Proceedings of the Frontiers in Mathematics and Science Education Research Conference
1-3 May 2014, Famagusta, North Cyprus

Cryptography: optional subject in the degree in computer engineering in information technologies

G. Rodríguez Sánchez[1,*], A. Hernández Encinas[1], L. Hernández Encinas[2], A. Martín del Rey[1], and A. Queiruga Dios[1]
[1] Department of Applied Mathematics, University of Salamanca, Salamanca, Spain
[2] Istitute of Physical and Information Technologies (ITEFI), Spanish National Research Council (CSIC), Madrid, Spain
For correspondence: gerardo@usal.es

Abstract: Cryptography subject is part of the curriculum of the Bachelor's Degree in Computer Engineering in Information Systems, at the University of Salamanca. This subject becomes easy to understand if the history of Cryptography is used. The basic mathematics includes the following main topics: Modular arithmetic, algebraic curves, finite fields and number theory. Cryptography is a means of protecting personal information to avoid an eavesdropper can access it. From the first century AD with the Julius Caesar cipher to the present day with RSA, ElGamal, knapsack or elliptic curve cryptosystems, the Cryptography has evolved. In this paper we will show the syllabus of Cryptography subject and how the history knowledge supposes an important part of it, and helps students to acquire the skills and competences included in the subject curriculum.

Keywords: Cryptography, skills and competences, collaborative work.

Introduction

Cryptography is part of the curriculum of the Bachelor's degree in Computer Engineering in Information Systems, at the University of Salamanca. This is an optional course in the third year, with 60 hours. This subject is particularly interesting if the history of Cryptography is used as a methodological tool. The basic Mathematics tools for Cryptography include the following main topics: Modular arithmetic, algebraic curves, finite fields and specially number theory.

Cryptography as a means of protecting personal information is an art as old as writing itself. For centuries it remained closely linked to the military and diplomatic circles, since they were the only ones who initially had real need of it (Fúster Sabater et al, 2012). Today the situation has dramatically changed: the development of electronic communications, combined with the massive and widespread use of computers, enables the transmission and storage of high flows of confidential information that must be protected.

In the first century AD the Julius Caesar cipher was used, it consisted of replacing each letter of the Latin alphabet by the third letter that follows. In Augustus encryption, each letter is replaced by the following. The algorithm used in these cases is a simple addition in modular arithmetic, which breaks easily using statistical techniques. It was during the First World War when Cryptography began its final takeoff, to turn into what it is today. At that time, working groups to design methods to encrypt texts where created, so those texts or messages can be transmitted by radio or telegraph without fear of enemy tracks. In the mid-seventies, the traditional Cryptography experienced a deep revolution with the advent of public-key cryptosystems. The development and proliferation of very cheap digital equipments allowed widespread use of technical data protection. At the same time, this generalization created the need for new types of cryptosystems. In 1976 the public key Cryptography was born, in which the use of two keys are needed: Public key to encrypt the message that will be send and private key to decrypt the message.

From the first century AD to the present day we have moved from a basic modular arithmetic operation to computationally intractable problems such as the Pseudo Random Number Generator (PRNG), the Discrete Logarithm Problem (DLP), the Integer Factorization Problem (IFP) or the Knapsack Problem (KP) (Menezes et al, 1997). We help students to understand that the Cryptography evolves keeping the same idea than in the past: original data is replaced by an encrypted one.

This paper is distributed as follow: The syllabus, the competences, and skill that should be acquired in the course are detailed in following section, together with the assessment process during the academic year. Finally some conclusions and the obtained results from this course are shown.

Cryptography subject: University Academic Guide of the subject

Competences, objectives, and contents included in the course syllabus
The specific skill to be achieved at the end of this course is the ability to understand and apply the theoretical and practical foundations associated to the mechanisms used to provide security to computer systems.

The course objectives are:

- To understand the cryptographic techniques.
- To get a better base knowledge of computer security.
- To apply previously acquired knowledge in other subjects.
- To get the ability to relate concepts, knowledge and information from related subjects.
- To acquire organizational capacity, work planning, analysis, review, synthesis and work individually and in teams.
- To develop skills in oral and written communication of knowledge, ideas, procedures, experiences and results.
- To promote the student's autonomous work, analysis, criticism and decision making.

