A Secure E-Exam Management System

Jordi Castellà-Roca[†],Jordi Herrera-Joancomarti[‡] and Aleix Dorca-Josa[§]
† Rovira i Virgili University of Tarragona, Dept. of Computer Engineering and Maths,
Av. Paisos Catalans, 26, E-43007 Tarragona, Catalonia
‡ Universitat Oberta de Catalunya, Av. Tibidabo 39, 08035 Barcelona
§ Universitat d'Andorra, Plaça de la Germandat, 7, AD600 Sant Julià de Lòria, Principat d'Andorra
E-mail: [†]jordiherrera@uoc.edu, [‡]jordi.castella@urv.net, [§]aleix.dorca@uda.ad

Abstract

1 Introduction

In e-learning environments, students and teachers use Internet in a regular basis in order to follow/receive lectures, ask/answer questions and send/receive assessments. However, e-learning (or in general distance learning) universities relay on an examination process in which students hold a face to face exam in a physical place determined by the university under supervised conditions. Such conditions ensure the correctness of the exam, a difficult task to achieve in a virtual exam model (see [**?**] for details). Face to face exams allow to ensure students identity and exam authoring using traditional means (checking an identity card and ensuring no one helps the student during the exam).

However, face to face exams represent an important effort for e-learning institutions. Typically, e-learning universities do not have enough physical facilities for all students so they have to rent buildings in order to allow students to hold their exams. Furthermore, exam management becomes more complex since such external examination centers must be provided with all management mechanism to ensure that students will be able to perform their exam in a desired location and later on, all exam answers will be properly collect and sent to the teachers that have to correct them.

In order to simplify exam management it is desirable that all exam stages can be performed electronically, so exams are turned into e-exams. Notice that we refer to e-exams to exams (in fact, all exam stages) that can be performed by electronic means. However, we do not assume that e-exams are distance o virtual exams, since such property implies different security concerns. In this paper, we assume that students hold the exam in a supervised environment, but electronically, that means the student uses a computer to answer the exam.

Intrinsically, exam management needs to achieve a good security level, since the correctness of this process ensures somehow the quality of the university. For that reason, when we design a electronic management system for exams, that is an e-exam management system, we take a special care of security properties that the system should provide.

Security in e-learning environments has been addressed in different literature works. A high level overview of this topic can be found in [**?**, **?**, **?**, **?**]. All of these works share the main ideas regarding the way to achieve better security levels in e-learning environments. Public key infrastructures (PKI) are identified as an adequate technology in order to provide confidentiality, authenticity, integrity and non-repudiation, in e-learning environments. According to these ideas, a PKI approach for an e-learning environment has been proposed recently in [**?**] showing that PKI solutions deliver flexibility and scalability to an e-learning environment.

Focus on electronic exam management, to our best knowledge, the only published work on this topic is due to Chadwick [**?**]. However, the project did not cover all stages of an exam detailed in [**?**], it only addresses the setting up stage where the examination questions are transferred between the teachers using secure electronic mail based on a PKI. On the other hand, two commercial solutions for on-line examinations are available [**?**, **?**]. However, these proposals do not describe their security measures so it is difficult to evaluate their suitability and security level.

In this paper we present a secure e-exam management system. Such system is based on different cryptographic protocols that offer a high security level for all exam stages. This scheme has been implemented in a Master Thesis [**?**].

The paper is organized as follows.....

2 Examination stages and security properties

In an examination process different stages can be identified. In this section we describe every examination stage and its security requirements based on our experience and on the contributions made in the literature papers [**?**, **?**, **?**, **?**]. This accurate description allows us to design a cryptographic protocol for each stage in order to secure all the examination process as it is shown in Section 3.

The examination process can be divided in the following stages:

Setting up an exam: the first stage is the preparation of the examination questions which is performed by the teacher.

Beginning, holding and submitting of the exam: in the second stage, when the exam begins, the student obtains the exam questions, she writes down the answers and finally she submits her answers. This stage must be performed within a fixed amount of time.

Gradding of exams: After the student has delivered the exam answer, the teacher grades it.

