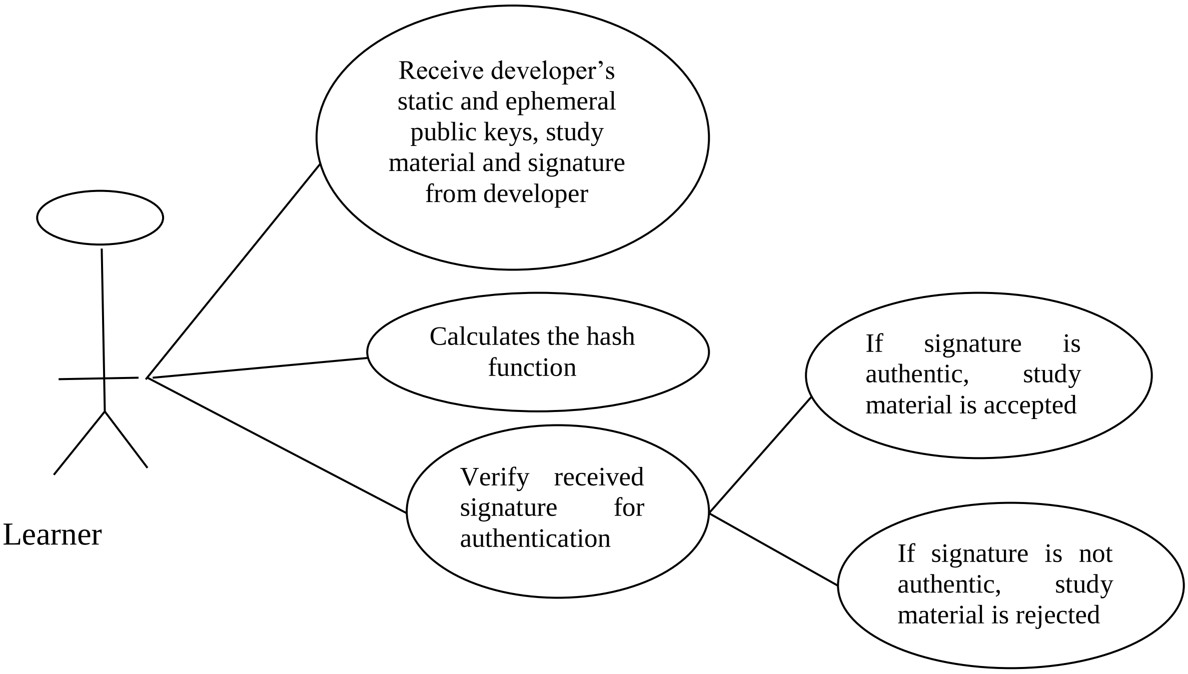
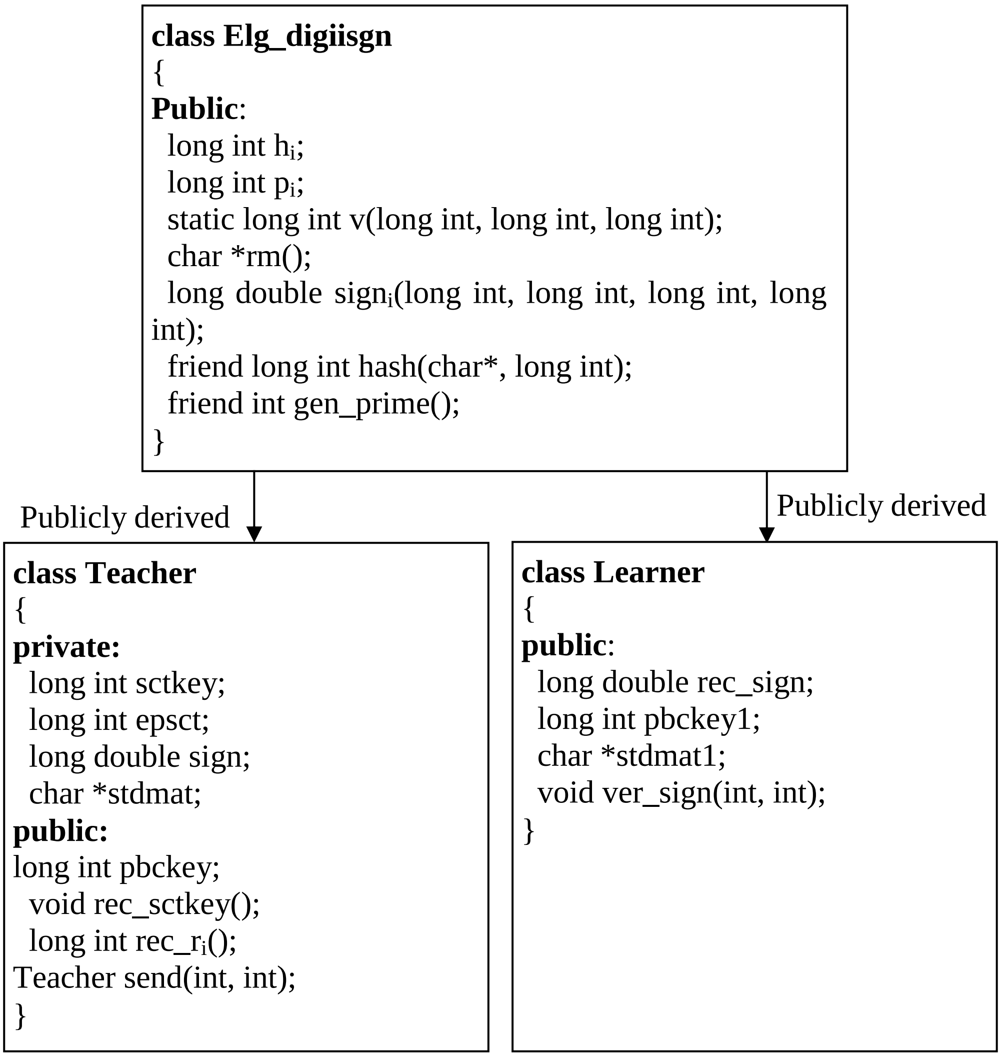

Receive developer's static and ephemeral public keys, study material and signature from developer
Calculates the hash function
Verify received signature for authentication
If signature is authentic, study material is accepted
If signature is not authentic, study material is rejected
Learner

Fig.14: Use case diagram of ElGamal signature verification

3.3.2: Class Diagram:



```
class Elg_digiisgn
{
Public:
  long int h_i;
  long int p_i;
  static long int v(long int, long int, long int);
  char *rm();
  long double sign_i(long int, long int, long int, long
int);
  friend long int hash(char*, long int);
  friend int gen_prime();
}
```

```
class Teacher
{
private:
  long int sctkey;
  long int epsct;
  long double sign;
  char *stdmat;
public:
long int pbckey;
  void rec_sctkey();
  long int rec_r_i();
Teacher send(int, int);
}
```

```
class Learner
{
public:
  long double rec_sign;
  long int pbckey1;
  char *stdmat1;
  void ver_sign(int, int);
}
```

Fig.15: Class Diagram of ElGamal Digital Signature for signature creation and verification

Analysis of class diagram:

The inheritance diagram of ElGamal Digital Signature is shown in the above fig.15. This diagram includes three classes: Elg_digiisgn, Teacher and Learner. The individual classes are discussed below:

Class Elg_digiisgn: This is the base class which does not contain any object. The main aim to use this class is for the inheritance. It has two data members and five member functions, inherited publicly by two other classes: Teacher and Learner. The functions of the data members and member functions are discussed below.

Public members:

long int h_i; //It is used to store the hash value

long int p_i; //It is used to store value of the ephemeral public key

static long int v(long int, long int, long int); //this function is used to calculate the public key

char *rm(); //this function is used to read the study material and returns it to the calling function

long double $sign_i$(long int, long int, long int, long int); //this function is used to generate a signature of the input study material

friend long int hash(char*, long int); //this is a friend function of this class and used to calculate the hash of the study material

friend int gen_prime(); //this is also a friend function of this class and used to generate prime number and return the prime number to the calling functions.

Class Teacher: This class is publicly derived from the base class Elg_digiisgn. This class contains four private data members and one public data member and three public member functions. The private data member can be accessed by only the class Teacher and the public data members are accessible by class Teacher and also by the member functions of other classes. All of these members are discussed below:

long int sctkey; //it is the secret key of the teacher

long int epsct; //it is the ephemeral secret key of the teacher

long double sign; //it is the sign of the study material

char *stdmat; //it is the study material prepared by the teacher

Public members:long int pbckey; //it is the public key of teacher

void rec_sctkey(); //it is used to get the secret key

long int rec_r_i(); //it is used to get the ephemeral key and return to the calling function

Teacher send(int, int); //it is used to send the signature, public key and the study material to learner.