Many courses related to Cryptography are structure like this (Al-Hamdani and Griskell, 2005), with theoretical contents and practice contents. The theoretical ones, in the Bachelor's Degree in Computer Engineering in Information Systems at the University of Salamanca, are separated into 4 units: (I) Introduction and preliminary concepts, (II) Mathematical Foundations, (III) Systems of secret key encryption, (IV) Systems of public key encryption, and (V) Digital signature and hash functions. The topics of the course cover from an historical introduction and preliminary concepts to the RSA Digital Signature and hash algorithms like MAC, MD5 or SHA.

Methodology
The teaching-learning methodology focuses on problem solving, but obviously in lectures the minimum theoretical foundations necessary for proper understanding of the different algorithms will be expose, in order to solve the problems used throughout the semester. Consequently, most of the activities in the classroom are practical, and include the resolution by the teacher and students of numerous problems that allow the acquisition of the subject's skills.

An important part in this course is the use of specific software, like Mathematica package, and programming languages such as C or Java. These computer practices are developed in medium-sized groups (depending on the classroom capacity), although training is completed by the individual work of students taking advantage of the Mathematica campus license that the University of Salamanca has. Therefore, classroom activities of students aimed at problem solving and the use of an advanced mathematical software that allows them to address calculations, in addition to implementing complex software solutions using problems. The teaching materials are available to students through the Moodle virtual learning environment (Studium platform and the University of Salamanca). The students must, individually and in small groups, develop a series of works and solve some problems, that allow their assessment and evaluation.

Contents and competences assessment

In recent years we are trying out different ways of assessing the subject of Cryptography. The types of assessment that we usually used are:

- Active participation in class, solving problems and doing activities that are proposed at all times.
- Tasks proposed in Moodle, such as questionnaires, wikis or active participation in the proposed forum environment (see Figure 1).
- Delivery of a work which can be individual or in groups. Besides delivery of the work, students must present it in class and the other students evaluate it (Gayoso Martínez et al, 2010).

The assessment process measures the achievement of the objectives and competences of the course. Additional papers (files) presented by the students about some theoretical aspects and skills related to the subject are also taken into consideration. In recent years, as a result of the entry of the Spanish universities in the European Higher Education Area (http://www.ehea.info/), assessment has become more important, since the evaluation techniques are changing, because now not only content knowledge of the matters are evaluated, but also the acquisition of necessary skills to pass the course (García et al, 2014).

Attending a tutorial personalized with the course tutor is recommended to students that fail the course. During this tutoring process, the teacher performs a program of activities for competencies achievement by student.

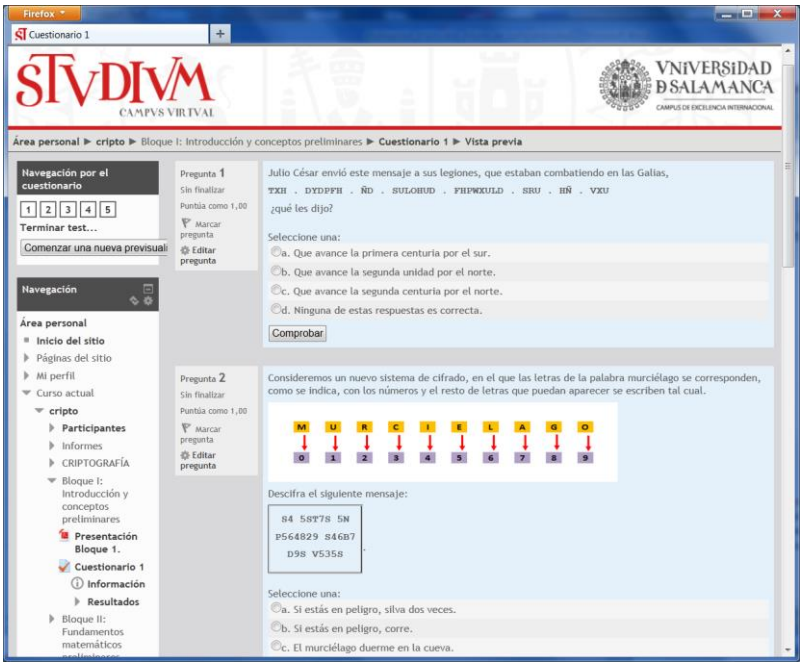

Figure 1: First proposed questionnaire inside model environment.

