Cryptography Adapted to the New European Area of Higher Education

A. Queiruga Dios[1], L. Hernández Encinas[2], and D. Queiruga[3]

[1]Department of Applied Mathematics, E.T.S.I.I., University of Salamanca
Avda. Fernández Ballesteros 2, 37700-Béjar, Salamanca, Spain
queirugadios@usal.es

[2]Department of Information Processing and Coding, Applied Physics Institute, CSIC
C/ Serrano 144, 28006-Madrid, Spain
luis@iec.csic.es

[3]Department of Business Administration, University of Salamanca
Campus Miguel de Unamuno, FES building, 37007-Salamanca, Spain
queiruga@usal.es

Abstract. A new experience for teaching Cryptography to engineering students is shown. The aim is to give them a better understanding of secure and cryptographic algorithms by using Maple software, in a graduate-level course. In this paper we discuss how to structure, define, and implement a web-based course as a part of the traditional classes, according to the convergence of the European Higher Education Project. The proposed course facilitates the use of new Information and Communication Technologies.

Keywords: Public key cryptography, implementation, Maple software, information and communication technologies, European area of higher education.

1 Introduction

The Bologna declaration (1999) proposes the creation of an European Area of Higher Education (EAHE) to unify university studies in Europe. It emphasizes the creation of the European Area of Higher Education as a key to promote citizens' mobility and employability and the Continent's overall development [2]. Spain is one of the 46 countries involved in the Bologna Process. The corner stones of such an open space are mutual recognition of degrees and other higher education qualifications, transparency (readable and comparable degrees organised in a three-cycle structure) and European cooperation in quality assurance.

This earthquake in thinking about the new education process means that we must approach the design, development, and implementation of learning environment such that the achievement and assessment of those competencies is made possible and is facilitated. This new proposal supposes a change of the instructional design process [12].

The use of Information and Communication Technologies (ICT) in higher education is considered a pre-requisite for the adaptation to the EAHE. University

M. Bubak et al. (Eds.): ICCS 2008, Part II, LNCS 5102, pp. 706–714, 2008.

studies must be adapted to the international European context and technology development facilitating new strategies of communication. This new situation forces Universities to renew some situations that until now seemed stable as teaching methodologies, and change their degrees and studies programmes. ICT become more and more important in the higher education process, claiming new spaces and conditions of learning, and new professional roles for lecturers [8].

One of the fields of greater projection in the future and greater impact, within the ICT, is Cryptography. As it is known, this science is closely related to the Mathematics in general, and Computer Sciences in particular. Its aim is the preservation of information, including confidentiality, integrity, and authentication. The goal of the Cryptography is to provide safe communications on insecure channels, to allow people send messages by means of a channel that can be intercepted by a third person (mail or e-mail, telephone, fax, etc.), so only the authorized receiver can read the messages [7], [15]. The great importance of Cryptography in our days is due to the proliferation of personal computers and the facility in the access to the Internet. These facilities have cause serious problems of security, like virus, spam, phising, publication of confidential information, etc. All of it makes necessary that students and future professionals are conscious of the dangers that browse the Internet without safety measures supposes. In this paper, we present some educational tools to learn about Cryptography and how to implement different cryptosystems by using Maple software together with Moodle environment. Moodle is an open source package, designed using pedagogical principles, in order to help educators to create effective online learning communities.

The rest of the paper is organized as follows: In section 2, we will comment the changes that are happening in the Spanish Universities to reach the European Area of Higher Education. The course *Cryptography and information security* will be detailed in section 3. Background and Maple concepts needed to follow this course are presented in section 4. In section 5 we will present the Moodle tools used in the University of Salamanca (`http://www.usal.es`), the detailed methods that we used in the course will be stated in section 6, and finally, the conclusions will be shown in section 7.

2 Changes in Higher Education

The knowledge society depends for its growth on the production of new knowledge, its transmission through education and training, and its dissemination through Information and Communication Technologies [1]. As it was mentioned in the Introduction, one of the means to get the convergence of European Higher Education and the common goal of the Bologna Declaration is the use of the ICT in higher education.