Class Learner: This class is publicly derived from the base class Elg_digiisgn. It contains three data members and one member function. The functions of these members are discussed below:

Public members: long double rec_sign; //it is used to receive the signature from the teacher
long int pbckey1; //it is used to receive the public key from the teacher
char *stdmat1; / /it is used to receive the study material from the teacher
void ver_sign(int, int); //this function is used to verify the signature

3.3.3 Activity diagram:

Here we use the activity diagram to show the links between the activities of the two main components of the e-learning system: Teacher and Learner or Student. Activity diagram is mainly used during the initial stages of requirement analysis and specification. The activity diagram of the Elgemal algorithm to create a Digital Signature, related with e-learning system, is shown in the fig.16.

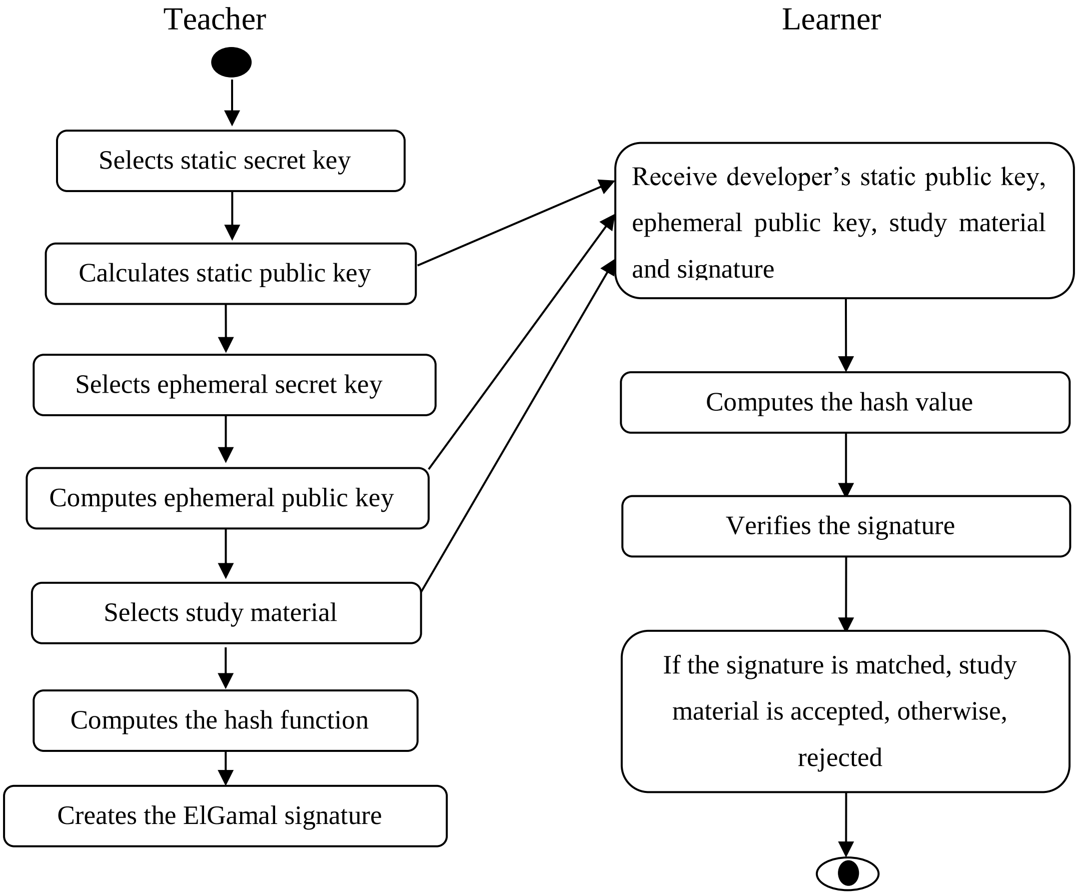

Teacher
Learner
Selects static secret key
Calculates static public key
Selects ephemeral secret key
Computes ephemeral public key
Selects study material
Computes the hash function
Creates the ElGamal signature
Receive developer's static public key, ephemeral public key, study material and signature
Computes the hash value
Verifies the signature
If the signature is matched, study material is accepted, otherwise, rejected

Fig.16: Activity diagram for sending study material from Teacher to learner using ElGamal Digital Signature

3.3.4Collaboration Diagram: Here we use the collaboration diagram in fig.17, to show the structural behavior and message flow between the objects in an e-learning system (here teacher and learner), and it also describes the structural organization and interaction among the objects of the same system.

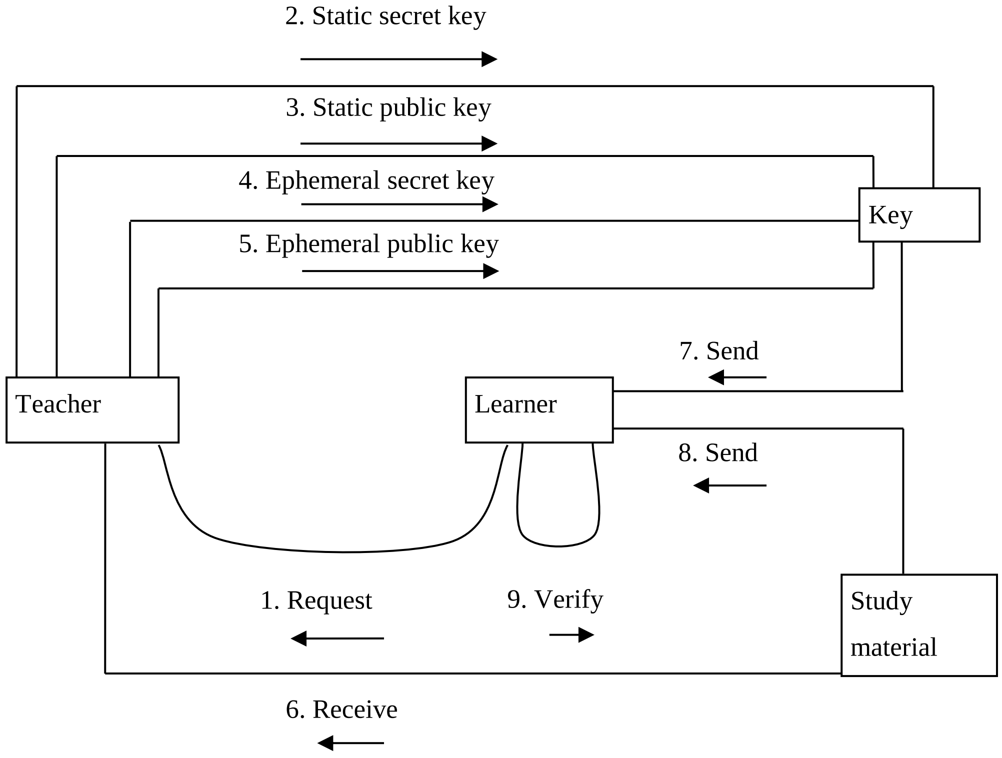


Fig.17: Collaboration Diagram for sending study material from teacher to learner using ElGamal Digital Signature in e-learning system

3.3.5: Sequence Diagram:

A sequence diagram shows the interaction among objects as a two dimensional chart. The chart is read from top to bottom. The sequence diagram is shown in fig.18, where teacher sends the study material along with the digital signature, which is generated using ElGamal Digital Signature Algorithm, to the learner. After receiving the study material from the teacher, before accepting the study material, verify the signature for authentication. In an e-learning system, when teacher sends the study material to the student, teacher also sends the static public key, ephemeral public key and digital signature along with the study material. After receiving all of these from the developer, students calculate the hash value and verify the signature. If the hash values are matched, the learner accepts the study material otherwise, request the teacher to resend it.