Conclusions and results

Throughout the semester students completed questionnaires, as can be seen in Figure 1. Moreover, as final work they proposed the creation of a collaborative web site, a wiki; see Parker & Chao (2007). Students used the wiki a research project, as was suggested by Duffy and Bruns (2006), students built a collaborative environment, a place where everyone will be able to add information related to Cryptography. Moreover, the wiki was used as a presentation tool where students and notes, comments and modifications every time.

In particular, students of this 2013-2014 academic year built a wiki including one "old" cryptosystem, with the corresponding implementation, also including the source code in Java o C language and a real example. The advantage of the wiki is that the source code could be improved by other students,

to make it more efficient, clearer, or to add comments. One of the students used the Asterix and Obelix comic to show an example of the Caesar cipher (see Figure 2). In such subjects, in whom the beginning is quite simple, it is normal for students to choose a simple and easy way to present the work, such as using cartoons or comics to explain a particular topic (Bringslid et al., 2011). In addition, the issue of Cryptography has been widely used in novels, films, and television series, making it especially interesting for these engineering students. Another student looked for a cipher used during the World War II, and he found the Purple cipher machine, used by Japanese Foreign Office to communicate with their diplomatic corp.

Figure 2: Example of Caesar cipher inside the proposed wiki (from Asterix and Obelix comic).

To summarize, students begin learning Cryptography history, how messages were ciphered in the ancient time, how secret messages were sent during the wars and how the spies attempted to get them. While algorithms have been greatly improved, the idea of what is Cryptography has not changed: an initial message (plaintext) is encrypted (called cryptogram) and sent over an insecure channel to a recipient, which will decrypt it to recover the original message. Using Caesar encryption, each letter is replaced by the letter occupying the 3rd position from it, and an "indecipherable" text was obtained. At present, systems such as RSA (Rivest et al, 1978), ElGamal (1985) or any other cryptosystem, the computational difficulty is very big. These algorithms require many operations to obtain the ciphertext from the plaintext, and also to decrypt and recover the plaintext from the cryptogram.

Acknowledgements

This work has been partially supported by Ministerio de Ciencia e Innovación (Spain) under the grant TIN2011-22668 (Spain), and by the University of Salamanca, grants ID2013/029 and ID2013/032.

References

Al-Hamdani, W.A., and Griskell, I. J. (2005). A proposed curriculum of cryptography courses. Proceedings of the 2nd annual conference on Information security curriculum development. ACM.

Bringslid, O., Hernández-Encinas, A., Martín del Rey, A., Martín-Vaquero, J., Queiruga-Dios, A. (2011). Case Study: Coding Theory Subject Design for Engineering Students at the University of Salamanca. *Transactions on Advanced Research*, **7**(2).

Duffy, P. and Bruns, A. (2006). The use of blogs, wikis and RSS in education: A conversation of possibilities. Proceedings of the Online Learning and Teaching Conference 2006.

ElGamal, T. (1985). A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. *IEEE Transactions on Information Theory*, **31**(4), 469-472.

García, A., García, F., Del Rey, . M., Rodríguez, G., and De La Villa, A. (2014). Changing assessment methods: New rules, new roles. *Journal of Symbolic Computation*, **61**, 70-84.

Gayoso Martínez, V., Hernández Encinas, A., Hernández Encinas, L., Queiruga Dios, A., and Visus Ruíz, I. (2010). Development of Capstone Projects on Secure Communications for Engineering Students. Proceedings of the 2010 World Congress in Computer Science, Computer Engineering, and Applied Computing (WORLDCOMP'10), The 2010 International Conference on Security and Management (SAM 2010).

Menezes, A., van Oorschot, P., Vanstone, S. (1997). *Handbook of applied cryptography*. CRC Press, Boca Raton, FL.

Parker, K. & Chao, J. (2007). Wiki as a Teaching Tool. *Interdisciplinary Journal of E-Learning and Learning Objects*, **3**(1), 57-72.

Queiruga Dios, A., Hernández Encinas, L., and Queiruga, D. (2008). Cryptography adapted to the new European Area of Higher Education, *Lect. Notes Comput Sci.*, **5101**, 706-714.

Fúster Sabater, A., Hernández Encinas, L., Montoya Vitini, F., Muñoz Masqué, J. Martín Muñoz, A. (2012). *Criptografía, protección de datos y aplicaciones*, RA-MA, Madrid.

Rivest, R.L., Shamir, A., Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems, *Commun. ACM*, **21**, 120-126