OBJECT ORIENTED MODELING OF ELGAMAL DIGITAL SIGNATURE FOR AUTHENTICATION OF STUDY MATERIAL IN E-LEARNING SYSTEM

Dr. Sunil Karforma[1], Soumendu Banerjee[2]

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

[2]*Research Scholar, Dept. of Computer Science, The University of Burdwan*

ABSTRACT

E-learning is now-a-days playing a vital role in our learning process. One of the most challenging things for developers in e-learning system is to secure data transmission. Being a fully online system, during transmission of study materials from developer to student, hacker can change or destroy those. At a student's point of view, non-repudiation is also an important issue in e-learning system. In this paper, we have only consider transmission of the study materials from developer to student, where verification of digital signature will check the hacking and the developer can't deny from sending the material. To provide authenticity and strong non-repudiation, we wrapped the ElGamal Digital Signature in object oriented models to get the also the benefits of the object oriented approach.

Keywords*: *ElGamal Digital Signature, E-learning, Activity diagram, Use case model, Sequence diagram, Class diagram, Collaboration Diagram

I INTRODUCTION

An e-learning system is totally a network-based and computerized online transaction system. Security issues of an e-learning system is Privacy, Integrity, Availability and Non-repudiation[8]. Here secrecy means only the authorized persons can access the information. Integrity means only the authorized persons can change or modify data. Availability means that if the network is too slow, then the student will face difficulty while giving exam or downloading study materials. Non-repudiation means no one can deny after sending any online documents. Let us consider a situation of an e-learning system, where the institute sends an incorrect result to a student. Now when the student will call the administrator about the result, he/she can deny about the sending of the result. This kind of situation can be handled using digital signature. In this paper we use object oriented models of ElGamal Digital Signature Algorithm[9,10] for authentication of study material. 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 the ElGamal Digital Signature, we have to consider two universally known data: generator and modulus and one hash function. Developer selects a private key, an

ephemeral secret key, calculates a public key, an ephemeral public key, receives the study material from the teacher, and generates a hash value and digital signature. Then the developer sends the two public keys, study material and the signature to the student. Now the student will reuse the signature for authentication. If the signature authentic, then the student will accept the study material, otherwise, they will reject the study material and request developer for sending the material again. In the meantime, the hacking is also checked out. During the sending of study material from developer to student, hackers can change or damage the material[4], which make a bad impression for the institution. In this competitive market[6], the developer should pay a great attention to save their study materials from hacking. The ElGamal Digital Signature also help the student to check whether the study material is manipulated or not during transmission. This makes a good image for the institution in students' mind.

In this paper, we present, the object oriented models[5,7] with the help of activity diagram, sequence diagram, use case model, collaboration diagram and class diagram of ElGamal Digital Signature. With the use of object oriented design[1], we can improve signature by eliminating redundant code, extending the use of existing classes or reusing the codes, which is the recent trend of software engineering. Using data hiding properties, we can also hide the data from the outside world, which is also a benefit of using object oriented programming.

In section II, we have design the object oriented models like, activity diagram, use case diagram, sequence diagram and collaboration diagram. In sections III we have discussed about the class diagram of the proposed e-learning system. Finally, we have concluded in section IV by highlighting some future scopes.

II OBJECT ORIENTED ANALYSIS AND DESIGN

2.1 Activity Diagram

Activity diagram is a tool of UML, showing relationship between the activities of the different components of a system for better understanding[12]. Here we use the activity diagram to show the links between the activities of the two main components of the e-learning system: Developer and Student. Activity diagram is mainly used during the initial stages of requirement analysis and specification[7]. The activity diagram of the Elgemal algorithm to create a Digital Signature, related with e-learning system, is shown in the fig.1 in the annexure.

2.2 Use Case Diagram

In this Use case diagram, shown in fig.2 and fig.3, in the annexure, we use two objects: Developer and Student. 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 developer calculates an ephemeral public key and a static public key. Then the developer receives the study material from the teacher and uses the hash function combined with the ephemeral public key. After that, the developer creates the ElGamal signature and sends the static public key, ephemeral public key, study material and signature to student. These all things are shown in the fig.2. In the fig.3, we have discussed about the ElGamal signature verification. Signature verification occurs at the student 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.

