Protection the Copyright in E-Education Process

Dr. Osama Amin Marie AL – Quds Open University e-mail: omarie@qou.edu	Dr. Khader Muspah Titi King Khaled University e-mail: drkhadermuspah@gmail.com

***Abstract*— Today's world, becoming more competitive, every day is demanding from organization the flexibility to adapt themselves to the permanent situations of market change, readiness for ongoing development and guarantee of the quality of products and services. At the same time, Internet, after being used initially as a great source of information exchange, rapidly happen to be used as an important means for providing learning and training services across the whole world. However, such advances have caused series of information system security issues to the face. The complexity of Internet infrastructures, such as in a Web services distributed system, can hide the potential risks of so many security issues, and subsequently become disadvantageous to e-learning users, applications and institutions.**

The main aim of this research is to provide an approach to protect the copyright of e-courses materials in the e-learning system. This new model will be deployed to protect the copyright of e-courses material from unauthorized distribution, and to protect the e-course material from being modified while transit. The design of model is provided to make the e-learning process more secure for both organization and students alike.

Key words: security, e-learning, encryption, RSA

1. Background to the Study

Information is now the most valuable resource in the world. Whether it is a personal letter, documents or an industrial secret, all information has a worth to somebody. This research considers issues of security and privacy for such information.

The world in which we exist is decreasing because virtually every person can be electronically connected either by satellite communication, Internet, electronic mail (e-mail), or a conventional telephone in a global village network that transcends geographic boundaries. Progress in communication and information technologies (CIT) has brought extraordinary changes to the whole of our world, which transforms us toward an information civilization. As we shift into the twenty one century, we discover that our dependence on information technology (IT) is increasing dramatically. IT continues to develop and continue to affect all parts of our civilization: government, educational institutions, medical, businesses and individuals.

Today educational institution and other commercial and non commercial organization cannot conduct its business without their dependence on complicated information technology infrastructures. Civilizations are competing to build information technology infrastructures to gain a competitive advantage. Organizations need these information technology infrastructures not only for their communication needs, but also for conducting there business activities.

In fact, there are quite a number of security issues in e-education system, for instance, user authentication and access control, non-repudiation for critical actions like course registration, examinations and assignment delivery, course tuition fee payment, confidentiality of user personal information, and course material copyright protection.

The security concerns may differ faintly depending on the type of courses offered by an organization. However, the most disturbing issue in e-learning system might be the copyright protection issue, which is essential to all kinds of electronic courses (e-course). This security issue may have the following picture:

One of the registered students violates the copyrights protection of the course materials by passing the course materials to other organization or to other non-registered students. Regularly, the organization that provides the course materials depends on the registration fee to keep up and maintain all activities and operations of the organization. Therefore, copyright protection violation rigorously exposes the income of the organization at risk.

New information and communication technologies have become major resources and basis for learning in higher education. Technologies have several potentials to support different instructional strategies and provide an efficient way of delivering e-course material and improving comprehension. The contemporary universities need to increase lifelong learning opportunities to its students any time, any place and at any rate to be successful in the global educational marketplace [1].

The use of e-leaning in the educational process has grown significantly in the last few years, however, it is a relatively insecure, hence, most educational organization haven't yet taken into considerations or any new strategy for securing e-learning process [2]. Implementing e-learning is complex. Implementing e-learning is about project management, change management and risk and security management [3]. Additionally, the topic e-learning or e-education is having much attention especially because world-class universities such as MIT, Harvard and Stanford in the United States and Oxford in the United Kingdom are implementing it [4].

E-learning can be defined as the online delivery of information for purposes of education, training and knowledge management [5]. This definition means that the Internet and computer will be used in the e-learning process. Thus, e-learning is more complex and intertwined the opportunities for intrusion and attack. E-learning security involves more that just preventing and responding to cyber attacks and intrusion, it involves copyright protection, integrity, availability, non-repudiation, authentication and authorization.

The use of Internet application in higher education and in most organizations is being optimistic. The reasons are various and complex and lecturers in educational institution are under high pressure to learn and adopt this latest technology to support their teaching and their students' learning.

Using the Internet in the educational process is very beneficial to both students and educational institutions. The core reason why Internet are gaining so much interest lies on its ability of joining and interoperating heterogeneous communities. A lot of users who use different platform can communicate with each other easily on the Internet. The Internet and its potential and capabilities are very attractive; however, the current standards behind the technology need to be justified very carefully before deploying the Internet for very sensitive applications such as e-learning system. Since, default Internet transactions are unencrypted and unsecured, and they can establish the potential for disaster and failure [6].