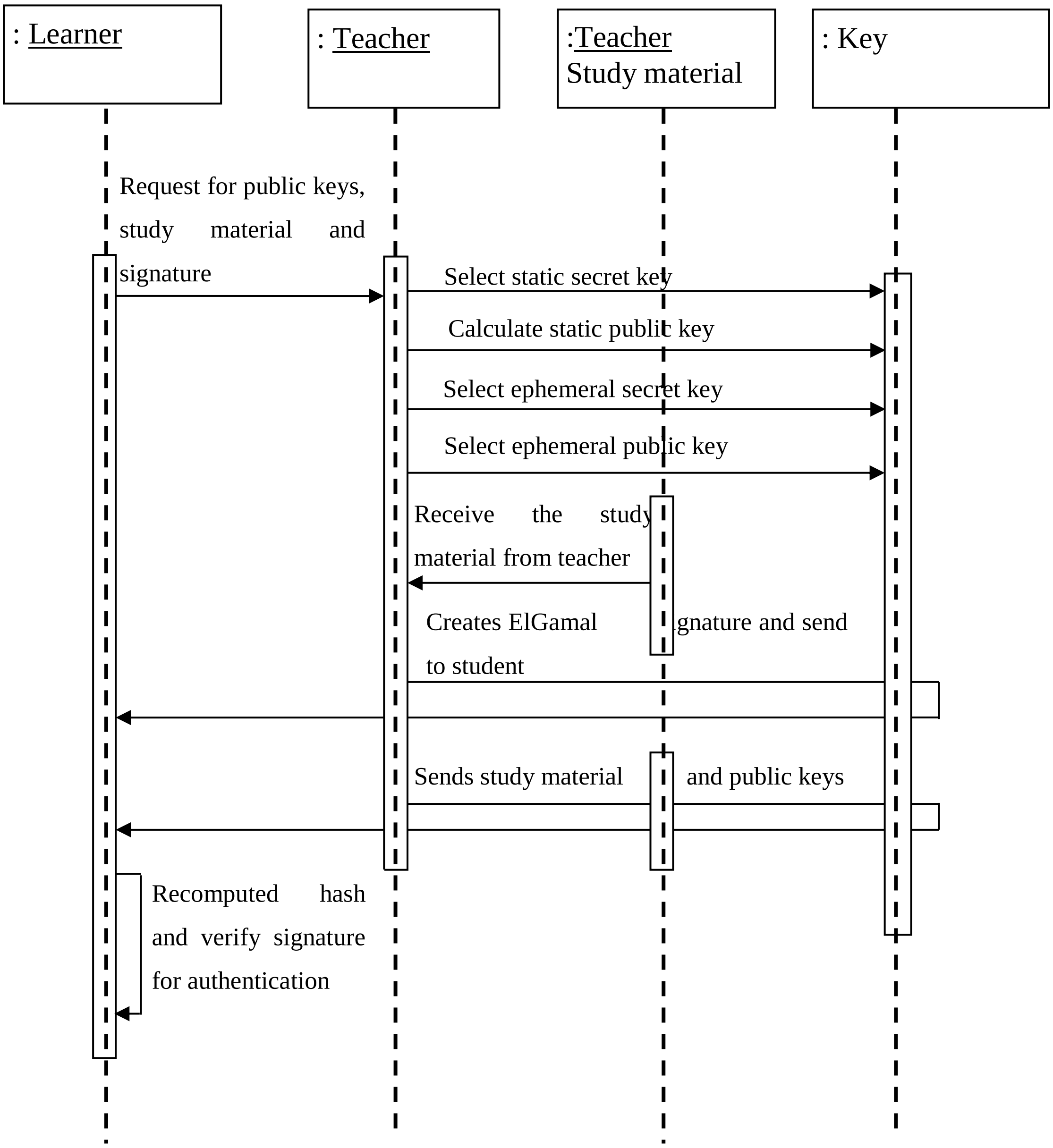

: Learner
: Teacher
:Teacher Study material
: Key
Request for public keys, study material and signature
Select static secret key
Calculate static public key
Select ephemeral secret key
Select ephemeral public key
Receive the study material from teacher
Creates ElGamal signature and send to student
Sends study material and public keys
Recomputed hash and verify signature for authentication

Fig.18: Sequence diagram for ElGamal Digital Signature based on e-learning system

3.4 GOST digital signature:

GOST digital signature algorithm is quite same as the Digital Signature Algorithm. This is officially called GOST R 34.10, which is a Russian digital signature standard. Since the algorithm is quite same as DSA, so the modeling of GOST digital signature algorithm is quite same as the modeling of DSA. So, here we give some short description of this algorithm[28]. The used parameters are:

p=a prime number, either between 509 and 512 bits long or between 1020 and 1024 bits long

q=a 254 to 256 bit prime factor of p-1

a=any number < p-1 such that a^q mod p=1

x=a number < q

y=a^x mod p

Now, we are going to show how a study material, m, can be signed using GOST digital signature:

[1] Teacher generates a random number, k < q

[2] Teacher generates r=(a^k mod p) mod q

S=(xr+k(H(m))) mod q

If H(m) mod q=0, then set it equal to 1. If r=0, then choose another k and start again. The signature is two numbers: r mod 2^{256} and s mod 2^{256}. Teacher sends this to learner.

Now, learner will verify the signature:

V=$H(m)^{q-2}$ mod q

Z_1=(sv) mod q

Z_2=((q-r)*v) mod q

U=(($a^z{}_1$ * $y^z{}_2$)mod p)mod q

If u=r, then the signature will be matched and the learner will accept the study material, otherwise, rejected. This algorithm also uses one-way hash function.

3.4.1: Use case Model:

Here using the use case diagram, we will discuss the transmission of study material from the teacher to learner based on the GOST digital signature. In this transmission, diagram contains two types of objects or two main participants of this system, teacher and learner.

In the first use case model shown in fig.19, we discuss about the creation of the signature, which has been done at the sender that means at the teacher's end. Teacher follows the steps, discussed on the above overview, creates the signature and one-way hash function and sends the study material along with the signature to the student.

The second use case model, shown in fig. 20, contains the discussion on the steps done at the receiver that means at the learner’s end. Here the student receives the public key, mark sheet along with the signature and recomputed the signature. Then he/she verifies the signature for authentication. If the signatures match, then learner will accept the study material, otherwise asked the teacher to resend it.

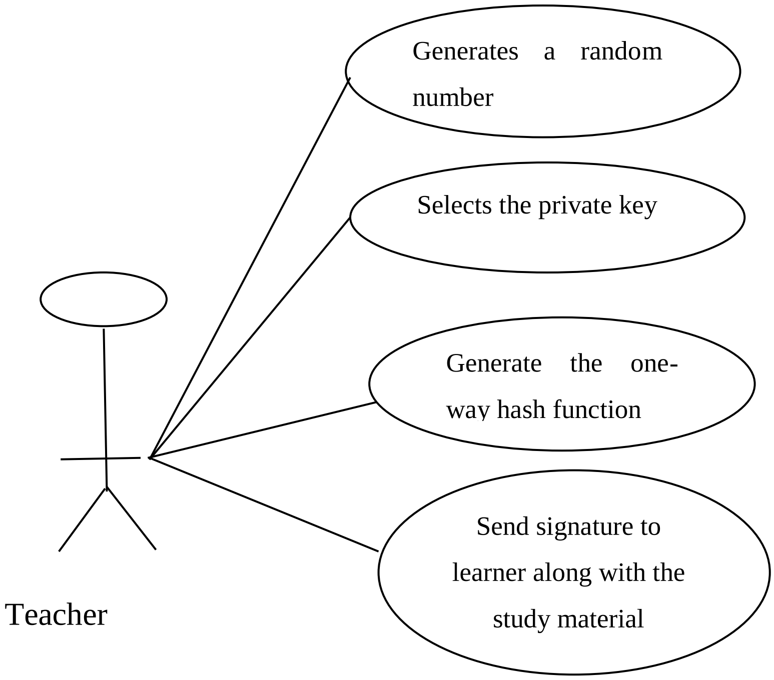

Generates a random number
Selects the private key
Generate the one-way hash function
Send signature to learner along with the study material
Teacher

