Object-oriented Modeling of IDEA for E-learning Security

Ambalika Ghosh and Sunil Karforma

Abstract E-learning system involves an open participation of student, teacher, and administrator among different regions in the world. Due to the use of Internet as electronic communication media, there are several types of risks and threats such as alternation or deletion of student's marks given by a teacher may hamper the E-learning environment in different ways. To implement privacy and confidentiality of the information, we must use suitable encryption technique. In this paper, we have proposed an object-oriented modeling of international data encryption algorithm (IDEA) for implementation of privacy and confidentiality of information which would be communicated between teacher and student at the time of viewing marks for a subject. For an efficient design, we use UML-based approach.

Keywords E-learning · Encryption · Privacy · Security · Confidentiality · IDEA · Object-oriented model · UML

1 Introduction

The use of information and communication technology (ICT) as a public communicating tool for delivery of services electronically in the public and private sectors has changed the scenario of every operation of the system. This has resulted in emergence of E-learning system [1, 2]. Nowadays, students may not be confined to any conventional school, college, and university campuses only to get their higher education. They may pursue their studies explaining the services of E-Learning [3, 4]. But, most challenging part of E-Learning system is to encrypt the information in public media such as network or Internet [5]. To do so, we have

A. Ghosh (✉) · S. Karforma
Department of Computer Science, Burdwan University, Burdwan, India
e-mail: ambalika_ghosh@yahoo.co.in

S. Karforma
e-mail: dr.sunilkarforma@gmail.com

D. Mandal et al. (eds.), *Intelligent Computing and Applications*,
Advances in Intelligent Systems and Computing 343,
DOI 10.1007/978-81-322-2268-2_12

applied the international data encryption algorithm (IDEA) in object-oriented design. IDEA avoids the use of any lookup tables [6].

E-learning is constructed in a variety of contexts [7], such as online examination, online admit card issue, online payment, and online result that utilize information communication technology (ICT) to promote educational interactions between students, faculties, and administrators [8, 9].

In this paper, we have wrapped IDEA in an object-oriented model for security [10] of information which is needed during view of marks for any subject of a student given by a faculty and published by admin electronically.

In our proposed system, each student is needed to enter his/her roll number, subject code, and subject name to view the marks. Faculty generates the mark slip for the respective subject of the particular student. This passing of information can be possible through admin. This roll number or marks may be altered by hacker causing insecure system. Using IDEA, an encryption–decryption technique is easily possible for protecting the unwanted alternation of roll number or marks from hacker [11].

In Sect. 2, we give a short outline about IDEA. In Sect. 3, we have outlined how object-oriented modeling can be used to implement IDEA for security of information during view marks of a subject. In this paper, we designed and embodied the UML [12–14]-based object-oriented model of E-learning system using IDEA. For an efficient design, we have used use case diagram (Fig. 2), class diagram (Fig. 3), and sequence diagram (Fig. 4) to represent the required class representation for programming purpose in the E-learning system [15, 16] (Fig. 1).

2 IDEA—An Overview

In cryptography [17], the IDEA [6], originally called improved proposed encryption standard (IPES), is a symmetric-key block cipher. The IDEA encryption algorithm provides high-level security not based on keeping the algorithm a secret, but rather upon ignorance of the secret key. It is fully specified and easily understood and also available to everybody. It can be economically implemented in electronic component such as VLSI chip and can be used efficiently. It is also patent protected to prevent fraud and piracy [4].

IDEA operates on 64-bit blocks using a 128-bit key and consists of a series of eight identical transformations (a *round*, see the illustration) and an output transformation (the *half round*). The processes for encryption and decryption are similar. IDEA derives much of its security by interleaving operations from different groups—modular addition and multiplication, and bitwise eXclusive OR (XOR)—which are algebraically “incompatible” in some sense. In more detail, these operators, which all deal with 16-bit quantities, are discussed below [18]:

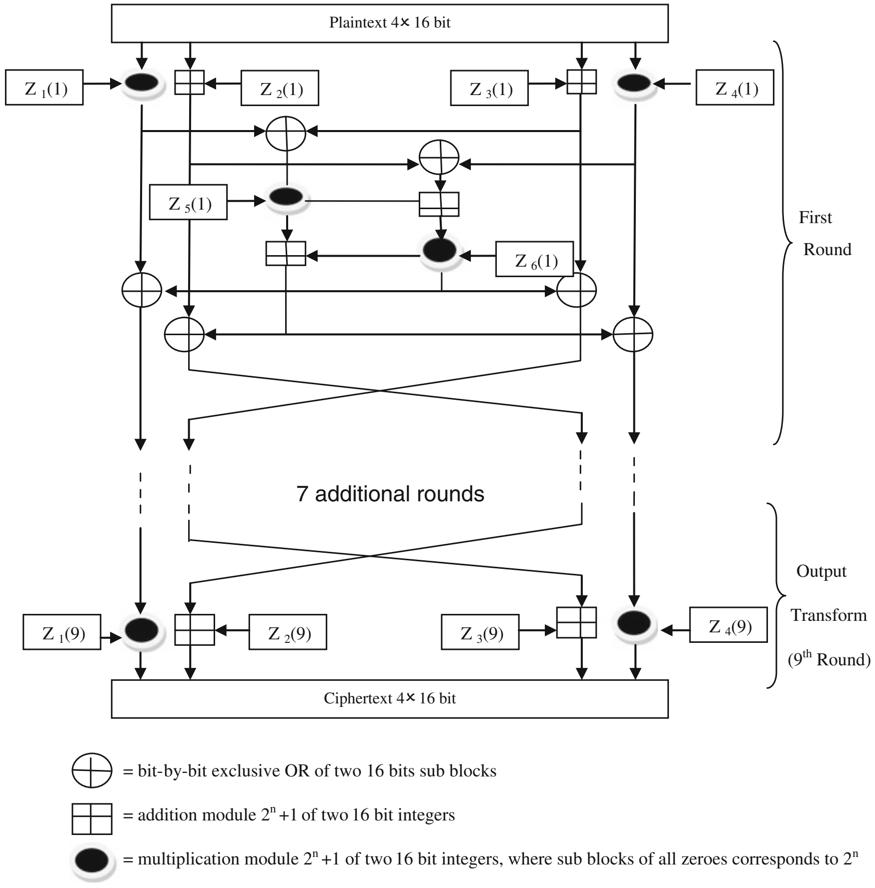
Plaintext 4× 16 bit
Z 1(1)
Z 2(1)
Z 3(1)
Z 4(1)
Z 5(1)
Z 6(1)
First Round
7 additional rounds
Output Transform (9th Round)
Z 1(9)
Z 2(9)
Z 3(9)
Z 4(9)
Ciphertext 4× 16 bit
= bit-by-bit exclusive OR of two 16 bits sub blocks
= addition module 2n +1 of two 16 bit integers
= multiplication module 2n +1 of two 16 bit integers, where sub blocks of all zeroes corresponds to 2n

Fig. 1 The IDEA structure

- Bitwise eXclusive OR (denoted with a blue circled plus $\oplus$).
- Addition modulo 2^{16} (denoted with a green boxed plus $\boxplus$).
- Multiplication modulo $2^{16} + 1$, where the all-zero word (0 × 0000) in inputs is interpreted as 2^{16} and 2^{16} in output is interpreted as the all-zero word (0 × 0000) (denoted by a red circled dot $\odot$).

After eight rounds comes a final “half round,” this is for output transformation.

3 UML-based Proposed Object-oriented Modeling

To depict our proposed system using UML, we only consider the use case diagram, class diagram, and sequence diagram.

3.1 Use Case Diagram

In the use case model, we can see that there are three types of objects such as student, faculty, and admin who are involved mainly in View Marks use case. In View Marks, let a student enter his/her roll number, subject code, and subject name to view his/her marks in that subject and the faculty provides the marks to him. It is necessary to protect the roll number and marks from any unwanted alternation in the public medium.

This View Marks may be subdivided into three use cases: key scheduling, encryption, and decryption.

In key scheduling, 128-bit key is processed that is used for encrypting the student's roll number and marks given by faculty.

In encryption, the information is encrypted through a repeated process of eight full round and one half round transformations.