Computer security is the shield that all types of organizations use to protect sensitive, commercial and classified information from unauthorized users. A break of this shield has implications that go far beyond any financial form that could be assigned to such an intrusion or adversary. The concepts of computer security are practically basic in nature, however, implementing security in a continually changing technological environment is a big challenge, but it has to be met by organizations, individual users and governments. Therefore, the threats in computer security must be understood.

This research presents the design and implementation of a global e-learning system that provides the basic security requirements including confidentiality, integrity, non-repudiation, replay protection and the most important entity authentication.

2. Cryptographic Techniques

Data communication is an important part of our living. Therefore, protection of data from misuse is essential. A cryptosystem defines a pair of data transformations called encryption and decryption. Encryption is applied to the plain text which is the data to be communicated to produce cipher text which is the encrypted data using encryption key. Decryption uses the decryption key to convert cipher text to plain text or the original data.

With strong encryption, computer users can send confidential contracts by email, or safely store corporate strategy on a notebook, or carry home spreadsheets on a floppy disk. The encryption software may even be free.

To improve the protection mechanism Public Key Cryptosystem was introduced in 1976 by Whitfield Diffe and Martin Hellman of Stanford University [7]. It uses a pair of related keys one for encryption and other for decryption. One key, which is called the private key, is kept secret and other one known as public key is disclosed to the public.

The message is encrypted with public key and can only be decrypted by using the private key. So, the encrypted message cannot be decrypted by anyone who knows the

public key and thus secure communication is possible. RSA [8] (named after its authors Rivest, Shamir and Adleman) is the most popular public key algorithm. In relies on the factorization problem of mathematics that indicates that given a very large number it is quite impossible in today's aspect to find two prime numbers whose product is the given number. As we increase the number the possibility for factoring the number decreases. Thus, we need very large numbers for a good Public Key Cryptosystem.

Authentication, confidentiality and data integrity can be addressed by studying cryptographic techniques [9]. In using such techniques, it is predictable that information in transmit through the Internet can bypass through various computers before it arrives its target. A malicious user of any of the intermediary computers can monitor the Internet traffic, eavesdrop, intercept, change or replace the data through its entire path. Cryptographic techniques can be used to protect these data. Encryption is the process that makes information indecipherable (cipher text) unless having a decryption key [10]. It uses mathematical algorithms and processes to convert intelligible plain text to unintelligible cipher text and vice versa [11]. It can, therefore, reduce risks from an eavesdropping on a network.

Cryptography is one of the most important tools that enable networks and Internet applications because cryptography makes it possible to protect electronic information. The effectiveness of this protection depends on a variety of mostly unrelated issues such as cryptographic key size, protocol design, and password selection.

.

3. The Proposed Model (SeS)

The secure e-learning System (SeS) is a set of software modules designed so as to work together to protect the copyright of e-course material and to make the e-learning process more secure and trustee for organization and student a like. These modules are shattered amongst different components.

The proposed design model (SeS) follows the three-tier architecture model. This model breaks the software application into three different layers or tiers as shown in figure 1 below:

- Entity Student
- Entity Server
- Database services

Each layer has its own goals and design constraints and will be briefly explained in following sections.