Fig.19: Use case diagram for GOST digital signature generation

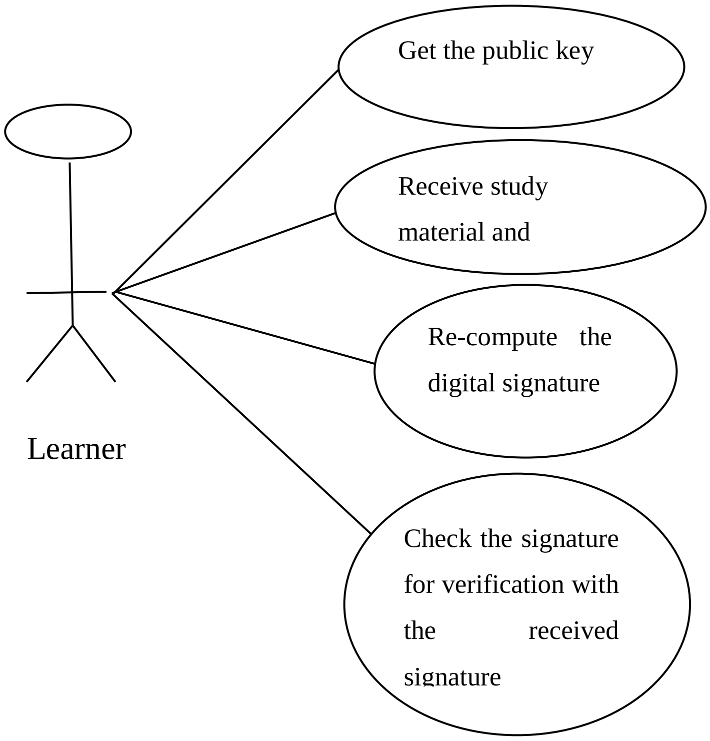

Get the public key
Receive study material and
Re-compute the digital signature
Learner
Check the signature for verification with the received signature

Fig.20: Use case diagram of ElGamal signature verification

3.4.2 Sequence Diagram:

The sequence diagram corresponding to this model is shown in fig.21. Here, the teacher uses GOST digital signature algorithm to generate the signature and send it along with the study material to the learner thorough online. In this diagram, teacher prepares the study material and hands over these documents to developer or the administrator of the institution. Learner collects all the necessary documents required to generate the signature and then verify it with the original one.

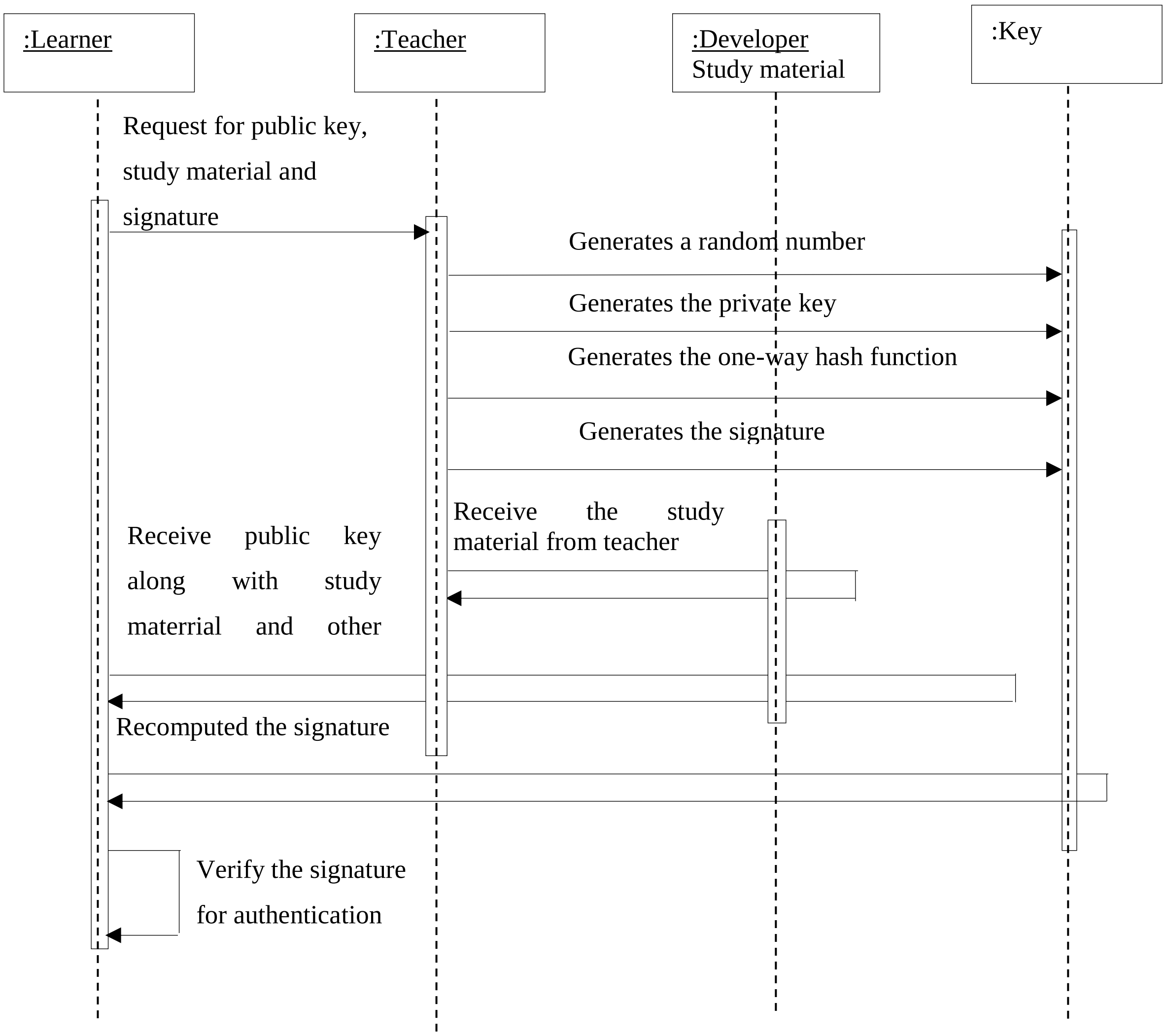

:Learner
:Teacher
:Developer
Study material
:Key
Request for public key, study material and signature
Generates a random number
Generates the private key
Generates the one-way hash function
Generates the signature
Receive the study material from teacher
Receive public key along with study materrial and other
Recomputed the signature
Verify the signature for authentication

Fig.21: Sequence diagram for GOST Digital Signature on the basis of e-learning system

4. OOM of Digital Certificate:

A digital certificate is simply an electronic message. It is signed by the issuer of the certificate, known as the certificate authority, CA, with that CA's private key, so that it uniquely identifies the user holding the issued key pair[29]. E-learning now–a–days is becoming a popular form of Information and Communication Technology (ICT) based education system. Here the system is totally dependent on Internet. So, security is obviously a great issue or challenge to the developer of the system or to the institute of e-learning. The three main security issues privacy, authenticity and non-repudiation, which we discussed earlier, can be achieved using digital certificate along with cryptographic techniques. In all cases of transmission of any material via Internet, the participants of any e-learning system can apply digital certificate[30]. But here consider a case where the teacher sends a set of study material to a learner. Then the teacher will send the encrypted study material, digital signature and digital certificate to the learner. Learner, after receiving all these, recomputed the hash value and verify for authentication. If the values matched, then learner will accept the material and decrypt it, otherwise, send a request to teacher to send the study material again. So, digital certificate is very essential to achieve the goal of security in any e-learning system.

Now, we will discuss on some of the object oriented modeling of digital certificate based e-learning system. According to our context, we will take the example of transmission of study material from teacher to learner using digital certificate.

4.1 Data Flow Diagram:

To make a better understand of the transmission of the study material, in this section, we use two Data flow diagrams, shown in the fig.21 and figure22.

The data flow diagram, shown in figure21, discusses about the secure transmission of the study material from the teacher to learner using digital certificate. Teacher sends the three part transmission (encrypted study material, digital signature and digital certificate) to the learner. The DFD, in figure2, discusses about the decryption of the study material, comparing of hash functions to verify digital signature and digital certificate at the developer's end. If the hash functions are equal, then the signature and certificate is considered as unchanged and accepted for further use.