Universities face an imperative necessity to adapt and adjust to a whole series of profound changes, including increased demand, internationalisation and links with business.

Online education also refers to learning methods that, at least, partly utilize the ICT available through the Internet. What we propose to the students is to use the online methods to get a more complete education in specific subjects. The online education is a new method of education, very different from traditional education, that take advantage of new media, new ways to communicate, and the design of new educational experiences. Educators are thus utilizing the Internet for professional networking, regionally and globally, they learn from one another about the new media and their applications to education [21], and renew their knowledge in virtually fields of enquiry.

The ICT have changed from being considered as a mere object of use towards an instrument of support in the educational innovation [20]. They affect to different aspects in relation to traditional education, as the change in the role of the teacher, who has changed from a simple transmitter of knowledge to be a mediator in the construction of the knowledge of the students; the role of the student has changed as the traditional educative models do not adjust to the processes of learning by means of the use of the ICT [18]. Finally, it is important to take into account that the use of new technologies does not require the invention of new methodologies, but it requires a modification in the strategies for the continuous learning of the student [13].

Modern e-Learning technology may act as a bridge: On the one hand, computer systems make real experiments available over the Internet, any time, anywhere, and – even more important – make the measured data electronically available for further analysis [11]. On the other hand students could access to simulation within virtual laboratories.

3 Cryptography and Information Security Course

The *Cryptography and information security* course has been revised from previous years to give more emphasis to the practical elements of the course. It is an introduction to Cryptography. The viewpoint of this course is specifically the design and analysis of real world cryptographic schemes. We consider tasks like encryption and decryption processes, digital signatures, authentication, and key distribution. The goal is to instil understanding of fundamentals into the design of cryptographic protocols. Formally, the assessed course consists of 7 modules and a set of laboratory software practices with Maple. The modules are:

1. Introduction to Cryptography
2. Mathematical tools
3. Private Key Cryptosystems
4. RSA Cryptosystem
5. ElGamal and Elliptic Curve Cryptosystems
6. Chor-Rivest knapsack Cryptosystem
7. Biometric recognition systems

In the beginning, this course was purely theoretical, nevertheless, in recent years, we have including laboratory practices, using Maple software, and now we make use of ICT to get rather than an online course: A set of tools making possible to work with students in classes or in their own houses.

3.1 A Brief Introduction to Cryptography

The objective of Cryptography is to assure the secrecy and confidentiality of communications between several users and the goal of Cryptanalysis is to break the security and privacy of such communications [15], [16]. In particular, in Public Key Cryptography (PKC) each user has two keys: The public key, which is publicly known and it is used by the sender to encrypt a message; and the private key, which is kept in secret by the receiver and it is used by him to decrypt the received encrypted messages. In general, PKC bases its security on the computational intractability of some Number Theory Problems, as factorization problem, discrete logarithm problem or knapsack problem.

3.2 Modules of the Course

The course starts with an introduction to Cryptography and to the necessary mathematical tools for the correct understanding and development of the different modules. This introductory part includes the main mathematical problems on which the different cryptosystems security are based. Later, a basic knowledge of the Cryptography will be approached, including the different types of cryptosystems and the schemes of digital signature associated to them.

The course includes the most important Secret Key or Symmetric Cryptosystems and as far as Public Key or Asymmetric Cryptosystems. RSA Public key cryptosystem [5], [19] and its protocol of digital signature will be detailed including the more important attacks against their security. ElGamal and Elliptic Curve cryptosystems [6], [14], are also included. The security of these cryptosystems is based on the discrete logarithm problem. Also the most important characteristics of the knapsack cryptosystems will be analyzed, in particular Chor-Rivest cryptosystem [4]. With the purpose of exemplifying in a practical way the schemes and protocols studied throughout the course, it will be carried out different practices from laboratory by means of the program of symbolic calculation, Maple. In this way, the analyzed difficulties of the mathematical problems considered and security of cryptosystems will be shown.

4 Implementation and Procedures in Maple

In this section we present the second part of the course, which is addressed to show the students how to work with Maple software in order to implement procedures, functions, and statements needed to transform the messages, to generate the keys, to encrypt, and to decrypt messages with the cryptosystems previously mentioned.