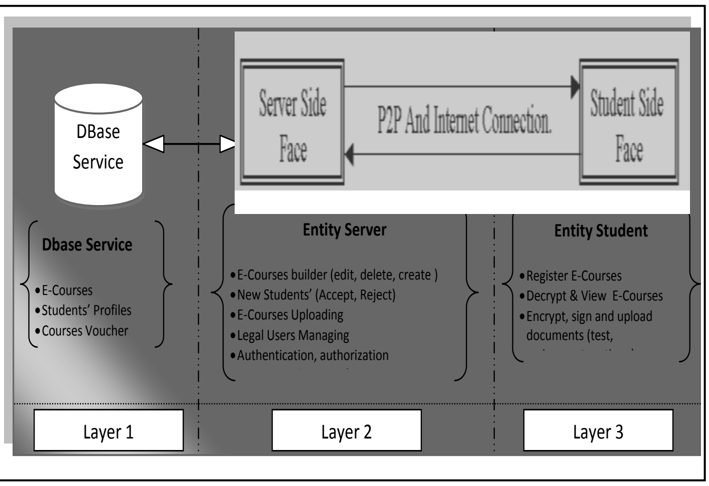
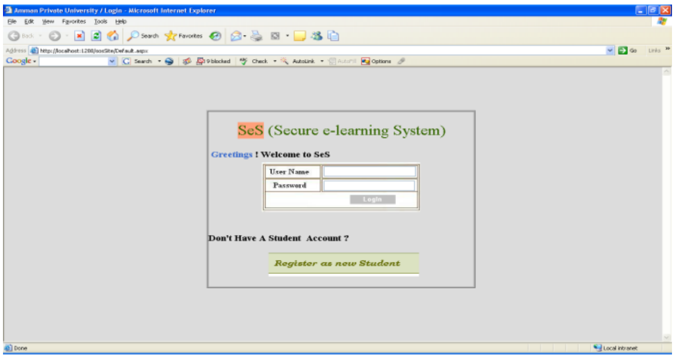


Figure 1: Faces of SeS Model, own model

4. SeS Organization and Structure

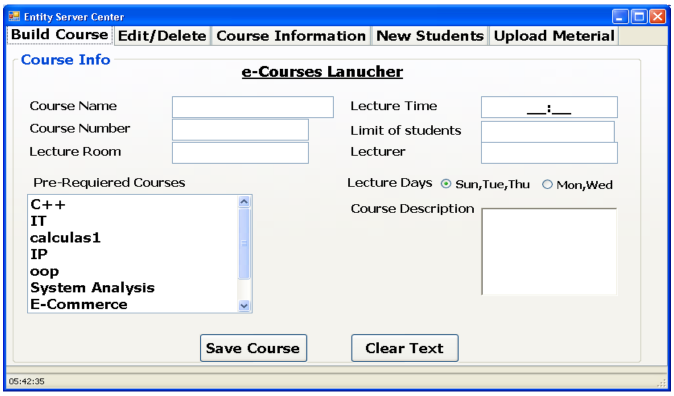
The proposed model is organized to be employed in a traditional classroom using a LAN (Local Area Network) network or a WAN (Wide Area Network) connected using the standard TCP/IP protocol with an entity server representing the educational institution and an entity student representing the student workstation with a piece of software installed in it. The proposed system will start when an entity student communicate with the entity server to register as a new student using the educational institution Web site published on the Internet (see figure 2). The entity server, (see figure 3), will accept the student information and send to him, using his e-mail, an attached file contains a username and a password that he/she can use to login into the site and download a software (Entity Student), (see figure 4), which he/she need to install into his computer so that he/she can use to register courses, add and remove courses and change his/her password. Additionally, with this software (Entity Student SW) the student can encrypt and decrypt files, view course materials and he/she can also send digital signed files using his/her public key to the instructor such as assignments, test, questions, etc.


Amman Private University / Login - Microsoft Internet Explorer
SeS (Secure e-learning System)
User Name
Password
Login
Register as new Student

Greetings ! Welcome to SeS

Don't Have A Student Account ?

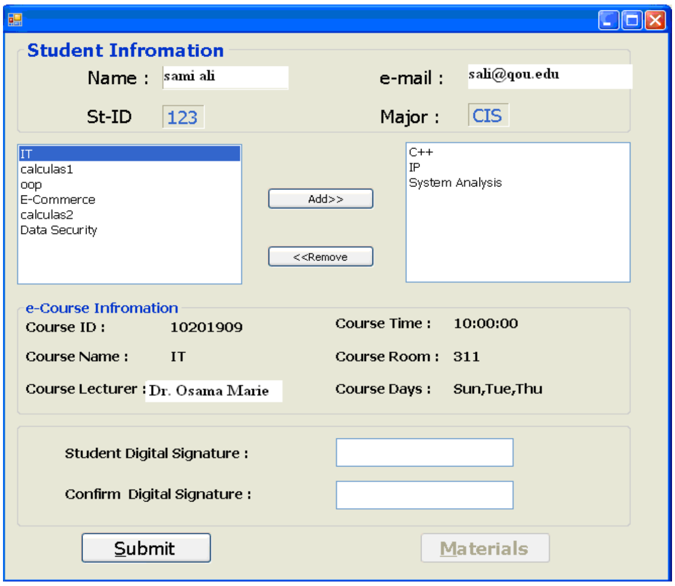
Figure 2: login and registration screen in the SeS system