In decryption, the encrypted information such as roll number and marks must be decrypted so that user can read correct message.

Use case model of the proposed E-learning system is shown in Fig. 2.

(1) **Key scheduling**
The 64-bit plaintext block is partitioned into four 16-bit sub-blocks: X_1, X_2, X_3, and X_4, since all the algebraic operations used in the encryption process operate on 16-bit numbers. Again, six 16-bit key sub-blocks: Z_1, Z_2, Z_3, Z_4, Z_5, and Z_6 from the 128-bit key are generated for each of eight rounds. Since a further four 16-bit key sub-blocks are required in the final half round for the subsequent output transformation, a total of 52(=8 * 6 + 4) different 16-bit sub-blocks have to be generated from the 128-bit key.

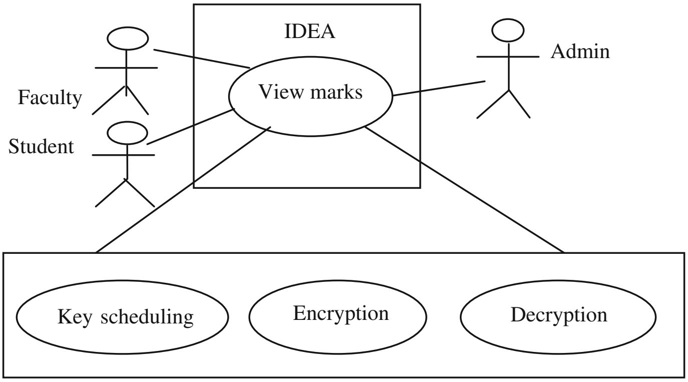

Fig. 2 Use case model of E-learning system

Scenario 1: *Mainline sequence*

1. IDEA system: Produces 52 16-bit sub-keys from 128-bit key using some steps that are given below:

   - First, the 128-bit key is partitioned into eight 16-bit sub-blocks which are then directly used as the first eight key sub-blocks.
   - The 128-bit key is then cyclically shifted to the left by 25 positions, after which the resulting 128-bit block is again partitioned into eight 16-bit sub-blocks to be directly used as the next eight key sub-blocks.
   - The cyclic shift procedure described above is repeated until all of the required 52 16-bit key sub-blocks have been generated.

(2) **Encryption**

There are fourteen steps of a complete round to encrypt data using IDEA. These fourteen steps will be repeated for eight rounds, and then a half round will be performed [19].

Scenario 1: *Mainline sequence*

1. Student: Enters his/her roll number, subject code, and subject name for viewing marks to faculty.
2. IDEA System: Accepts information and encrypts it using fourteen steps given below [1]:

   - Multiply X_1 and the first sub-key Z_1
   - Add X_2 and the second sub-key Z_2
   - Add X_3 and the third sub-key Z_3
   - Multiply X_4 and the fourth sub-key Z_4
   - Bitwise XOR the results of steps 1 and 3
   - Bitwise XOR the results of steps 2 and 4
   - Multiply the result of step 5 and the fifth sub-key Z_5
   - Add the results of steps 6 and 7
   - Multiply the result of step 8 and the fifth sub-key Z_6
   - Add the results of steps 7 and 9
   - Bitwise XOR the results of steps 1 and 9
   - Bitwise XOR the results of steps 3 and 9
   - Bitwise XOR the results of steps 2 and 10
   - Bitwise XOR the results of steps 4 and 10

   For every round except the final transformation, a swap occurs and the input to the next round is given as: Concatenation between result of step 11, result of step 13, result of step 12, and result of step 14 which becomes $X_1X_2X_3X_4$, the input for the next round.

After round 8, a ninth half round final transformation occurs:

- Multiply X_1 and the first sub-key Z_1
- Add X_2 and the second sub-key Z_2
- Add X_3 and the third sub-key Z_3
- Multiply X_4 and the fourth sub-key Z_4

The concatenation of the block is the output.

3. IDEA system: Transfer the output encrypted data through the public medium to the admin site.

(3) **Decryption**

The decryption method is same as encryption algorithm except that key scheduling is slightly different. Each of the 52 16-bit key sub-blocks used for decryption is the inverse of the key sub-block used during encryption in respect of the applied algebraic group operation.