Maple is a comprehensive environment for teaching and applying Mathematics which contains thousands of math procedures. It permits to define specific procedures by using the Maple programming language. It contains several packages to help professors to teach and students to understand mathematical concepts. A package is a collection of routines that are collected together. For example, `numtheory`, `ListTools` and `LinearAlgebra` are packages, which provides a range of functionality, by commands, for solving problems in some well-defined problem domain. Maple has excellent online help. In fact, it is possible to access to this help by choosing Maple Help from the Windows menu, typing a question tag in the command prompt, or clicking on F1 key.

After knowing the Maple syntax, the students will practice with the main commands needed to implement different cryptosystems. For example, for RSA cryptosystem they will need some commands like `ifactors(n)`, which returns the complete integer factorization of the integer n; `phi(n)` which is the one that calculates Euler's phi function or totient function of n, which is the number of positive integers not exceeding n and relatively prime to n; or `Power(c, d) mod n` which computes $c^d \bmod n$. In case of the Chor-Rivest knapsack cryptosystem [9], the `GF(q,h,f)` command returns a table of functions and constants for doing arithmetic in the finite field of q^h elements: $GF(q^h) = GF(q)[T]/(f(T))$, where $f(T)$ is an irreducible monic polynomial of degree h over the integers modulo q. If f is not specified, Maple uses a random one. The `Powmod(a,n,f,x)` function computes the remainder of a^n in $GF(q^h)$. Finally, if $u = [u_1, \ldots, u_n]$ is a list of integers and $m = [m_1, \ldots, m_n]$ a list of moduli, pairwise relatively prime, the function `chrem(u,m)` solves the Chinese Remainder Theorem, i.e., it computes the unique positive integer a, $0 < a < M$ (M denotes the product of the moduli), such that $a = u_1 \bmod m_1$, $a = u_2 \bmod m_2$, $\ldots$, $a = u_n \bmod m_n$.

5 Working Environment

5.1 EUDORED

Although the implantation of modern models of complementary education, b-Learning or e-Learning, not yet are a reality in the Spanish universities, their use have considerably increased in recent years. The University of Salamanca has a virtual environment to distribute its teaching: EUDORED (University of Salamanca environment for web learning). This tool is available for students and teachers to incorporate new educative technologies to the development of educational tasks, allowing virtual teaching. EUDORED is constructed on a technological structure that canalizes the formation through the Internet. In this way, it facilitates web tools to transfer the interaction processes teacher-student.

The virtual campus, EUDORED (`http://www.usal.es/eudored`), is based on a web platform called Moodle (Modular Object Oriented Distance Learning Environment), a course management system designed to help educators for creating quality online courses. This platform is used by universities, schools, companies and independent teachers. Moodle is an open source software package and completely free to use (`http://www.moodle.org`).

5.2 Moodle Platform

Moodle is a virtual environment for education which allows to place contents and tasks in the web and provides online communication tools. The design and development of Moodle is guided by a particular philosophy of learning: social constructionist Philosophy. With this learning philosophy people actively construct new knowledge as they interact with their environment, under the hypothesis that learning is more effective when you are constructing something. Constructivism is a philosophy of learning founded on the premise that, by reflecting on our experiences, we construct our own understanding of the world we live in. Each of us generates our own rules and mental models, which we use to make sense of our experiences. Learning, therefore, is simply the process of adjusting our mental models to accommodate new experiences. Constructivism calls for the elimination of a standardized curriculum. Instead, it promotes using curricula customized to the students' prior knowledge. Also, it emphasizes hands-on problem solving [3].

Another important characteristic of Moodle is that could be considered as a set of Web 2.0 learning tools. It is known that Web 2.0 refers generally to web tools that, rather than serve as a forum for authorities to impart information to a passive or receptive audience, actually invite site visitors to comment, collaborate, and edit information, creating a more distributed form of authority in which the boundaries between site creator and visitor are blurred [17]. Web 2.0 is related to a perceived second generation of web-based communities and hosted services – such as social-networking sites, wikis and folksonomies – which aim to facilitate collaboration and share information between users. Although the term suggests a new version of the World Wide Web, it does not refer to an update to any technical specifications, but to changes in the ways software developers and end-users use the web.