Lecture Days ● Sun,Tue,Thu ○ Mon,Wed

Pre-Requiered Courses: C++, IT, calculas1, IP, oop, System Analysis, E-Commerce

Figure 3: entity server solution



Name : sami ali

e-mail : sali@qou.edu

St-ID 123

Major : CIS

IT, calculas1, oop, E-Commerce, calculas2, Data Security

C++, IP, System Analysis

Course ID : 10201909

Course Time : 10:00:00

Course Name : IT

Course Room : 311

Course Lecturer : Dr. Osama Marie

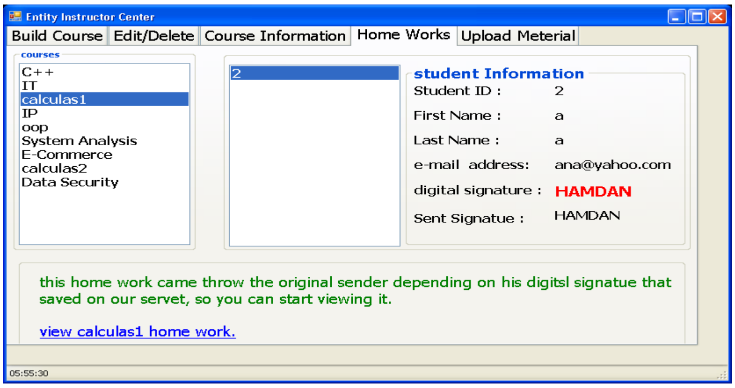
Course Days : Sun,Tue,Thu

Student Digital Signature :

Confirm Digital Signature :

Figure 4: entity student software

Instructor in the educational institution could use a software called entity instructor to communicate with his/her students, send to them assignment, notes, receive from entity student assignment, check the digital signature of the entity student, and use this software to build and launch new e-course materials(see figure 5). However, when the entity student communicates with the entity server, an authentication scheme will be verified to insure security. These authentication scheme will include a precise time test, private and public key matching. When the entity server successfully completes the authentication scheme verifications, the entity student can be allowed to access the system and get what it requested. Otherwise the entity server will not allow the entity student to get through the system.



courses: C++, IT, calculas1, IP, oop, System Analysis, E-Commerce, calculas2, Data Security

2

Student ID : 2

First Name : a

Last Name : a

e-mail address: ana@yahoo.com

digital signature : HAMDAN

Sent Signatue : HAMDAN

this home work came throw the original sender depending on his digitsl signatue that saved on our servet, so you can start viewing it.

view calculas1 home work.

Figure 5: entity instructor software solution

This model, SeS, proposes a solution for the security problem of the e-learning system. The SeS based on the eXC model by Yau [2]. The eXC model proposed a solution for the copyright protection. The model uses the hardware configuration of the student's computer to protect the copyright of the organization's recourses materials. It supposes to provide a mechanism to protect the learning material from unauthorized distribution, and shows how this mechanism can be integrated in the operation model of online learning e-course providers. However, this model for Yau [2] is not fully protected. Hence, the student is able to do the copying or saving of the e-material using copy or save commands within the operating system. However, if the content of the e-Course includes many different files, the student might only be able to save one Web page at a time [12], and would have to call up the save function many times in order to get a complete copy of all the files of the e-Course. Or, better yet, the student or maybe an opponent may use some commands line based Web client that is able of downloading Web content recursively for example "wget" [13], which can significantly speed up the process of illegally copy the material.

This type of attack to a copyright protection system is very common, and can beat the system by creation illegal copies of the e-content. Therefore, this model that proposed by Yau need to be modified and optimized to prevent this type of making illegal copy of the e-content of the courses.

Additionally, this model for Yau used the commercial SET (Secure Electronic Transaction) to perform all activities related to encryption and decryption, which make this model incomplete and ambiguous.

What the researcher is proposing will prevent student from using all commands used to save, copy, or move the contents of e-course materials. The student will not even select the text or used the right click button of the mouse, he/she wont be able to use all control functions such CTRL + C or CTRL + X. Additionally, with this proposed system every thing will be shown and briefly explain in minutes details, the encryption, decryption, protocol and all scheme used will be explained widely. The following sections contain more detailed description of the design and software implementation for each of the entities software that involved in the e-learning process.