Obtaining the score of the exam answer: Once the exam answer has been graded, the student obtains the result.

Revising of exams Finally, if the student does not agree with the obtained grade, she can apply for an exam revision.

Regarding the stages described above, we have identified the following security requirements, although some of them had already been pointed out in previous works [**?**, **?**, **?**, **?**].

Authenticity:
- The student must be sure that the exam questions and the exam grade have been proposed by the teacher.
- The teacher must be sure that the exam answer belongs to a valid student.

Privacy:
- The exam score process should be blind in order to obtain a maximum impartiality. Then, the teacher should not know the student identity of an exam answer. However, the teacher must be convinced that the answer belongs to a valid student.

Correction:
- The exam questions can not be modified once the exam has started, that means that the integrity of the questions must be preserved.
- Once the examination time has finished, it should not be able to deliver a new answer.
- Once an answer has been delivered it must not be possible to alter it.
- It should not be able to deliver more than one exam answer per student.
- The deletion of one exam answer should be avoided or at least detected.

Secrecy:
- Exam questions must be kept secret, so the exam only can be obtained by valid students during the time of the exam.
- The exam solution must be kept secret until the exam grades are published.
- The student answers must be kept secret so only the teacher should have access.
- The exam answer grade should only be delivered to the student that delivered such answer.

Receipt: The student must obtain a receipt as a proof that she has delivered her exam answer.

Copy detection: The student should respond the exam alone, so cheating must be avoid.

3 The proposed scheme

In this section we propose a secure scheme for electronic exam management. We rely on the fact that there is no solution to obtain the copy detection property if the students answers the exam at home [**?**, **?**, **?**, **?**]. Therefore in our proposal, the exam takes place in a supervised environment.

In our proposal, we shall be faced with interactions between three kinds of parties or actors, namely:

Student: We will use the term *student* to refer to both a person taking part in the exam, and the software used to that end, since cryptographic operations must be performed.

Teacher: The *teacher* is the one that propose exam questions and grade the answers. Also in this case, we refer to both the person and the software used to that end.

Manager: The *manager* is the central authority that takes the control over the exams. It manages the exam questions, answers, solutions and grades.

For each stage enumerated in section 2 we propose one cryptographic protocol.

3.1 Notation

The following notation is used in order to describe the protocols presented.

- (P_{entity}, S_{entity}): Asymmetric key pair of $entity$, where P_{entity} is the public key and S_{entity} is the private key.
- $S_{entity}(m)$: Digital signature of message m signed by $entity$, where digital signature means computing the hash value of message m using a collision-free one-way hash function and encrypting this hash value with S_{entity}.
- $P_{entity}(m)$: Encryption of message m under the public key of $entity$.
- $H(m)$: Hash value of message m using a collision-free one-way hash function.

3.2 System set-up

The proposed scheme requires that *students, teachers* and the *manager* have a key pair of a public key criptosystem.

- (P_T, S_T) *teacher*'s key pair.
- (P_S, S_S) *strudent*'s key pair.
- (P_M, S_M) *manager*'s key pair.

Each key pair must be certified, we assume the use of a Public Key Infrastructure (PKI), as it is proposed in [**?**].

3.3 Setting up an exam

The *teacher* and the *manager* do the following steps to set up an exam.

Protocol 1

1. *The* teacher *performs the following actions:*
   (a) *Compute an unique examination identifier, Id, composed by the following data:*
      - *$\mathcal{S}$: Subject.*
      - *$\mathcal{S}c$: Subject code.*
      - *$\mathcal{Q}$: Four month period.*
      - *$\mathcal{D}$: Exam date.*
      - *$\mathcal{T}$: Fixed time to answer the exam.*
      - *$\mathcal{N}$: Exam serial number.*

   (b) *Propose the exam questions, $\mathcal{E}$.*
   (c) *Compute the digital signature of Id and $\mathcal{E}$ with S_T, $s_1 = S_T(Id, \mathcal{E})$.*
   (d) *Encrypt Id, $\mathcal{E}$ and s_1 using the managers' public key P_M, $c_1 = P_M(Id, \mathcal{E}, s_1)$.*
   (e) *Authenticate himself using his key pair (P_T, S_T).*
   (f) *Send c_1 to the* manager
2. *The* manager *perform the following actions:*
   (a) *Decrypt c_1 using S_M and obtain Id, $\mathcal{E}$ and s_1.*
   (b) *Verify the digital signature s_1 using the* teacher*'s public key P_T.*
   (c) *Store c_1 in a secure way, bound to the exam Id.*

3.4 Beginning, holding and submitting the exam

The *student, teacher* and *manger* use the Protocol 2 in order to perform an exam.