2.3 Sequence Diagram

A sequence diagram[2,7] 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.5, in annexure, where developer sends the study material along with the digital signature, which is generated using ElGamal Digital Signature Algorithm, to the student and the student, before accepting the study material, verifying the signature for authentication. In an e-learning system, when developer sends the study material to the student, he/she also sends the static public key, ephemeral public key and digital signature. After receiving all of these from the developer, students calculate the hash value and verify the signature.

2.4 Collaboration Diagram

Collaboration diagram[7] is one kind of UML interaction diagram. The purpose of this diagram is to emphasize on the structural organization of the objects that sends and receive messages[11]. Here we use the collaboration diagram in fig.6, to show the structural behavior and message flow between the objects in an e-learning system, and it also describes the structural organization and interaction among the objects of the same system.

III CLASS DIAGRAM

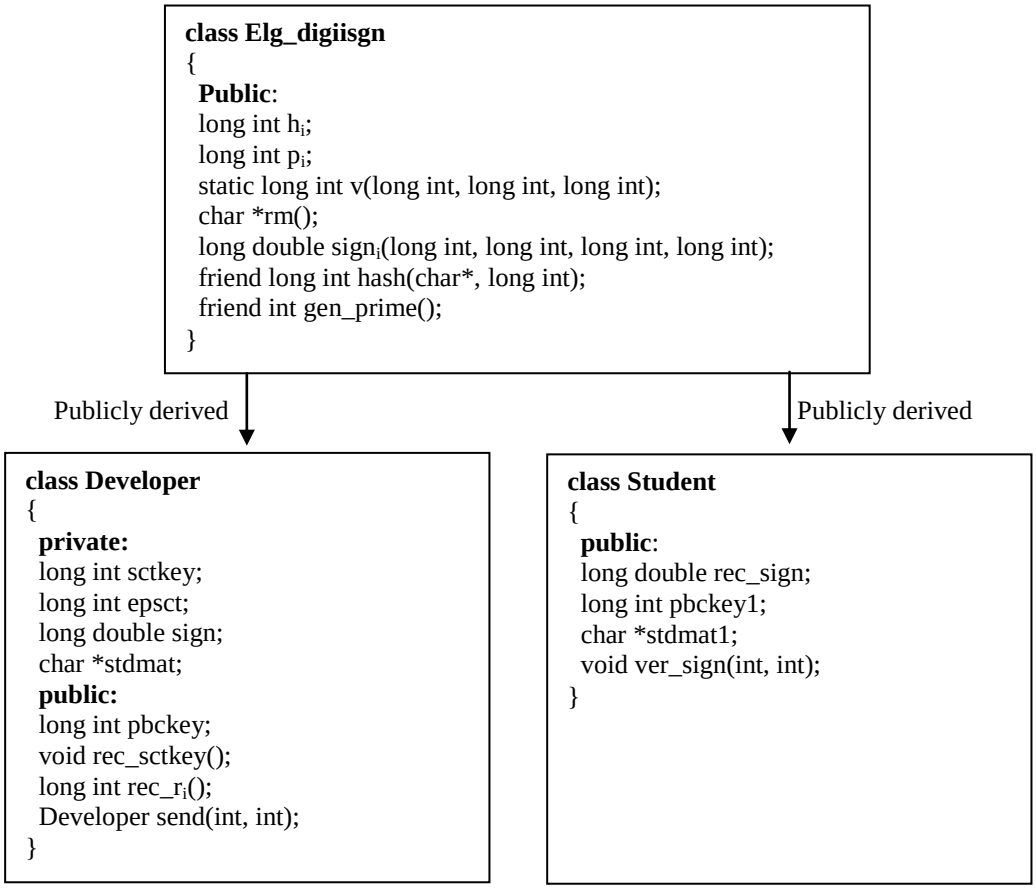

Fig.4: Class Diagram of ElGamal Digital Signature for signature creation and verification

3.1 Analysis of class diagram

The inheritance diagram[1,3] of ElGamal Digital Signature is shown in the above fig.4. This diagram includes three classes: Elg_digiisgn, Developer and Student. 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 which is inherited publicly by two other classes: Developer and Student. 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 metrial 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 Developer

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 Developer and the public data members are accessible by class Developer 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 developer
long int epsct; //it is the ephemeral secret key of the developer
long double sign; //it is the sign of the study material
char *stdmat; //it is the study material received by the developer from the teacher

Public members

long int pbckey; //it is the public key of developer
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
Developer send(int, int); //it is used to send the signature, public key and the study material to student.