5. The Entity Server (server side face)

The SeS model software consists of the server side application (entity server) that performs the business and education logic of the system. This software (see figure 2) is the core component of the SeS. It is responsible for performing the requirement for secure electronic transaction of e-course processing at the server level.

The modular approach for the design calls for the separation of work on dedicated servers each has its own functionality. Allocating the work in this approach assures the highest availability of resources and meets the scalability needs. Consequently, the educational institution environment consists of two essential servers: the institution web server and the institution database server. These two servers together form a logical entity which can be called the entity server. The Content of the entity server system is designed for the administrator and instructors to create and to launch e -course materials.

There is a SeS sub-module, called the Course Launcher, residing in the entity server which is used for launching e-course. The entity server is the administration center of the whole platform. It is used for handling student registration, course registration, course payment, managing encryption and decryption, authorization and authentications as well as course materials hosting and downloading.

The entity server is the piece of software that does the entire procedures and operations in the e-learning model, for example is accountable for entity authentication, care of all e-learning procedures and related rules. Therefore, the entity server needs are as follows:

- entity server should be able to achieve entity authentication
- entity server should have sufficient space memory to store the entire databases, queries and solutions.
- entity server should give a time-stamp service to record the process
- entity server should supply concurrent computer links by a wireline technology.

6. Course Voucher and Course Package Process

When the e-course launcher is used to launch the e-course materials, two objects will be created: the course package and the course voucher for each e-course created.

Each course had a course voucher, which contains related information to a specific course such as course name, course number and course contents (index), prerequisite etc. It also contains an encryption key which can be used for decrypting the Course Package. This means that, for viewing the e-course material, student must have both the Course Package and the Course Voucher for the specific e-course. Once the e-Course is successfully launched, the Course Package will be distributed over the network and could be downloaded in an encryption form by entity student.

When legal entity student request to view a specific e-course, several processes have to be done:

1. The course launcher will send the course voucher encrypted using the private key (Kpr) of the specific course concatenation with the course package encrypted with a key to the entity server.
2. The course voucher will be encrypted using the private key of the course (Kpr) and will be stored in the courses database within the database service server.
3. The authorized entity student can download the course voucher, decrypt it using his public key and then can get the key for the specific e-course,
4. Entity student now can use this key to decrypt the course package and eventually view the course material offline using his own computer, (see figure 8).

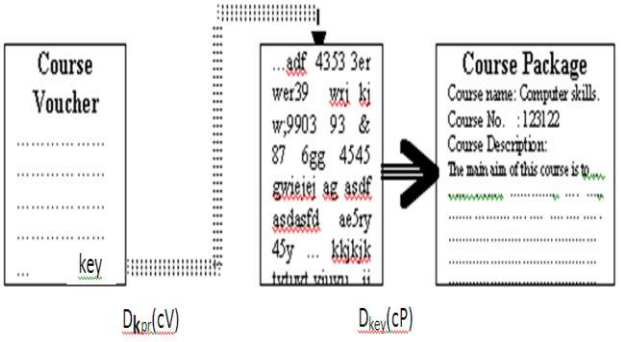


Figure 5: The Mechanism of Viewing The E-course and Contents, own model

7. Digital Signature for Student

Each student completes the registration and the fees payment will be granted a public and private key (Digital Signature), which he/she can use to encrypt documents (Course Voucher, Courses Packages, announcements, courses details, grades, assignments etc.) to send them to the entity server or entity instructor and to decrypt documents, messages or files send to him by the entity server or entity instructor.

The RSA is a public-key cryptosystem has been used to present both encryption and digital signatures (authentication). Digital signatures are generated through entity server, as well as verified. Signatures are generated in conjunction with the use of a private key; verification takes place in reference to a corresponding public key. Each signatory (Registered student) has his own-paired public (assumed to be known to the general public) and private (known only to the student) keys. Because an authorized student using his private key can only generate a signature, the corresponding public key can be used by anyone to verify the signature.

Therefore, a digital signature uses cryptographic technology to create an electronic identifier, but it can be used with any message, whether the message is encrypted or not. Thus, digital signatures can go together with an unencrypted or an encrypted message. Due to these criteria, a digital signature can be trusted and used like a written signature. For example, an entity student can use his digital signature with a private key that he keeps to himself. He then attaches this signature to a document and sends it to the entity server. His private key is mathematically linked to a public key that he posts on the entity server where his public key is stored. The recipient can then retrieve the sender's public key and reverse the process to determine the authenticity of the document.