Scenario 1: *Mainline sequence*

1. IDEA system: Accepts the encrypted data from student side and decrypts the data in same way which is used in encryption use case but decryption key is constructed in some reverse fashion.
2. IDEA system: Provides the decrypted original information made by student to admin.

Scenario 2:

1. Admin: Sends the received information to faculty
2. Faculty: Gives the marks according to information

3.2 Class Diagram

The given Fig. 3 demonstrates the organization of class hierarchy showing how a student can view his/her marks of a particular subject given by a faculty with the help of admin using IDEA in object-oriented approach [16].

Class hierarchy of the proposed E-learning system is shown in Fig. 3.

The necessary class diagram for the use of IDEA in E-learning security is given below:

The required four types of classes are: student, faculty, admin, and IDEA system.

Class Student: Some variables are-roll_no, sub_code, sub_name, and methods are- input(), display(), setmsg(), receiveinfo()

Class Faculty: Some variables are- Fid, name, subject and methods are- input(), display(), marks()

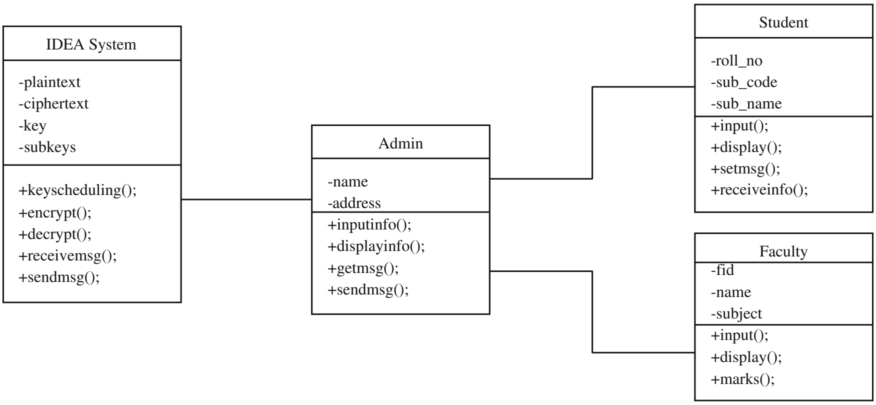

Fig. 3 Class hierarchy diagram of E-learning system

Class Admin: Some variables are- address, name, and methods are- inputinfo(), displayinfo(), getmsg(), sendmsg()
Class IDEA System: Some variables are- Plaintext, Ciphertext, Key, Subkeys and methods are- keyscheduling(), encrypt(), decrypt(), receivemsg(), sendmsg()

3.3 Sequence Diagram

A sequence diagram shows interaction among objects as a two-dimensional chart [11]. Here, we only describe the steps that are needed to encrypt and decrypt any

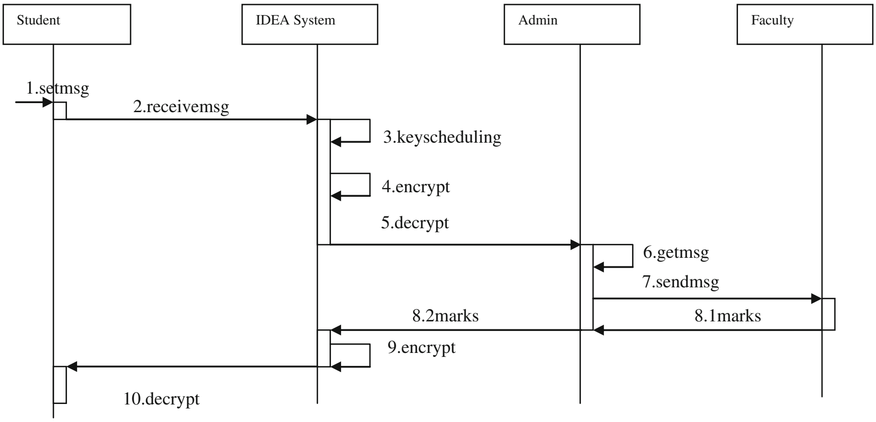

Fig. 4 Sequence diagram of view marks in E-learning system

information providing by student and faculty with the help of administrator during view marks using IDEA algorithm in E-learning system with the help of sequence diagram as in Fig. 4.