Class Student

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 developer

long int pbckey1; //it is used to receive the public key from the developer

char *stdmat1; / /it is used to receive the study material from the developer

void ver_sign(int, int); //this function is used to verify the signature

ANNEXURE

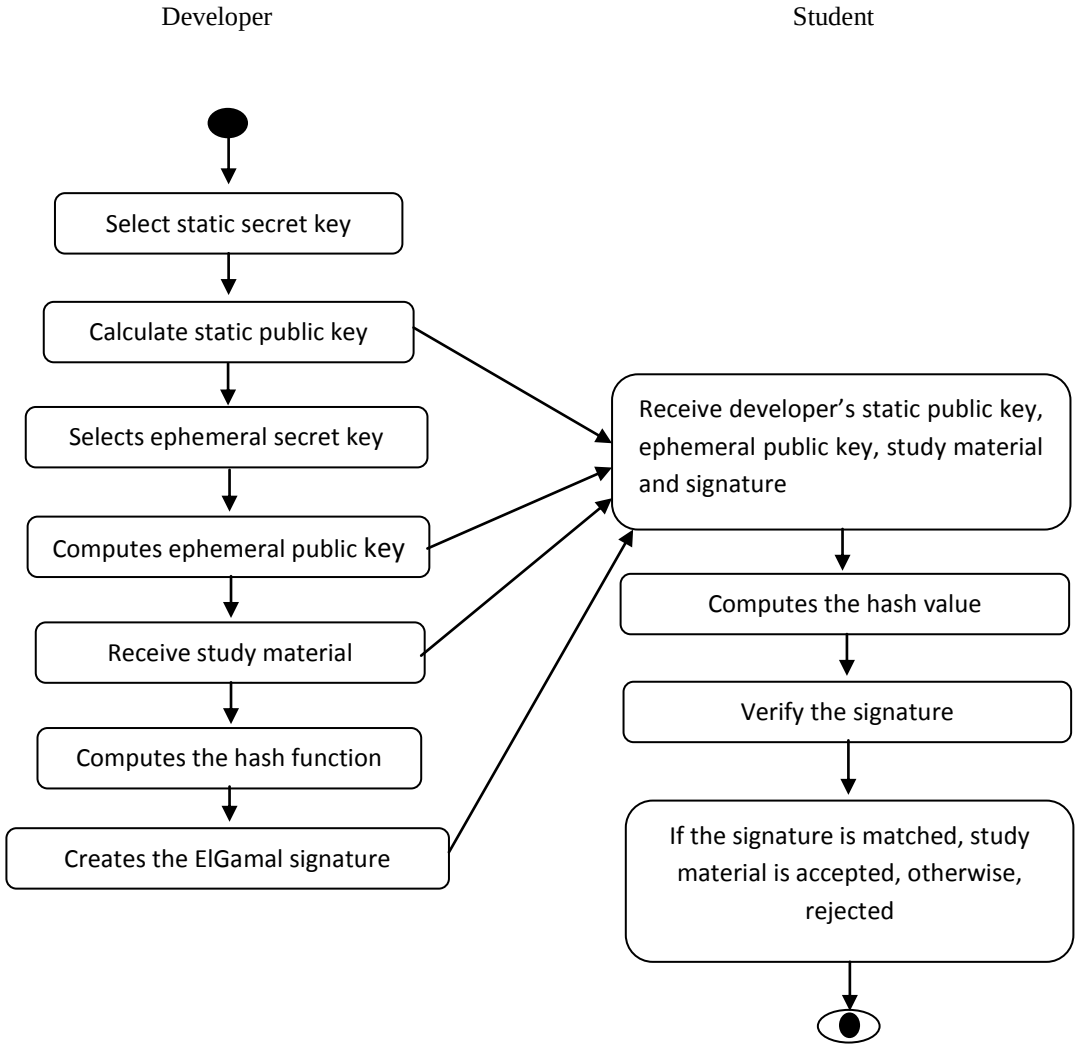

Fig.1: Activity diagram for sending study material from developer to student using ElGamal Digital Signature