Protocol 2

1. *The* teacher *makes public the exam identifier, Id;*
2. *The* student *authenticates herself using her key pair (P_S, S_S);*
3. *The* student *asks for the exam Id to the* manager.
4. *The* manager *performs the following steps:*
   (a) *Verify if the* student *is registered in the subject $\mathcal{S}$.*
   (b) *Check if the current date $\mathcal{D}'$ and time $\mathcal{T}'$ are in the fixed time to answer the exam $\mathcal{D}$ and $\mathcal{T}$ ($\mathcal{D}$ and $\mathcal{T}$ are in the Id).*
   (c) *If the previous verifications are correct:*
      i. *Decrypt c_1 using S_M obtaining Id, $\mathcal{E}$ and s_1.*
      ii. *Encrypt Id, $\mathcal{E}$ and s_1 using P_S, $c_2 = P_S(Id, \mathcal{E}, s_1)$.*
      iii. *Send c_2 to the* student.
   (d) *Otherwise, return an error code to the* student.
5. *The* student *obtains and verifies the exam questions and submits the exam answer in the following way:*
   (a) *Decrypt c_2 using S_S obtaining Id, the exam questions $\mathcal{E}$, and s_1.*
   (b) *Verify the digital signature s_1 using P_M.*
   (c) *Write down the exam answer, $\mathcal{A}$.*
   (d) *Obtain at random an answer identifier, Ia.*
   (e) *Compute the digital signature of s_1, Ia and $\mathcal{A}$ using S_S, $s_2 = S_S(s_1, Ia, \mathcal{A})$.*
   (f) *Encrypt Id, $\mathcal{E}$, s_1, Ia, $\mathcal{A}$ and s_2 using P_M, $c_3 = P_M(\mathcal{E}, Id, s_1, Ia, \mathcal{A}, s_2)$.*

(g) *Send* c_3 *to the* manager.

6. *The* manager *follows the next steps:*

   (a) *Check if the current date* $\mathcal{D}''$ *and time* $\mathcal{T}''$ *are in the fixed time to answer the exam* $\mathcal{D}$ *and* $\mathcal{T}$.

   (b) *Verify if the* student *has submitted an exam answer previously.*

   (c) *If the previous verifications are correct:*

      i. *Decrypt* c_3 *using* S_M *and obtain* $\mathcal{E}$, Id, s_1, Ia, $\mathcal{A}$, *and* s_2.

      ii. *Verify the digital signatures* s_1 *and* s_2 *using* P_T *and* P_S *respectively.*

      iii. *Obtain the actual time* t.

      iv. *Compute the digital signature of* Id, Ia *and* t *using* S_M, $s_3 = S_M(Id, Ia, t)$. s_3 *is the exam answer receipt, the proof that the* student *has delivered her answer.*

      v. *Send* Id, Ia, t *and* s_3 *to the* student.

      vi. *Compute the digital signature of* s_1, *and* $\mathcal{A}$ *using* S_M, $s_4 = S_M(s_1, \mathcal{A})$.

      vii. *Encrypt* $\mathcal{E}$, Id, s_1, $\mathcal{A}$ *and* s_4 *using* P_T, $c_4 = P_T(\mathcal{E}, Id, s_1, \mathcal{A}, s_4)$.

      viii. *Store in a secure way,* c_3, s_3, Ia, t *and* c_4 *as one answer of the exam* Id.

   (d) *Otherwise, return an error code to the* student

7. *The* student *does the following steps:*

   (a) *Verify the digital signature* s_3 *using* P_M.