5.3 Moodle Activities

One of the most important advantages of Moodle environment is that it has implemented all the useful tools and activities needed for online classes and e-Learning in general. The following features are part of the learning environment:

1. Chat: The Chat module allows participants to have a real-time synchronous discussion via the web. This is a useful way to get a different understanding of each other and the topic being discussed.
2. Forums: It is in forums where most discussion takes place. Forums can be structured in different ways, and can include peer rating of each posting. The postings can be viewed in a variety for formats, and can include attachments.
3. Glossaries: This activity allows participants to create and maintain a list of definitions, like a dictionary. The entries can be searched or browsed in many different formats.
4. Hotpot: This module allows teachers to create multiple-choice, short-answer, jumbled-sentence, crossword, matching/ordering and gap-fill quizzes using Hot Potatoes software [10]. The Hot Potatoes suite is a set of six authoring

tools, created by the Research and Development team at the University of Victoria Humanities Computing and Media Centre. They enable you to create interactive Web-based exercises of several basic types. The exercises are standard web pages using XHTML code for display, and JavaScript for interactivity.

5. Lessons: A lesson delivers contents in an interesting and flexible way. It consists of a number of pages. Each page normally ends with a multiple choice question. Navigation through the lesson can be straight forward or complex.
6. Resources: Resources can be prepared files uploaded to the course server; pages edited directly in Moodle; or external web pages made to appear part of this course.
7. Wiki: A wiki is a web page that anyone can add to or edit. It enables documents to be authored collectively and supports collaborative learning. Old versions are not deleted and may be restored if required.

6 Course Objectives - Training in Cryptography

We have used Moodle to create a new interactive educational teacher-student context. Students need to construct their own understanding of each cryptographic concept, so that the primary role of teacher is not to explain, or attempt to 'transfer' knowledge, but to create situations for students that allow them to make the necessary mental constructions. In 21st century students are familiarized with the Internet and with the new technologies. They usually use them to chat with friends, to send and receive e-mails, to meet people or to organize holidays, but they are not conscious that it is a useful tool in the daily classes. Sometimes they do not see possible that personal computers and the Internet could be used effectively for classes about Mathematics or Cryptography.

With the purpose of obtaining a suitable training of the students, in each module we will give the students access to some interesting and introductory documentation, and we will create a forum to discuss about the current module. For example, with RSA cryptosystem module we start a new Moodle activity which is a questionnaire with different items related to the algorithms and the encryption and decryption processes. Other exercises will be proposed to the students so that they can comment and debate them in the forums created for that goal. Moreover, some theoretical questions or Hot Potatoes exercises, that enable the creation of interactive tests [10], will be proposed for the students assessment.

Another interesting and practical exercise that we propose the students is to generate their own keys and the possibility of sending encrypted messages to other students and to decrypt messages that they receive from other classmates or from the teacher. All of it could be possible using the cryptosystems studied during the course, because they have developed some of them using Maple software.

At the moment the only way that we use to check Maple source code, is to write it in a text file and check the right functionality in Maple itself, but it could be a good learning tool an API that allows students to write their own source code (could be Maple, Matlab, Mathematica,...) and to test it at the same time, without install those programs in their PCs.

7 Conclusions

We have designed a new experience for teaching Cryptography in the University of Salamanca, Spain. The aim is to give the students a better understanding of secure and cryptographic algorithms by using Maple software, in a graduate-level course. In this paper we have proposed a web-based course according to the convergence of European Higher Education Project, to increase the use of new Information and Communication Technologies. This course will be available, for the students of the university, in the virtual environment EUDORED, which is based on the Moodle platform, and offers a reachable environment easy to work with.

The course allows us to get a formative evaluation (focuses on improvement the security and Cryptography knowledge while the course is in progress) as much as a summative evaluation (focuses on results or outcomes). To make both evaluations possible, students can access to the online course by the Internet including the theory, papers and links related to the topic of the subject. The students will e-mail all the questions, suggestions, or whatever they need to make this e-Learning possible. Moreover, they will have access to electronic chat room, and forums to make possible an online participation whenever they want.