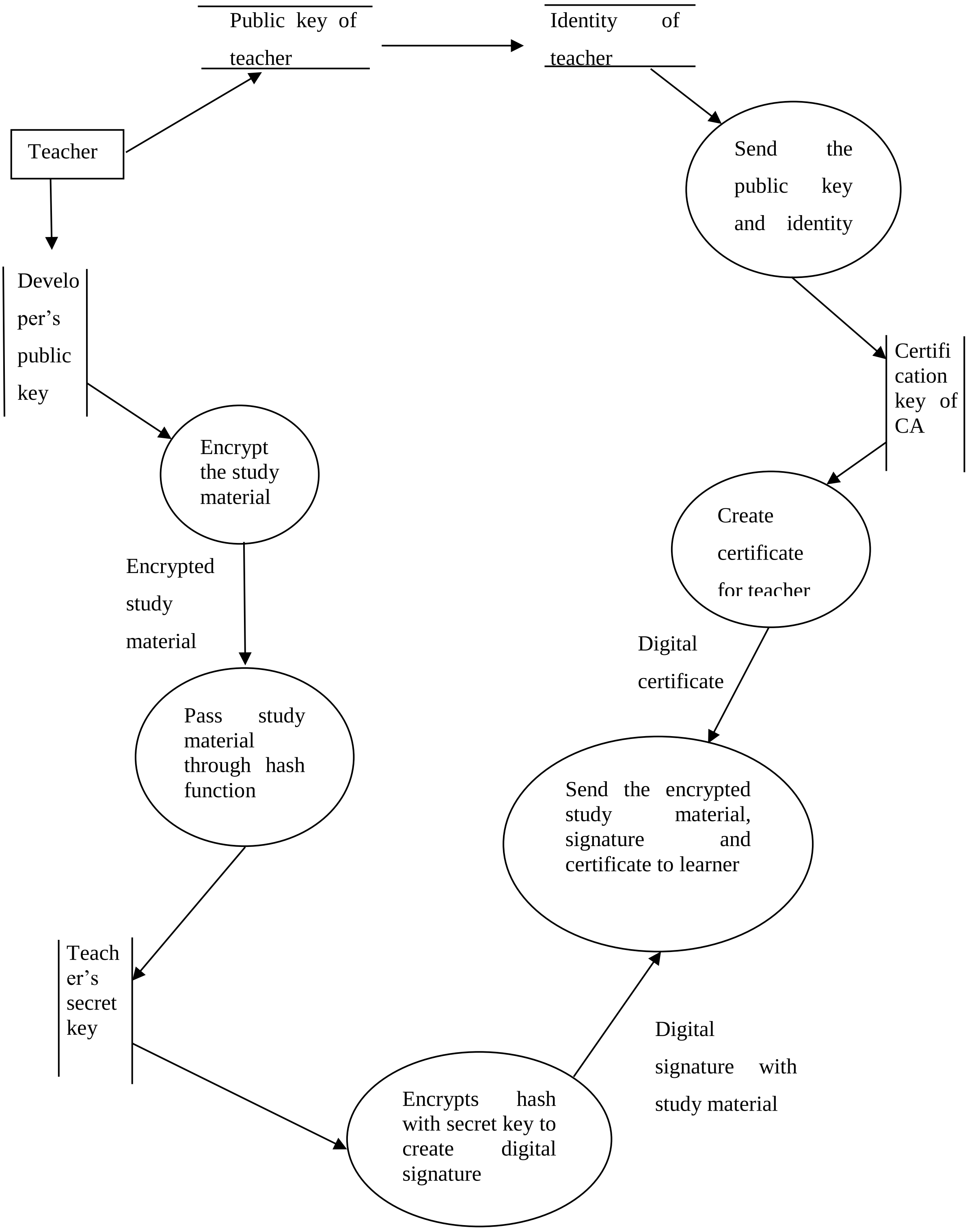

Public key of teacher
Identity of teacher
Teacher
Send the public key and identity
Develo per's public key
Certifi cation key of CA
Encrypt the study material
Create certificate for teacher
Encrypted study material
Digital certificate
Pass study material through hash function
Send the encrypted study material, signature and certificate to learner
Teach er's secret key
Digital signature with study material
Encrypts hash with secret key to create digital signature

Fig.21: DFD for transmission of study material from teacher to learner

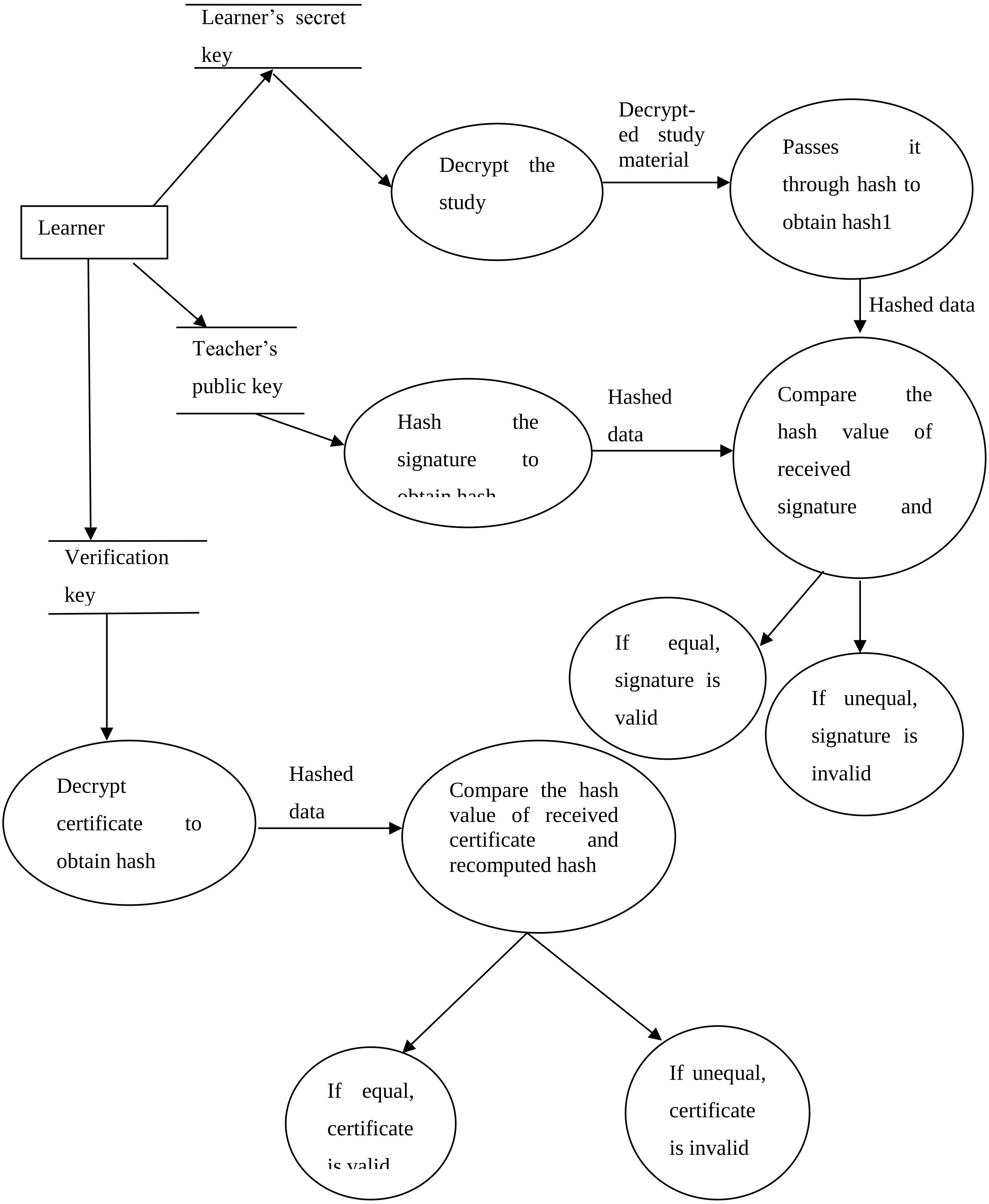

Learner's secret key
Learner
Decrypt the study
Decrypt-ed study material
Passes it through hash to obtain hash1
Hashed data
Teacher's public key
Hash the signature to obtain hash
Hashed data
Compare the hash value of received signature and
Verification key
If equal, signature is valid
If unequal, signature is invalid
Decrypt certificate to obtain hash
Hashed data
Compare the hash value of received certificate and recomputed hash
If equal, certificate is valid
If unequal, certificate is invalid

Fig.22: DFD at the learner's end

4.2 Use Case Model:

To draw the diagram of the use case model, in this context, we use three types of objects, Certificate Authority or CA, teacher as sender and learner as receiver.

The first use case model, shown in fig.23, includes the discussion about the creation of certificate of teacher by the Certificate Authority or CA. Certificate Authority first receives the public key of teacher and the identity proof. The certificate authority does not directly receive these. Usually CA delegates Registration Authority for this purpose. For this reason, digital certificate is also known as a trusted third party system. After being sure about the teacher's identity and the authentication of public key, CA creates the digital certificate for him and sends this to the teacher.