   (b) *Store* Id, Ia, t *and* s_3 *as the examination receipt.*

3.5 Gradding of exams

The *teacher* and the *manager* use Protocol 3 in order to grade one exam answer.

Protocol 3

1. *The* teacher *perform the following steps:*

   (a) *Authenticate himself to the* manager *using his key pair* (P_T, S_T).

   (b) *Request for one answer of a given exam* Id.

2. *The* manager *does the following steps:*

   (a) *Obtain one exam answer that has not been graded previously,* c_4.

   (b) *Send* c_4 *to the* teacher.

3. *The* teacher *does the following steps:*

   (a) *Decrypt* c_4 *using* S_T *obtaining* $\mathcal{E}$, Id, s_1, $\mathcal{A}$ *and* s_4.

   (b) *Verify the digital signature* s_4 *with* P_M.

   (c) *Grade the answer* $\mathcal{A}$ *with a value* $\mathcal{G}$.

   (d) *Compute the digital signature of* $\mathcal{E}$, Id, s_1, $\mathcal{A}$, $\mathcal{G}$ *using* S_T, $s_5 = S_T(\mathcal{E}, Id, s_1, \mathcal{A}, \mathcal{G})$.

   (e) *Encrypt* Id, $\mathcal{E}$, s_1, $\mathcal{A}$, s_4, $\mathcal{G}$ *and* s_5 *using* P_M, $c_5 = P_M(\mathcal{E}, Id, s_1, \mathcal{A}, \mathcal{G}, s_5)$.

   (f) *Send* c_5 *to the* manager.

4. *The* manager *does the following steps:*

   (a) *Decrypt* c_5 *using* S_M *obtaining* $\mathcal{E}$, Id, s_1, $\mathcal{A}$, s_4, $\mathcal{G}$ *and* s_5.

   (b) *Verify the digital signatures* s_1, s_4 *and* s_5 *with* P_T, P_M *and* P_T *respectively.*

   (c) *Obtain the* c_3 *that corresponds to* c_4.

   (d) *Decrypt* c_3 *using* S_M, *and obtain* $\mathcal{E}$, Id, s_1, Ia, $\mathcal{A}$ *and* s_2.

   (e) *Encrypt* $\mathcal{E}$, Id, s_1, Ia, $\mathcal{A}$, $\mathcal{G}$, s_2 *and* s_5 *using* P_S, $c_6 = P_S(\mathcal{E}, Id, s_1, Ia, \mathcal{A}, \mathcal{G}, s_2, s_5)$.

   (f) *Store* c_6, Id *and* Ie *in a secure way.*

3.6 Obtaining the score of the exam answer

The *student* obtains her exam score by running the Protocol 4 together with the *manager*.

Protocol 4

1. *The* student *authenticates herself in front of the* manager *using her key pair* (P_S, S_S).

2. *The* student *request from the* manager *the score of the answer* Ia.

3. *The* manager *perform the following steps:*

   (a) *Verify if* Ia *belongs to the* student *that has been authenticated.*

   (b) *Obtain* c_6 *that had been stored;*

   (c) *Send* c_6 *to the* student.

4. *The* student *obtains the grade* $\mathcal{G}$ *by following the next steps:*

   (a) *Decrypt* c_6 *using* S_S, *and obtain* $\mathcal{E}$, Id, s_1, Ia, $\mathcal{A}$, $\mathcal{G}$, s_2 *and* s_5.

   (b) *Verify the digital signatures* s_1, s_2 *and* s_5 *using* P_T, P_S *and* P_T *respectively.*

3.7 Revising of exams

The *student* may apply for an exam grade revision by running the Protocol 5 together with the *manager*.

Protocol 5

1. *The* student *does the following steps:*
   (a) *Authenticate herself in front of the manager using her key pair* (P_S, S_S).
   (b) *Obtain at random number that will be the revision identifier* Ir.
   (c) *Compute a digital signature of* Id, Ia, Ir *using* S_S, $s_6 = S_S(Id, Ia, Ir)$. s_6 *is the request to review the score of the answer* Ie.
   (d) *Send* Id, Ia, Ir *and* s_6 *to the* manager.
2. *The* manager *does the following steps:*
   (a) *Verify the digital signature* s_6 *using* P_S.
   (b) *Store* Id, Ia, Ir *and* s_6.