The process for sending a digitally signed encrypted message is similar. In this case, the sender (entity server) must retrieve the entity student's public key from a public key database. Then uses it to encrypt the document and send it to the student. The recipient then uses his own private key to decrypt the document, and with this mechanism the entity server will be sure that only the recipient student can read it, thus, integrity, confidentiality and authentication will be assured. Additionally, the digital signature provides another advantage, the non-repudiation. In a cryptographic context, the word repudiation refers to the act of disclaiming responsibility for a message (ie, claiming it was sent by a third party). The mechanism strategy in the SeS model insist that the student attach a signature in order to prevent later repudiation, since the instructional organization may show the message to a third party to reinforce a claim as to its origin.

8. Student PC's License (STPCLicense.dll)

Potential student registers, fills the required information (Student Profile), pays fees and sends this information to the entity server using the Web site of the educational institution or any other secure communication channel. The entity server will receive and saved this information in the students' database.

Student now will be ready to register the course(s) needed according to his/her specification using the software installed in his PC. He could invoke the entity server to register the course. The entity server will immediately perform an authentication and authorization process. During the student registration process student's profile will be checked. A digital signature and a private key will be added to the student's profile.

Through the installation, a public key-pair is generated using RSA scheme. A hardware profile copy the hardware (serial number of student PC's motherboard) configuration of the student's computer is also generated. The public key of the key-pair and this hardware profile are both stored inside a file called student PC's License (STPCLisence.dll). Besides, some personal information about the student is also stored in this student PC's License. This makes the STPCL unique to each computer. This License is then sent to the entity server. The entity server will verify this License, assign to it an expiry date, and sign it digitally. The server will send the signed License back to the student's computer. This copy of student PC's license will be stored during the student invocation of the server entity. This student PC's license will be checked when the student request the e-course material for viewing. All communication between the entity student and the entity server will be performed using encryption techniques to guarantee secure transferring of information between the two sides.

9. Requesting and Viewing e-Course

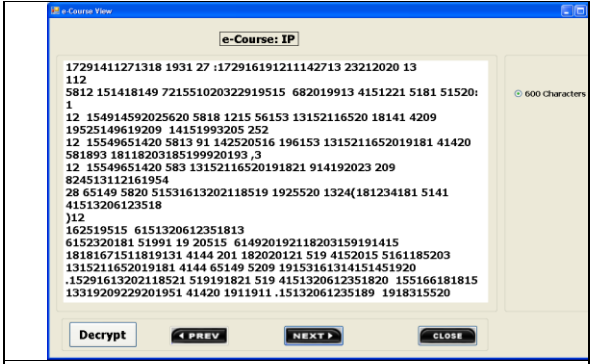
When an entity student invokes the entity server for viewing the course material, the student PC's License will first be examined and checked if this invocation is valid. The student will be allowed to access and have an encrypted copy of the e-course material if and only if the following conditions are satisfied:

1. The student PC's license file has not been expired yet.
2. The student PC's license file had properly signed by the server entity.
3. The software is invoked on the computer on which it was originally installed

During the invocation, a hardware configuration profile of the entity student's PC will be generated to test the current hardware configuration of the entity student's PC. This hardware profile is compared with the hardware profile that had been stored in the entity student PC's License. The third condition will only be meted if the two hardware profiles match.

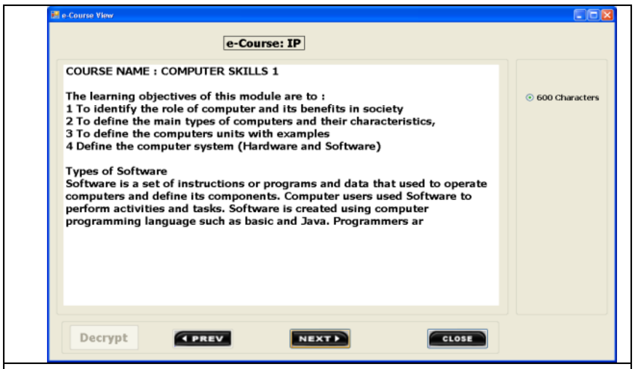
When an entity student registered an e-Course, both the Course Package and the Course Voucher will be under the student's ownership. Since the encryption key to the Course Package is contained in the Course Voucher, the Course Voucher must also be protected on the student's computer. When the Course Voucher is received from the e-learning, it is encrypted with the computer's public key using the RSA asymmetric cryptographic algorithm. This public key is in fact the one stored in the students PC's License. After that, encrypted Course Voucher received from the entity server will be stored encrypted in the entity student's computer. Since it is encrypted with the computer's public key, using the computer's private key can only decrypt it. The private key to this key-pair is stored in some special location on the student's computer hard disk.