In the second use case diagram, shown in fig.24, discusses about the activities of teacher. Teacher creates his key pairs, public key and private key. Teacher sends the public key and identity key to the CA to create digital certificate and use developer's public key to create encrypted message and his secret key to create hash function. Finally, teacher sends the encrypted study material, digital signature and digital certificate to the learner.

The third use case diagram, shown in fig.25, discusses about the activities of the learner. After receiving the three part transmissions from the teacher, the learner decrypts the study material, recomputed the hash functions and compares the recomputed values with the hash value of the teacher.

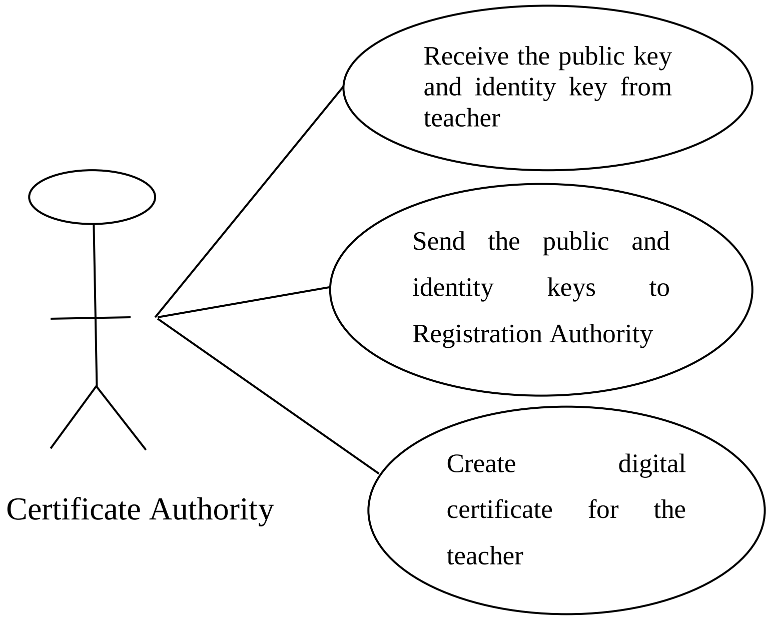

Receive the public key and identity key from teacher
Send the public and identity keys to Registration Authority
Create digital certificate for the teacher
Certificate Authority

Fig.23: Use case diagram of Certificate Authority (CA) to create digital certificate

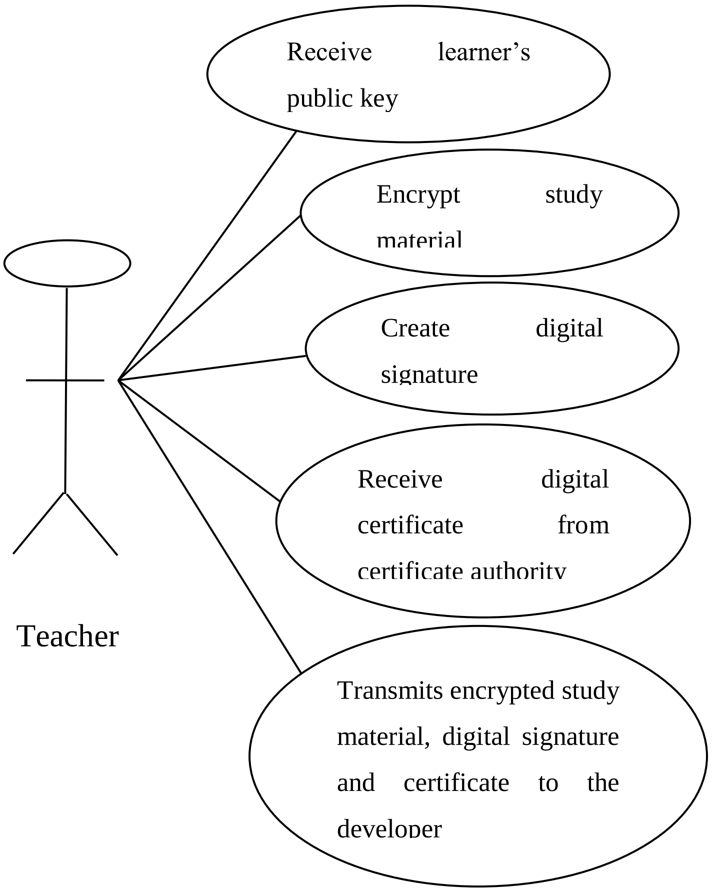

Receive learner's public key
Encrypt study material
Create digital signature
Receive digital certificate from certificate authority
Transmits encrypted study material, digital signature and certificate to the developer
Teacher

Fig.24: Use case diagram of Teacher for authentication using digital certificate

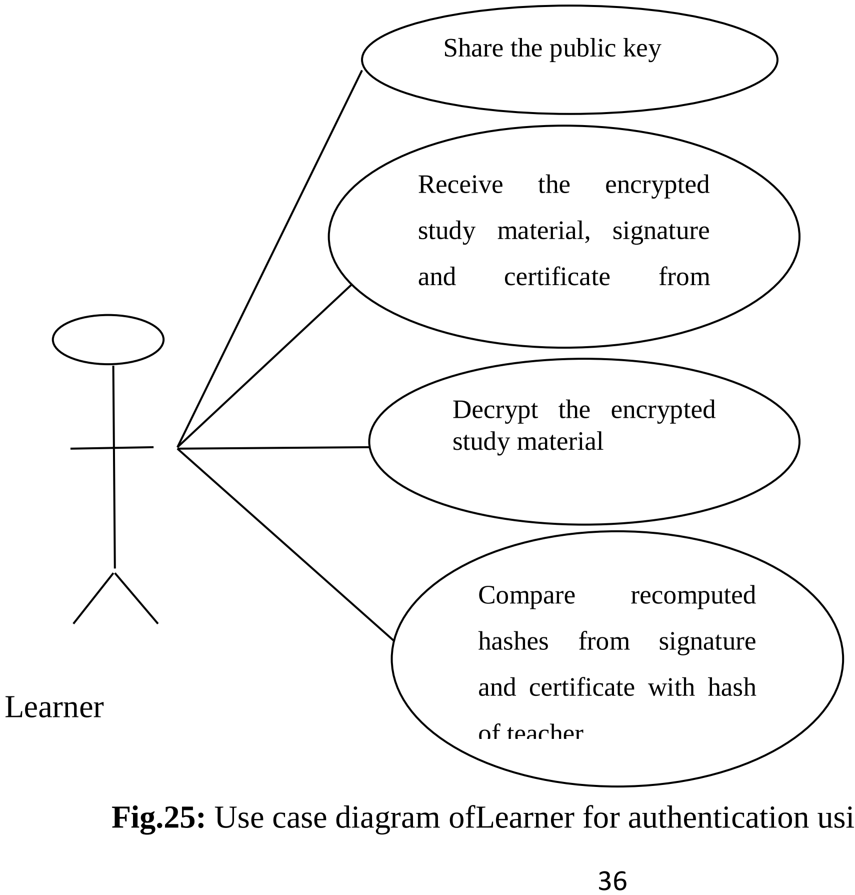

Share the public key
Receive the encrypted study material, signature and certificate from
Decrypt the encrypted study material
Compare recomputed hashes from signature and certificate with hash of teacher
Learner

Fig.25: Use case diagram ofLearner for authentication using digital certificate

4.3: Sequence Diagram

Here we use two sequence diagrams, shown in the fig.26 and fig.27. The sequence diagram, shown in fig.26, includes the discussion about the transmission of encrypted study material, along with digital signature and digital certificate to provide security and authenticity, from teacher to learner.

The another sequence diagram, shown in fig.27, shows the decryption of the study material, re-computation of the hash functions from the digital signature and digital certificate and also of the verification of the digital signature and certificate by comparing the hash functions, which have been done at the learner's end.