The *teacher* uses a modification of Protocol 3 in order to review one exam.

4 Security analysis

We assume that *manager* is honest, so our protocol is based on a Trusted Third Party (TTP), that is the *manager*.

Authenticity:
- In Step 1c of Protocol 1 the teacher digitally signs the exam. The student verifies this signature in Step 5b of Protocol 2, and then she ensures the exam questions have been proposed by the teacher.
- In Step 3d of Protocol 3 the teacher digitally signs the grade. The student verifies the digital signature in Step 4b of Protocol 4, so she is convinced that grade has been proposed by the teacher.
- In Step 5e of Protocol 2 the student digitally signs the exam answer. The manager verifies the student's signature in Step 6(c)ii of Protocol 2 and computes a digital signature of exam answer in Step 6(c)vi. The teacher verifies the manager's digital signature in Step 3b of Protocol 3. Assuming *manager* honesty, the teacher has no doubt the answer has been written by a valid student.

Privacy:
- In Step 3a of Protocol 3 the teacher receives an exam answer c_4, and he decrypts it obtaining $\mathcal{E}$, Id, s_1, $\mathcal{A}$ and s_4. This information does not reveal the student identity. However, the digital signature s_4 convinces the teacher that $\mathcal{A}$ belongs to a valid student.

Correction:
- In Step 1c of Protocol 1 the teacher digitally signs the exam obtaining s_1. The Student computes the digital signature of s_1, Ia and $\mathcal{A}$ in Step 5e of Protocol 2 obtaining s_2. The digital signatures s_1 and s_2 grant that the exam questions have not been modified once the exam has started.
- In Step 6a of Protocol 2 the manager verifies whether the examination time has finished, denying any exam answer submission once the time has expired.
- The student digitally signs the exam answer in Step 5e of Protocol 2. So, if the answer is modified the digital signature verification will fail.
- In Step 6b of Protocol 2 the manager verifies if the student has previously delivered an exam answer, and in this case, the exam answer is not accepted.
- If one exam is deleted there is one student that will not obtain her grade, so the deletion is detected. Moreover, the student can prove that has delivered the exam, because she can show the examination receipt obtained in Step 7 of Protocol 2.

Secrecy:
- The teacher encrypts the exam questions in Step 1d using the *manager*'s public key. The *manager*'s private key is needed to obtain the exam questions, and such key is restricted to the *manager*. The *manager* sends the exam questions to the *student* in Step 4(c)iii of Protocol 2 if the student is registered in the exam subject and if the current time and date are in the fixed time to answer the exam, Steps 4a and 4b of the Protocol 2.
- The *teacher* can deliver the exam solution to the *manager* using a modification of Protocol 1, so the solution is encrypted and only can be obtained by the *manager*.
- In Step 5f of Protocol 2 the *student* encrypts her answer using the *manager*'s public key. At this point, the exam answer only can be obtained by the *manager*. Later on, the *manager* encrypts the exam answer with the *teacher*'s public key in Step 6(c)vii. The teacher obtains the exam answer encrypted in Step 3. We conclude that student's answers are kept secret, so only the teacher (and the manager) have access to them.
- The *manager* authenticates the Student in Step 1 of Protocol 4 and verifies that she is the owner of the answer Ia in Step 3a of Protocol 4. If the above verification holds the *manager* sends c_6 to

Figure 1. System overview

the *student*. c_6 is the exam grade encrypted using the *student*'s public key, so that only the *student* can obtain her grade.

Receipt: The student obtains a receipt in Step 7 of Protocol 2 as a proof of exam delivery.

Copy detection: The exam takes place in a supervised environment, so the copy detection is prevented using traditional means.

5 Implementation

The secure e-exam management system described in previous sections has been implemented in a Master Thesis [**?**]. The system has been developed in Java language since it is platform independent so the system can be deployed in any architecture. Moreover, The Java languages offers several cryptographic APIs with the cryptosystems needed in our systems. We have used the IAIK [**?**] because contains an implementation of the whole Java Cryptography Extension (JCE) framework, it has a good documentation.