Acknowledgment. This work has been supported by Ministerio de Industria, Turismo y Comercio (Spain) in collaboration with Telefónica I+D (Project SEGUR@) with reference CENIT-2007 2004.

References

1. Blackstone, T.: Education and Training in the Europe of Knowledge (January 2008), http://www.uniroma3.it/downloads/297_Lezione%20Blackstone.doc
2. Bologna Declaration (January 2008), http://www.ond.vlaanderen.be/hogeronderwijs/bologna/documents/MDC/BOLOGNA_DECLARATION1.pdf
3. Brooks, J., Brooks, M.: *In Search of Understanding: The Case for Constructivist Classrooms, Revised Edition*, ASCD, 1999.
4. Chor, B., Rivest, R.L.: A knapsack-type public key cryptosystem based on aritmethic in finite fields. IEEE Trans. Inform. Theory 34(5), 901–909 (1988)
5. Durán Díaz, R., Hernández Encinas, L., Muñoz Masqué, J.: El criptosistema RSA, RA-MA, Madrid (2005)
6. ElGamal, T.: A public-key cryptosystem and a signature scheme based on discrete logarithm. IEEE Trans. Inform. Theory 31, 469–472 (1985)
7. Fúster Sabater, A., de la Guía Martínez, D., Hernández Encinas, L., Montoya Vitini, F., Muñoz Masqué, J.: Técnicas criptográficas de protección de datos, RA-MA, 3ª ed., Madrid (2004)

8. García-Valcárcel Muñoz-Repiso, A., Tejedor Tejedor, F.J.: Current Developments in Technology-Assisted Education. In: Méndez-Vilas, A., Solano Martín, A., Mesa González, J.A., Mesa González, J. (eds.) FORMATEX (2006)
9. Hernández Encinas, L., Muñoz Masqué, J., Queiruga Dios, A.: Maple implementation of the Chor-Rivest cryptosystem. In: Alexandrov, V.N., van Albada, G.D., Sloot, P.M.A., Dongarra, J. (eds.) ICCS 2006. LNCS, vol. 3992, pp. 438–445. Springer, Heidelberg (2006)
10. Hot Potatoe Home page, `http://hotpot.uvic.ca/`
11. Jeschke, S., Richter, T., Scheel, H., Thomsen, C.: On Remote and Virtual Experiments in eLearning in Statistical Mechanics and Thermodynamics. In: Proceedings of the Fifth IEEE International Conference on Pervasive Computing and Communications Workshops, pp. 153–158. IEEE Computer Society, Los Alamitos (2007)
12. Kirschner, P.A.: Using integrated electronic environments for collaborative teaching/learning. Research Dialogue in Learning and Instruction 2(1), 1–10 (2001)
13. Mason, R.: Models of online courses. ALN Magazine 2, 2 (1998)
14. Menezes, A.: Elliptic Curve Public Key Cryptoystem. Kluwer Academic Publishers, Boston (1993)
15. Menezes, A., van Oorschot, P., Vanstone, S.: Handbook of applied cryptography. CRC Press, Boca Raton (1997)
16. Mollin, R.A.: An introduction to cryptography. Chapman & Hall/CRC, Boca Raton (2001)
17. Oberhelman, D.D.: Coming to terms with Web 2.0. Reference Reviews 21(7), 5–6 (2007)
18. Pérez i Garcías, A.: Nuevas estrategias didácticas en entornos digitales para la enseñanza superior. En Didáctica y tecnología educativa para una univesidad en un mundo digital (J. Salinas y A. Batista), Universidad de Panamá, Imprenta universitaria (2002)
19. Rivest, R.L., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM 21, 120–126 (1978)
20. Salinas, J.: Innovación docente y uso de las TIC en la enseñanza universitaria. Revista de Universidad y Sociedad del Conocimiento (RUSC) 1, 1 (2004)
21. Weiss, J., et al. (eds.): The International Handbook of Virtual Learning Environments, vol. 14. Springer, Heidelberg (2006)