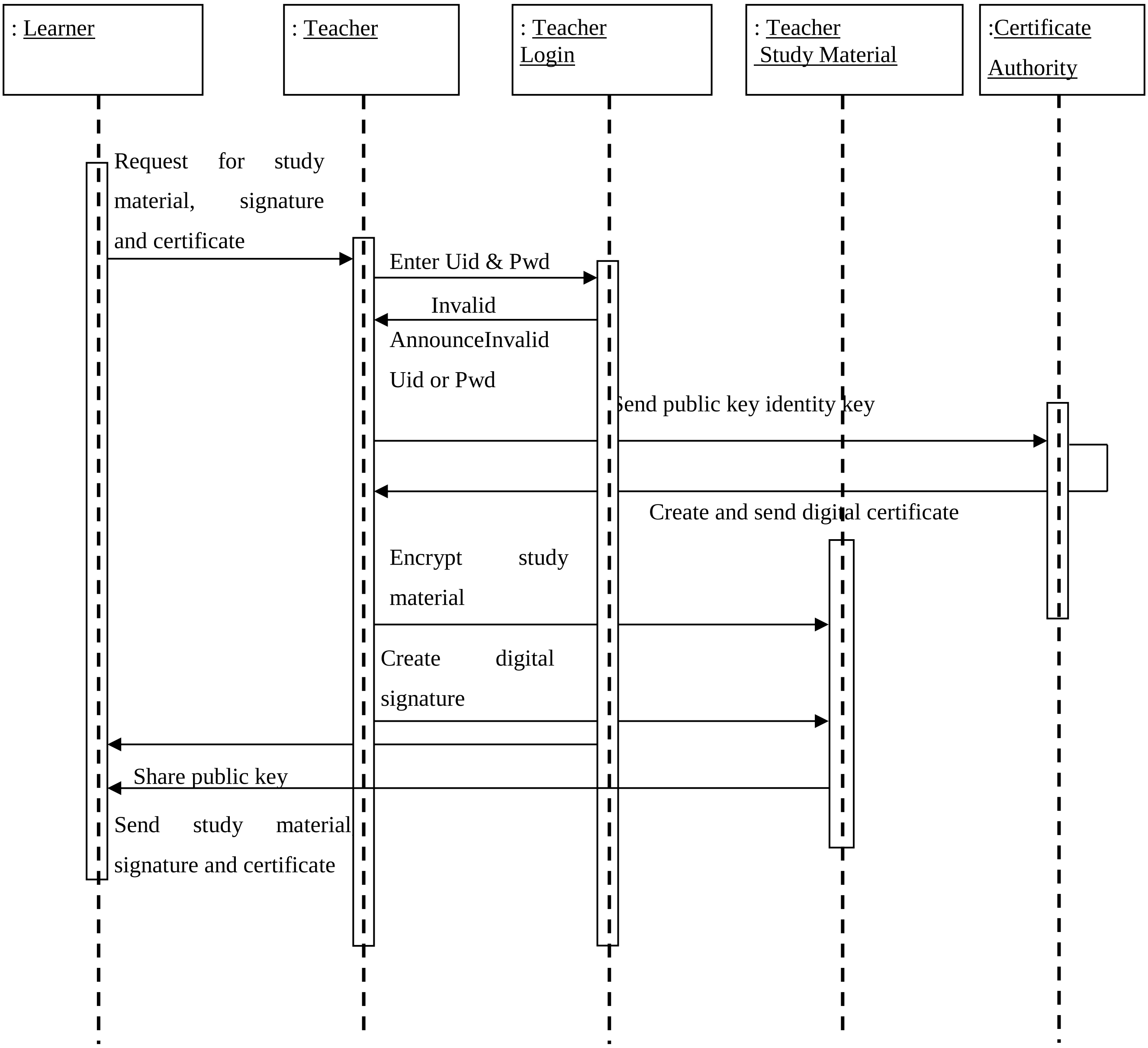
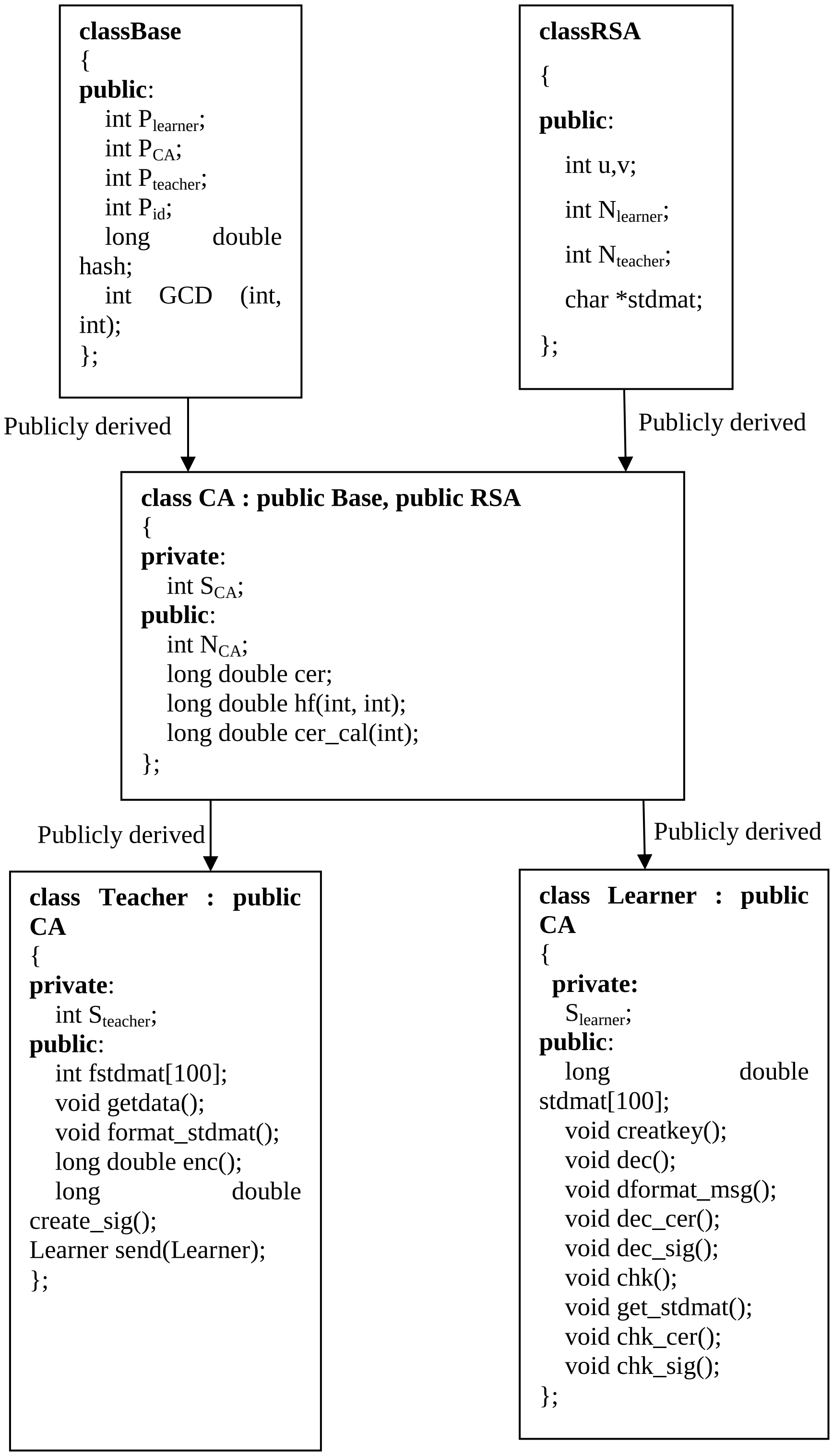

: Learner
: Teacher
: Teacher Login
: Teacher Study Material
:Certificate Authority
Request for study material, signature and certificate
Enter Uid & Pwd
Invalid
AnnounceInvalid Uid or Pwd
Send public key identity key
Create and send digital certificate
Encrypt study material
Create digital signature
Share public key
Send study material signature and certificate

Fig.26: Sequence diagram for teacher regarding the secure transmission of study material using digital certificate

4.4 Class Hierarchy Diagram:



classBase
{
public:
int $P_{learner}$;
int P_{CA};
int $P_{teacher}$;
int P_{id};
long double hash;
int GCD (int, int);
};

classRSA
{
public:
int u,v;
int $N_{learner}$;
int $N_{teacher}$;
char *stdmat;
};

class CA : public Base, public RSA
{
private:
int S_{CA};
public:
int N_{CA};
long double cer;
long double hf(int, int);
long double cer_cal(int);
};

class Teacher : public CA
{
private:
int $S_{teacher}$;
public:
int fstdmat[100];
void getdata();
void format_stdmat();
long double enc();
long double create_sig();
Learner send(Learner);
};

class Learner : public CA
{
private:
$S_{learner}$;
public:
long double stdmat[100];
void creatkey();
void dec();
void dformat_msg();
void dec_cer();
void dec_sig();
void chk();
void get_stdmat();
void chk_cer();
void chk_sig();
};

Fig.27 Class hierarchy diagram of transmission of study material using digital certificate

Analysis of Class Diagram:

Now, we will discuss on the classes and their private and public data members and member functions, we use in the above diagram.