The system is composed by five main components: cryptographic scheme component, XML, RMI, Data Base (DB), and finally the graphic interface. In figure 1 we can see system overview.

5.1 Cryptographic scheme component

The cryptographic scheme component contains the implementation of the cryptographic functions presented in Section 3. There is one class for each protocol, so the class encapsulates all operations done in the protocol. Each part of the protocol uses one instance of the class to run the specific protocol.

5.2 XML component

The outputs of the cryptographic scheme component are stored in an XML document using the XML component. XML documents are exchanged between the actors, i.e. *manager*, *student* and *teacher*. Once a document is received, the cryptographic information is obtained using the XML component, and checked using the cryptographic scheme component. If verifications hold the document is stored.

The XML data format allows efficient data management, and, additionally, the system becomes more flexible in terms of updating or modification.

Our implementation uses the JDOM [**?**] API in the XML component, because is open source and it provides a low-cost entry point for using XML.

5.3 RMI component

Java Remote Method Invocation (Java RMI) [**?**] technology has been used since it enables to create a distributed system, in which the methods of remote Java objects can be invoked from other Java virtual machines on different hosts. In this way, communication between the *manager*, *student* and *teacher* is transparent and implementation becomes easier.

5.4 Data base component

The exam questions, answers, grades, and reviews must be stored in a persistent way. Moreover, we need to keep information about *teachers* and *students*.

The system stores the above information in a MySQL [**?**] Data Base server. Such database has been chosen since it is open source, and there are implementations available for the main architectures, Microsoft© Win32, Linux, and MacOSX ©.

The Data Base (DB) is not accessed directly. The Data base component is the middleware between the DB and the other system components.

5.5 Graphic interface component

The system becomes useless without a good user interface. We have developed a basic graphical interface that allows users to do the basic operations described in Section 2 in a way intuitive.

We have used the Standard Widget Toolkit (SWT), because is easy to use and is open source.

Once we run the teacher's application or student's application, the presentation view is shown, see figure 2.

Figure 2. Presentation view

As it has been said previously, each user has a key pair. We have stored this key pair in a PKCS#12 [**?**] file. In the first step, in any of the two applications, the user must introduce her PKCS#12 file and the password used to protect it. In figure 3 we can see the form where the user enters the above information.

The figure 4 shows the *teacher*'s application. In the upper left side there is the exam identifier information. In the upper right side there are the control buttons: send exam, obtain exam answers, grade exam answer, and obtain exam

Figure 3. Users' authentication dialog

reviews. The $<<$ and $>>$ buttons allow to obtain the next exam answer or the next exam that must be reviewed. In the middle of the application there are the exam questions, and in the lower of the view there is the exam answer.

Figure 4. Teacher's application

The figure 5 shows the *student*'s application. In the upper left side, like in the *teacher*'s application, there is the exam identifier information. The control buttons are in the upper right side. The control buttons are the following: get exam, get exam grade, send exam grade and ask for exam revision. The exam questions and the exam answer are in the same layout as in the *teacher*'s application.

Figure 5. Student's application

6. Conclusions

We have presented a secure e-exam management system. Such system is based on different cryptographic protocols that offer a high security level for all exam stages. Moreover, the scheme has been implemented in [**?**], in order to test his functionality.

Although the graphical interface allows the basic operations, our future work is to improve it with the users feedback. A second future work is to use smart-cards to keep in a secure way the users' key pair.

Acknowledgements and disclaimer

This work is partially supported by the Spanish MCYT and the FEDER funds under grant SEG2004-04352-C04-04 PROPRIETAS-WIRELESS. The work described in this paper has been supported in part by the European Commission through the IST Programme under Contract IST-2002-507932 ECRYPT. The information in this document reflects only the author's views, is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability. The first author is partly supported by the Catalan Government under grant 2005 SGR 00446, and by the Spanish Ministry of Science and Education through project SEG2004-04352-C04-01 "PROPRIETAS".

References