B- learning en Codificación de la Información

Alfonsa García, Ana Isabel Lías

Title— A b-learning course on Codification of Information

***Abstract*— This paper presents how a subject of Cryptography and Corrector Codes is adapted to conform to European Convergence didactic guidelines. This is a 6 ECTS course aimed at both Computer engineers and Software engineers, with a b-learning approach and a student-centered methodology based on competencies. The present paper shows the contents, methodology, assessments methods and students performance over the last two years.**

***Index Terms*— blended learning, student centered learning, cryptography, error-corrector codes, competence assessment.**

I. Introducción

El curso 2009-10, la Escuela Universitaria de Informática de la Universidad Politécnica de Madrid (UPM) puso en marcha los títulos de grado de Ingeniería de Software e Ingeniería de Computadores adaptados al Espacio Europeo de Educación, con el nuevo sistema de créditos europeos (ECTS) (ver [1]). En ambas titulaciones se ofreció un curso de adaptación para que los titulados de las antiguas Ingenierías Técnicas de Informática de Gestión e Informática de Sistemas pudieran obtener, cursando 60 ECTS en un año académico, alguno de los nuevos títulos de grado.

La mayoría de los estudiantes que acceden a este curso de adaptación lo compatibilizan con un trabajo remunerado a jornada completa y, por lo general, compatibilizar estudio y trabajo suele ser complicado. Por ello, las actividades presenciales del curso se planifican en horario de 18 a 21 horas de lunes a viernes.

De los 60 ECTS que han de cursar los estudiantes del curso de adaptación, 12 corresponden al proyecto Fin de Carrera y se pueden reconocer hasta 18 por prácticas en empresa. Además, en caso de no haberlas cursado en los estudios anteriores, deben hacer algunas asignaturas obligatorias y completar con asignaturas optativas.

La oferta de asignaturas para los estudiantes del curso de adaptación relacionadas con la Seguridad Informática es: *Implantación de la Seguridad de la Información*, obligatoria para la titulación de Ingeniería del Software, y *Codificación de la Información (CI)*, optativa para las dos titulaciones, Ingeniería del Software e Ingeniería de Computadores.

Concretamente, la asignatura *Codificación de la Información* (ver [2]) es responsabilidad del departamento de Matemática Aplicada y se ofrece en modalidad b-learning. Esta asignatura tiene asignados 6 ECTS, por lo que se estima una carga total entre 156 y 162 horas de trabajo del estudiante, de las que sólo 45 son presenciales. Para las horas no presenciales se ha usado la *Plataforma Institucional de Telenseñanza de la UPM*, basada en Moodle ([3]). Dicha herramienta presenta entre otras las siguientes ventajas:

- Facilidad de acceso, ya que es de código abierto y libre de pago.
- Facilidad de uso, ya que su manejo es muy intuitivo.
- Variedad de recursos para gestionar las actividades.
- Soporte institucional.
- Amplia difusión, lo que permite aprovechar otras experiencias (ver [4], [5], [6]).

Además, el material elaborado para la plataforma Moodle se puede usar como apoyo en un curso presencial.

II. Puesta en marcha de la asignatura

En los anteriores planes de estudio impartíamos, de manera totalmente presencial, la asignatura *Fundamentos de Criptología*. Partiendo de esta experiencia previa, diseñamos una asignatura más ambiciosa, en cuanto a contenidos y al desarrollo de competencias. Realizamos una planificación, análoga a la descrita en [4], con las siguientes fases:

1. Definición de competencias y resultados de aprendizaje.
2. Diseño de un programa de actividades de aprendizaje asequibles y que permitan alcanzar los resultados previstos.
3. Planificación de un calendario de actividades docentes.
4. Diseño de un modelo de evaluación continua, que potencie el papel formativo de la evaluación introduciendo mecanismos de retroalimentación inmediata.
5. Establecimiento de un protocolo de calidad, que incluya recogida sistemática de datos para la mejora del proceso.

El diseño y planificación de actividades supuso un reto, dado el escaso número de horas presenciales, así como el perfil de los estudiantes, que compatibilizan estudios y trabajo. Por ello, siguiendo criterios similares a los expuestos

DOI (Digital Object Identifier) Pendiente
Las autoras Alfonsa García, y Ana Isabel Lías son profesoras de la Universidad Politécnica de Madrid, del área de Matemática Aplicada, Emails (por orden de firma): alfonsa.garcia@eui.upm.es, alias@eui.upm.es.

por Alcover et alter en [7], hicimos una estricta selección de contenidos y una planificación precisa y rigurosa.