Class Base:

This class is publicly inherited by the class CA, short form of Certificate Authority. In the Base class we use five data members and one member function. From the five data members, four of them contain the public keys of the objects used here and one is used to store the hash value. The member function is used to find the GCD value of the given two co-prime numbers.

Public members:

int $P_{learner}$; // learner's public key

int P_{CA}; //certificate authority's public key

int $P_{teacher}$; // teacher's public key

int P_{id}; //teacher's identity number

long double hash; //hash function

int GCD (int, int); /*this is the only function in this class and this is used for finding an appropriate public key from two co-prime numbers supplied to it.*/

Class RSA:

This class is also publicly inherited by the class CA. In this class, we use four data members. This class is used to store the two co-prime numbers and the study material, send by the teacher to learner and the other two data members are used to encrypt and decrypt this study material.

Public members:

int u,v; // these are two co-prime numbers used to create public and secret key

int $N_{learner}$, $N_{teacher}$; //these are used to encrypt or decrypt the message

char *stdmat; //this is the study material (character string), sent to the learner by the teacher

Class CA:

This class corresponds to the certificate authority and it inherits the classes Base and RSA publicly and it is inherited by both the classes Teacher and Learner. This class is used to store the data and functions of certificate authority. It stores the secret and public key of CA, certificate of the teacher; create by CA and two member functions for the hash function, to create certificate and the certificate calculation.

Private member:

int S_{CA}; //this is the secret key of CA, used to encrypt certificate

Public member:

int N_{CA}; // public key, used to encrypt or decrypt certificate

long double cer; //holds the certificate

long double hf(int, int); //used to calculate sign hashed value for certificate of study material

long double cer_cal(int); //calculate certificate

Class Teacher:

This corresponds to the customer and it inherits the class CA publicly i.e. it is in turn inheriting the classes Base, RSA and CA. Though it contains the public members of the Base, RSA and CA classes, it also has one private and public data member and five public member functions. The private member is assign to the secret key of teacher, which is used to create digital signature. The array stores the study material of the teacher. The member functions are used to do the other processes like creation of keys, encryption of study material and the other tasks which have been done at the teacher's end.

Private Member:

int $S_{teacher}$; //this is the secret key of teacher

Public members:

int fstdmat[100]; //this array holds the study material after being converted into integers

void getdata(); //get study material and also creates the public and secret key

void format_stdmat(); //used to format the study material into an integer array containing integer

long double enc(); //this is used to encrypt the study material

long double create_sig(); //it is used to create the digital signature

Learner send(Learner); //this function sends three part (stdmat, sig, cer) information to learner

/*Here the **send(Learner)** function is actually calling the other three methods of this class and also the cer_cal() method of the class CA to calculate certificate.*/

Class Learner:

This corresponds to the Learner and it inherits the class CA publicly i.e. it is in turn inheriting the classes Base, RSA and CA. Except of containing the other public members of the Base, RSA and CA classes, it also has a private and public data member and some other member functions which are used to perform the tasks of the learner related to the study material.

Private member:

$S_{learner}$; //secret key of learner and it is used to decrypt the study material

Public members:

long double stdmat[100]; //it stores received study material after decryption void creatkey(); //create public and secret keys for learner

void dec(); ////decrypts the encrypted message

void dformat_msg(); //used to get actual message after getting the decrypted formatted message

void dec_cer(); //decrypts the encrypted digital certificate

void dec_sig(); //decrypts the encrypted digital signature

void chk(); //invokes functions get_stdmat(), chk_cer() and chk_sig() for authentication checking

void get_stdmat(); //invokes decrypt() function to get the original study material

void chk_cer(); //invokes dec_cer() function to check the certificate

void chk_sig(); //invokes dec_sig() methods to verify the signature

5. Conclusion:

E-learning is emerging at a great speed through the whole world. Since, it has no barrier of place and the learners need not to move from one place to another for learning and to get degree, so the it is mainly becoming very popular to the working persons, who can't effort so much time like a regular learner. Security is the most important aspect for the success of implementation of e-learning in our society. We have successfully developed object oriented models of secured e-learning system where privacy, integrity, non-repudiation and authenticity of learning respective are proposed utilizing secret key cryptography and public key cryptography. We have prepared object oriented modeling of most popular industry standards encryption algorithms such as DES, triple DES. Similar model can be implemented using IDEA, which is beyond the scope of this article. This article also contains the object oriented implementations of some of the public key cryptographies, like: DSA, RSA digital signature and ElGamal digital signature and also the object oriented modeling of digital certificate. Above object oriented models are not only securing the e-learning materials but also transacting them more efficiently among the communicating parties. Object oriented modeling tools are implying software quality also. Many authentication techniques also may be wrapped in proper object oriented modeling in e-learning system. These techniques are based on digital watermarking, digital right management, steganography, biometric scanner etc. but these are very cost effective and time consuming.

References:

[1] Weippl, R.E (2005), Security in E-Learning, Springer

[2]http://24x7learning.com/blog/prospect-of-elearning-in-the-indian-scenario

[3] B.Holmes and J.Gardner, “E-learning-concepts and practice”, Sage publications, New Delhi, 2006

[4] http://www.virtual-college.co.uk/elearning/elearning.aspx

[5] Karforma S. and Banerjee S., “Object Oriented Implementation of DES for Security in E-Learning”, Asian Resonance, VOL.-III, ISSUE-IV, October-2014, pp:12-20

[6] http://blog.schneider-electric.com/datacenter/2011/08/19/understanding-firewalls-and-their-role-in-network-security

[7]http://www.dba-oracle.com/t_object_oriented_approach.htm

[8] https://en.wikipedia.org/wiki/Object-oriented_analysis_and_design#Object-oriented_design

[9] https://www.tutorialspoint.com/uml/uml_standard_diagrams.htm

[10] https://www.tutorialspoint.com/uml/uml_use_case_diagram.htm

[11] Rajib Mall, Fundamentals of Software Engineering, Prentice Hall of India, New Delhi, 2006

[12] http://www.tutorialspoint.com/uml/uml_activity_diagram.htm

[13] http://www.tutorialspoint.com/uml/uml_interaction_diagram.htm

[14] Andrew, S. Tanenbaum (2005), Computer Networks, Pearson Prentice Hall

[15] Balagurusamy, E, Object Oriented Programming with C++, Tata McGraw Hill, New Delhi, 2006

[16] Karforma S. and Banerjee S., “Object Oriented Implementation of DES for Security in E-Learning”, Asian Resonance, VOL.-III, ISSUE-IV, October-2014, pp:12-20

[17] Karforma S. and Mukhopadhyay S., “A Study on the application of Cryptography in E-Commerce”, The university of Burdwan, W.B, India, July, 2005

[18] Behrouz, A Forouzan, “Data Communication and Networking”, Tata McGraw Hill, 2006

[19] http://www.cryptographyworld.com/des.htm

[20] https://en.wikipedia.org/wiki/Triple_DES

[21] Schneier Bruice, “Applied Cryptography”, Wiley India Edition, 2008

[22] http://arxiv.org/ftp/arxiv/papers/1003/1003.4085.pdf

[23] http://web.townsendsecurity.com/bid/72450/What-are-the-Differences-Between-DES-and-AES-Encryption

[24] Ghosh A. and Karforma S., “Object Oriented Modeling of DSA for Authentication of Student in E-Learning”, International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064, pp: 2293-2297

[25] Karforma S. and Banerjee S., “Object oriented modeling of RSA Digital Signature for security in E-learning”, IJATES, Vol No,2, Special issue no-01, September-2014, pp:283-290

[26] Karforma S. and Banerjee S., “Object Oriented modeling of ElGamal Digital Signature for authentication of study material in E-learning system”, IJARSE, Vol. No.4, Special Issue (02), February 2015, pp: 455-460

[27] http://whatis.techtarget.com/definition/use-case-diagram

[28] Graff, J.C., “Cryptography and E-commerce”, John Wiley & Sons, New York, 2001

[29] Ghosh A. and Karforma S.,”An UML based Design of E-Learning System using Digital Certificate**”,** Oriental Journal of Computer Science and Technology,Volume 05 No. 02 Page No. 257-262 Dec 2012

[30] Karforma S. and Banerjee S., “Object oriented modeling of Digital Certificate in E-learning”, IJETTCS, Vol-3 Issue-5, sept-oct 2014, pp 205-211