4 Conclusion

To ensure the privacy and confidentiality of information, suitable encryption technique is necessary for E-learning security [15, 20]. The proposed system is implementing security of information in E-learning employing IDEA in which encryption and decryption of any content is done very efficiently compared to other algorithms. With implementation of IDEA wrapped in object-oriented model using UML, we can realize a level of safety, reliability and hence trust in the mind of huge number of students. This proposed system will help to reuse the code design [21]. An effortless secure transfer and exchange of data between the faculty and student along with other component of the system become easy. The level of security of the proposed system can be improved further by the efficiency measurement of object-oriented metrics can be considered as the future scope of this work.

References

1. Ghosh, A., Karforma, S., Singh, A.K.: Object oriented modeling of E-learning system. In: Proceedings of ICCS-2010, pp. 103–111. ISBN: 93-80813-01-5
2. Singh, A.K., Mukhopadhyay, S., Ghosh, A., Karforma, S.: Object oriented design of E-library for E-education. In: Proceedings of ICCS-2010, pp. 163–167. ISBN: 93-80813-01-5
3. Weippl, E.R.: Advances in E-Learning, Springer, Berlin
4. Chang, H.S.: International Data Encryption Algorithm, CS-627-1, Fall (2004)
5. Schneier, B.: Applied Cryptography, 2nd edn. Wiley, New York (2008)
6. Roy, A., Banik, S., Karforma, S., Pattanayak, J.: Object oriented modeling of IDEA for E-governance security. In: Proceedings of ICCS-2010, pp. 263–269. ISBN: 93-80813-01-5
7. Eibl, C.J., et al.: Development of E-learning design criteria with secure realization concepts. In: Mittermeir, R.T., Syslo, M.M. (eds.) ISSEP 2008, LNCS 5090, pp. 327–336. Springer, Berlin (2008)
8. Ghosh, A., Karforma, S.: Object oriented modeling of digital certificate based E-learning system. In: Proceedings of RHECSIT-2012, pp. 103–111. ISBN: 978-81-923820-0-5
9. Ghosh, A., Karforma, S.: Object oriented modeling of digital certificate for secure transaction in E-banking. In: Proceedings of NaCCS-2012, pp. 103–111. ISBN: 93-80813-18-X
10. Jamwal, D., Bhat, A.: E-Learning security Concepts. www.google.com/ejel.com
11. Ghosh, A., Karforma, S.: Object oriented modeling of SET for security in E-learning. Int. J. Adv. Res. Comput. Sci. Softw. Eng. **4**(8) (2014). ISSN: 2277-128X
12. Mall, R. (ed.): Fundamentals of Software Engineering, 2nd edn. PHI Publications, New Delhi
13. Aggarwal, K.K., Singh, Y.: Software Engineering, revised 2nd edn. New Age International Publishers, New Delhi
14. Hawryszkiewyez, I.T.: Introduction to System Analysis and Design, 2nd edn. PHI Publication, New Delhi

15. Ghosh, A., Karforma, S.: Object oriented modeling of SSL for secure information in E-learning. In: Proceedings of ICCS-2013, pp. 62–66. ISBN-13: 978-9-35-134273-1, ISBN-10:9-35-134273-5
16. Ghosh, A., Karforma, S.: Object oriented modeling of DSA for authentication of student in E-learning. Int. J. Sci. Res. **3**(7) (2014)
17. Graff, Jon C.: Cryptography and E-commerce. Wiley, New York (2001)
18. Kahate, Atul: Cryptography and Network Security, 2nd edn. Mc Graw Hill, New York City (2003)
19. C code implementation of IDEA algorithm. Available at http://www.koders.com/c/fid43C02E2565B7947584D23C36A6C32E198E06C.aspx?s=des
20. Ghosh, A., Karforma, S.: An UML based design of E-learning system using digital certificate. Orient. J. Comput. Sci. Technol. **5**(2), 257–262 (2012)
21. Lafore, R.: Object Oriented Programming in C++, 4th edn. Techmedia, New Delhi