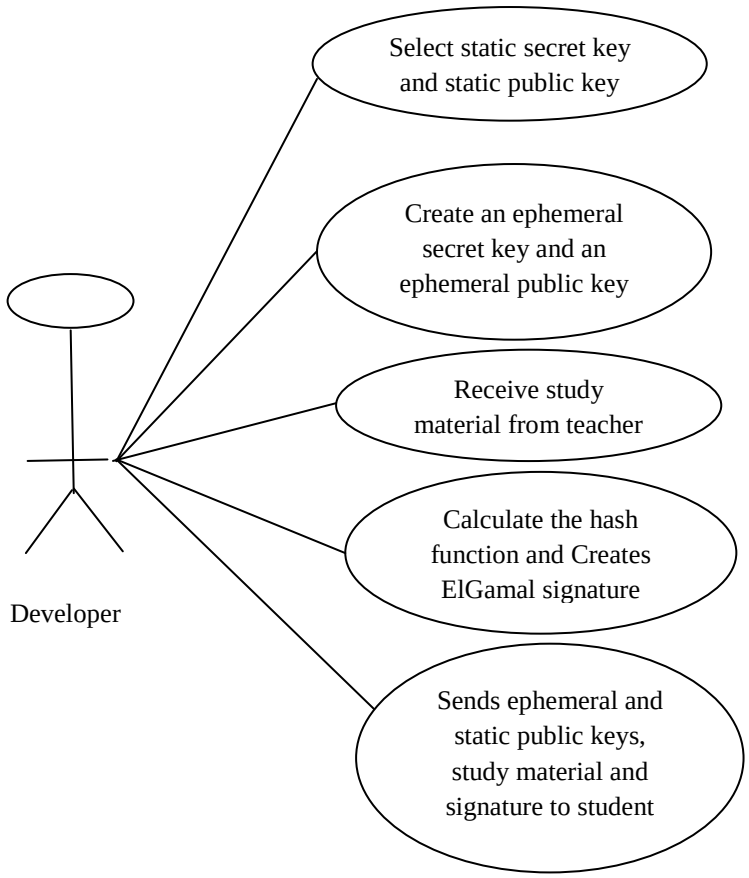

Fig.2: Use case diagram for ElGamal signature generation

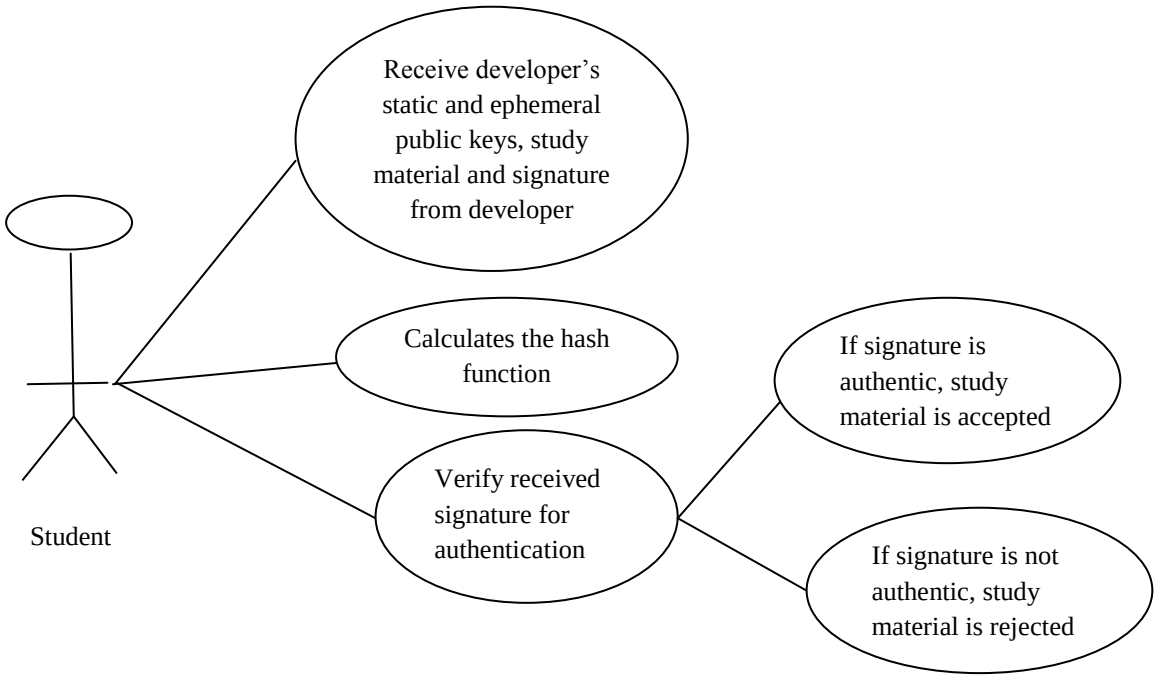

Fig.3: Use case diagram of ElGamal signature verification

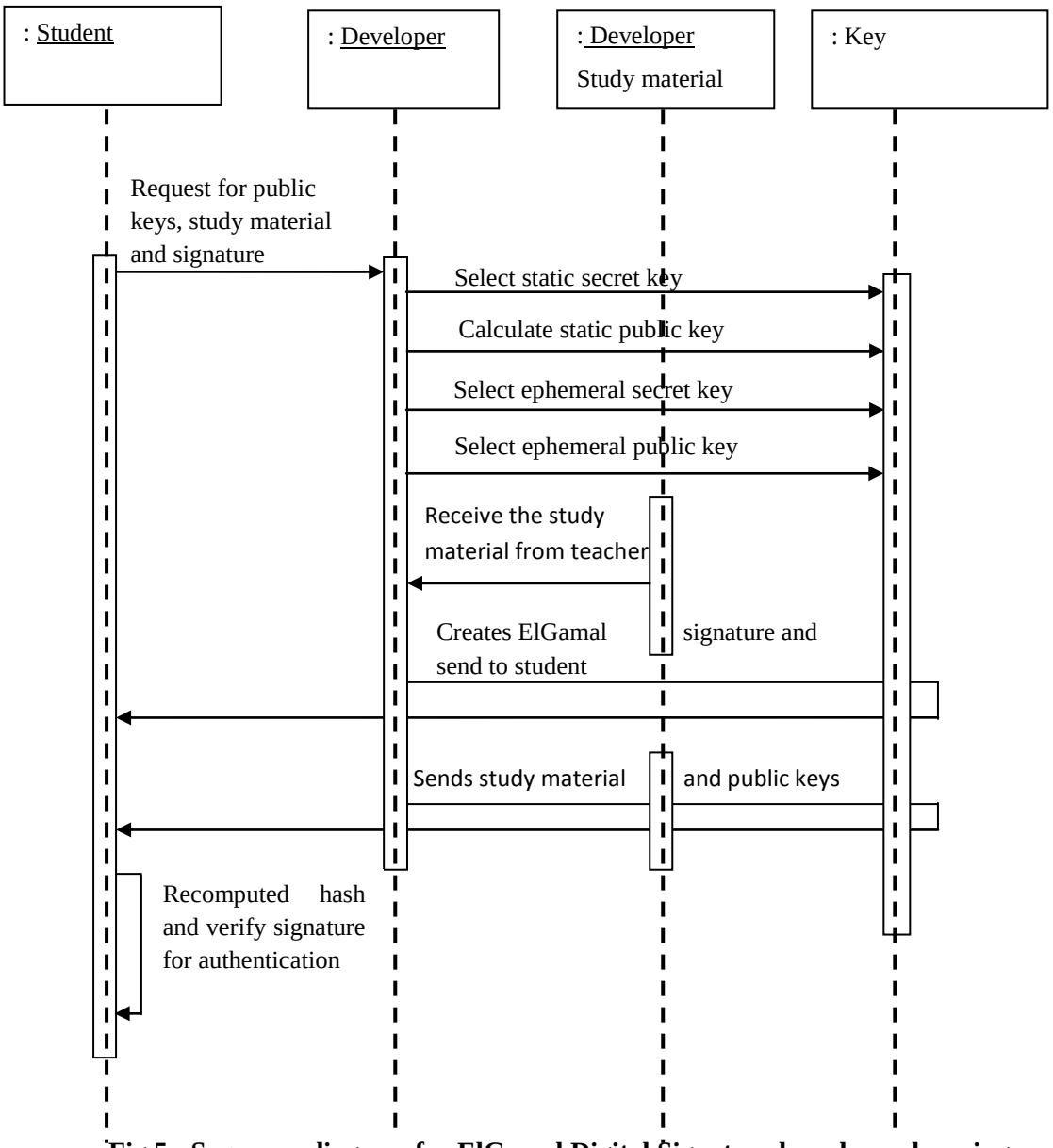

Fig.5: Sequence diagram for ElGamal Digital Signature based on e-learning system

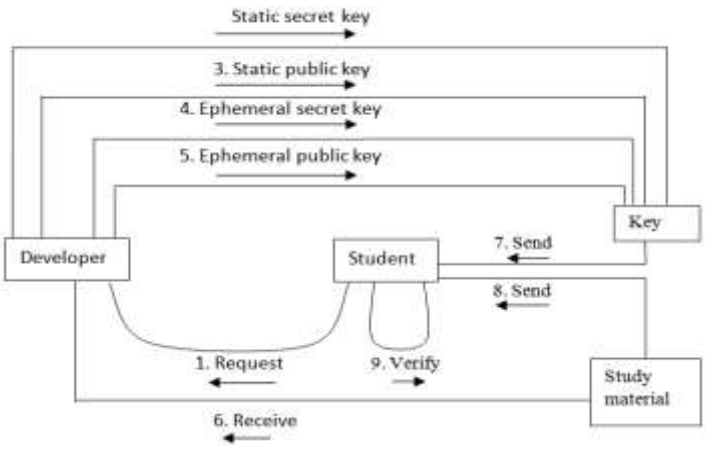

Fig.6: Collaboration Diagram for sending study material using ElGamal Digital Signature in e-learning system

IV CONCLUSION

The proposed models, we use in this paper, are utilizing the benefits of Object Oriented Programming. This object oriented approach of ElGamal Digital Signature Algorithm can be used for other types of transmissions in e-learning system, like transmission of registration certificate, admit card, score card etc. This approach is also applicable for secure transmission in other online systems, like e-banking, e-commerce, e-governance etc.

REFERENCES

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

[2] Karforma S. and Ghosh A., "Object Oriented Modeling of SSL for secure information in E-learning", ICCS-2013, Department of Computer Science, The University of Burdwan, West Bengal, India, pp 62-66, September, 2013

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

[4] Karforma S. and Nikhilesh B., "Risks and Remedies in E-learning System", International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.1, pp 51-59, January, 2012

[5] Karforma S. and Nikhilesh B., "Object Oriented Modeling of Secured E-Assessment System", International Journal of Scientific & Engineering Research Volume 3, Issue 8, August, 2012

[6] Gupta K.S. and Kuriachan K.J., "Issues and Solutions in E-learning System", International Journal in Multidisciplinary and Academic Research (SSIJMAR), Vol. 2, No. 2, March 2013

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

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

[9] Karforma S. and Banerjee S., "Object Oriented Modeling of Digital Certificate in E-learning", International Journal of Emerging Trends and Technology in Computer Science, Volume-3, Issue-5, September-October 2014, pp: 205-211

[10] Graff, J.C., "Cryptography and E-commerce", John Wiley & Sons, New York (2001)

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

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