If all conditions are met the entity student will be allowed to download the course material to their own computers, decrypt and view the material offline, while making it difficult to perform unauthorized copying (see figure 6 and 7).



```
17291411271318 1931 27 :1729161912111142713 23212020 13
112
5812 151418149 721551020322919515  682019913 4151221 5181 51520:
1
12  154914592025620 5818 1215 56153 13152116520 18141 4209
19525149619209  14151993205 252
12  15549651420 5813 91 142520516 196153 1315211652019181 41420
581893 18118203185199920193 ,3
12  15549651420 583 13152116520191821 914192023 209
824513112161954
28 65149 5820 51531613202118519 1925520 1324(181234181 5141
41513206123518
)12
162519515  6151320612351813
6152320181 51991 19 20515  61492019211820315919141 5
18181671511819131 4144 201 182020121 519 4152015 5161185203
1315211652019181 4144 65149 5209 1915316131415145192 0
.15291613202118521 519191821 519 4151320612351820  155166181815
133192092292019 51 41420 1911911 .15132061235189  1918315520
```

Figure 6: the encrypted e-course ready to be decrypted and viewed



COURSE NAME : COMPUTER SKILLS 1

The learning objectives of this module are to :
1 To identify the role of computer and its benefits in society
2 To define the main types of computers and their characteristics,
3 To define the computers units with examples
4 Define the computer system (Hardware and Software)

Types of Software
Software is a set of instructions or programs and data that used to operate computers and define its components. Computer users used Software to perform activities and tasks. Software is created using computer programming language such as basic and Java. Programmers ar

Figure 7: viewing the decrypted e-course material

Additionally, the Computer License is designed to have an expiry date, and the average lifetime of the students PC's License is six months. Before a Computer License expires, the entity server will keep track of students' Computer Licenses, it will make sure that there is only one valid student PC's License for each entity student. In a case where an entity student cheats and request for re-issuing the student License, or the student's private key is compromised, the old student License will be cancel, however, the student have to pay the registration fees once time again if he want to have another copy of the e-course material.

10. Online Submission of Assignments

The online learning system involves a variety of communication flows between the entity server and remote entity student, each of which may have different security requirements:

- general broadcasts (e.g. lectures, module material);
- student-specific (e.g. assignment, grades);
- submission (e.g. work for assessment);
- interactive (e.g. tutorials).

To make the communication between the entity student and entity server more trustee for both side, each entity student will be granted a unique public key. This public key must be used by the entity student to digitally sign every document he/she sends to the entity server.

The SeS system will help students to solve and submit student homework assignments encrypted using their own private key. This will give great opportunity to e-education institute to force their students not to repudiate any document sent by them with their own private signature.

10.1 Digital Signature for Student

In the past, people perform their signature by signing a name or affixing a seal on a document to build the related rights and duties [14]. Hence, now we are lining in the age of Internet, e-commerce and e-government, the use of digital signature is very important.

- **Public Key Signature**

To provide for integrity, strong data authenticity and non-repudiation of all directory information is important to achieve some security features. In this way the student and organization can be sure that he/she is talking to the trusted directory when retrieving information. Digital signatures can be used to implement three important security services:

- Authentication – ensures that a principal is really who he/she claims to be.
- Data authentication – ensures that the data origin cannot be forged.
- Data integrity – ensures that no modification of data has been performed by unauthorized principals.
- Non-repudiation – ensures that a principal cannot deny performing some actions on the data (e.g. authoring, sending, and receiving).

Each entity student will be granted a digital signature that he must use to sign every document he sends to the entity server. This digital signature will be based on the RSA public key signature. Since entity student will be given two keys: public and private key. Using these two keys entity student will encrypt a secret word that is only known to him/her and chosen by him/her. This encrypted word will be sent to the entity server and be stored in the student database table to be checked and compared whenever entity student send each signed document. The following steps illustrate the public key signature scheme used in the SeS:

Suppose ES: entity server, EC: entity student, M: message

EC: (dEC, n)=Private key for Entity student

: (Xword) / entity student will select any secret word only known to him/

EC→ES: C= EKpr (Xword)

ES: M= DKpu(xword)

The above Public key signature can be explained as follows:

1. The RSA public key encryption will be used to generate a private key for the entity student (nEC, dEC). Now student assume to recall a secret word that is only known to him.
2. Entity student send to entity server the secret word encrypted using his private key (dEC) so as to be used for verifying signature and documents or messages send by entity student.
3. Entity server will decrypt the secret word (XXX) using the entity server public key (eES) and store it the student database table.
4. Now whenever an entity student sends a signed document, his/her signature will be compared with his/her decrypted secret word which has been stored in the student database table.

Conclusion

E-educational institutions organizations have to present innovative approaches in its e-educational process. Effective adoption of e-education system has to be comprehensive and should include all aspects of security regards organizations and students alike

The e-learning security measures include the formulation and implementation of a policy for server security, configuration access control, users' access control and login passwords, in conjunction with public and private key cryptographic techniques, which used to achieve user authentication, provide a safeguard against attacks, and prevent non-repudiatory usage of system by legitimate students. These techniques in result will allow data integrity and confidentiality of the organization recourses

References:

[1] Schocken, S. (2001), "**Standardized frameworks for distributed learning**", *Journal of Asynchronous Learning Networks*, Vol. 5 No.2, pp.97-110.

[2] Yau, J.C.K., Hui, L.C.K., Cheung, B.S.N., Yiu, S.M., Cheung, V.L.S. (2002), "**A cryptographic schemes in secure**

e-Course eXchange (eCX) for e-Course workflow", Conference Proceedings of SSGRR 2002 (Summer) International Conference on Advances in Infrastructure for e-Business, e-Education, e-Science, and e-Medicine on the Internet (SSRGG 2002s), L'Aquila, Italy, 29 July-4 August.

[3] Phillips, T., (1995) "**System Security in the National Information Infrastructure: Networks at Risk"**, NCSA Conference Proceedings, April 1995.

[4] Efrain Turban, David King, Dennis Viehland, Jae Lee, 2006, "**E-Commerce A managerial Perspective**", Prentice Hall, U.K, London.

[5] Allen, M. W. Michael Allen's, 2003, "**Guide to e-learning** ". Hoboken, NJ: John Wiley and Sons, 2003.

[6] David G. Rosado, Carlos Gutiérrez, Eduardo Fernández-Medina, Mario Piattini, 2006, ""**security patterns and requirements for internet-based applications**", Volume 16 Number 5 2006 pp. 519-536 , Emerald Group Publishing Limited ISSN 1066-2243

[7] Needham, R.M., Schroeder, M.D. (1978), "**Using encryption for authentication in large networks of computers**", *CACM*, Vol. 21 No.12.

[8] R.L. Rivest, A. Shamir, and L.M. Adleman, **A method for obtaining digital signatures and public-key cryptosystems**, Communications of the ACM (2) 21 (1978), 120-126.

[9] Needham, R.M., Schroeder, M.D. (1978), "**Using encryption for authentication in large networks of computers**", *CACM*, Vol. 21 No.12.

[10] Chou, D. C. et al. (1999), "**Cyberspace security management", Industrial Management & Data Systems**, Volume 99, Number 8, pp. 353-361, available at:
http://ejournals.ebsco.com/direct.asp?ArticleID=E35WHE69Q8AW23NFTVNX

[11] RSA Security (2003), "**Understanding Public Key Infrastructure (PKI**)", RSA Security Inc., available at: http://www.computel.com.lb/Downloads/PKI.pdf

[12] Joe Cho-Ki Yau1, Lucas Chi-Kwong Hui1, Siu-Ming Yiu1 and Bruce Siu-Nang Cheung, (2006), "**Towards a Secure Copyright Protection Infrastructure for e-Education Material: Principles Learned from Experience**", international Journal of Network Security, Vol.2, No.1, PP.21–28, Jan. 2006

[13] GNU (wget), GNU wget,http://www.gnu.org/software/wget/wget.html.

[14] Sattar J. Aboud and Mohammad A. Al-Fayoumi, (2007), " **A new Multisignature Scheme using re-encryption technique**" , Journal of Applied sciences, ISSN 1812-5654, Asian network for scientific information.