III. Competencias previstas

La asignatura *CI* se centra en el estudio, manejo y análisis de algoritmos relativos a los distintos tipos de codificación de la información según el objetivo perseguido (corregir errores, cifrar la información o comprimirla). De este modo, pretende contribuir al desarrollo de las siguientes competencias específicas de las titulaciones de Ingeniería Informática:

- Capacidad para comprender y dominar los conceptos básicos de algorítmica y complejidad computacional, y su aplicación para el tratamiento automático de la información por medio de sistemas computacionales y su aplicación para la resolución de problemas propios de la ingeniería.
- Capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos.

Además, el diseño de la asignatura contribuye al desarrollo de las siguientes competencias genéricas:

- G1: Aprendizaje autónomo.
- G2: Uso de tecnología.
- G3: Resolución de problemas.
- G4: Capacidad de análisis y síntesis.
- G5: Comunicación escrita.

Tal y como afirman Zabala y Arnau en [8], el aprendizaje de las competencias es siempre funcional. Su vinculación al contexto y la necesidad de la acción implica un planteamiento metodológico múltiple y variado. En la asignatura CI, estas competencias genéricas no se evalúan de modo separado, sino que están íntimamente ligadas a los contenidos del curso y se desarrollan y evalúan en las distintas actividades de aprendizaje y evaluación.

De modo específico, hemos establecido como resultados de aprendizaje los siguientes:

1. Distingue los distintos tipos de codificación de la información según el objetivo perseguido.
2. Identifica y conoce criptosistemas de clave pública y clave privada.
3. Cifra y descifra utilizando los criptosistemas matricial afín, RSA y ElGamal.
4. Conoce y aplica protocolos de autenticación (firma digital) basados en criptosistemas de clave pública.
5. Codifica, detecta y corrige errores utilizando los códigos lineales.
6. Conoce y aplica test de primalidad deterministas y probabilísticos.
7. Comprime ficheros usando códigos compresores.
8. Utiliza adecuadamente software para la resolución de problemas de codificación de la información.
9. Conoce la complejidad computacional de las operaciones aritméticas elementales y es capaz de determinar la de ciertos algoritmos sencillos.
10. Entiende la importancia del coste computacional de determinados algoritmos matemáticos y su relación con la seguridad de los protocolos de clave pública.
11. Redacta documentos e informes relacionados con la asignatura, escribiendo con precisión y argumentando con solidez.

Los contenidos teóricos de la asignatura (ver [9], [10], [11], [12], [13]), los hemos organizado en los siguientes temas:

1. Introducción a la Codificación de la Información y la Criptología: Transmisión de la Información. Códigos criptográficos, correctores y compresores. Criptografía: criptosistemas, clave privada y pública. Criptosistema afín y matricial. Criptoanálisis.
2. Complejidad computacional: Problemas y algoritmos. Complejidad de las operaciones aritméticas. Clasificación de los problemas según su complejidad.
3. Teoría de números: Unidades de Z_n. Función Phi de Euler. Teoremas de Euler y Fermat. Orden de un elemento. Raíz primitiva. Logaritmo discreto.
4. Criptosistemas de clave pública: Protocolo de Diffie-Hellman. Criptosistemas RSA y ElGamal. Firma digital. Otras aplicaciones.
5. Test de primalidad: Test deterministas. Criba de Eratóstenes. Divisiones sucesivas. Test probabilísticos. Test de Fermat, de Miller y de Miller-Rabin.
6. Códigos detectores/correctores de errores y códigos compresores: Códigos correctores lineales. Matriz generadora y matriz de control. Descodificación por síndrome. Códigos de Hamming. Códigos de redundancia cíclica. Polinomio generador de um código. Polinomio primitivo. Códigos compresores. Código de Huffman de varianza mínima.

IV. Metodología

Las tecnologías actuales permiten nuevas formas de aprendizaje con un mayor protagonismo del estudiante y en las que el profesor tiene un papel de guía en la construcción del conocimiento. Una de esas nuevas formas es el blended-learning o aprendizaje semipresencial, en el que se combinan sesiones de clase presencial con trabajo virtual. Este formato es muy conveniente en nuestro caso, dado el perfil de los estudiantes. Por ello ha sido elegido para impartir la asignatura.

Dado el escaso número de horas presenciales, desde el inicio los estudiantes cuentan con material de soporte para su organización y para abordar la asignatura con garantías (Fig. 1). En concreto, los estudiantes disponen de:

a) una planificación de la asignatura y una *Guía de Aprendizaje* en la que se detallan los objetivos y resultados de aprendizaje de los temas, el material a utilizar y referencias, así como instrucciones concretas sobre las actividades a realizar.

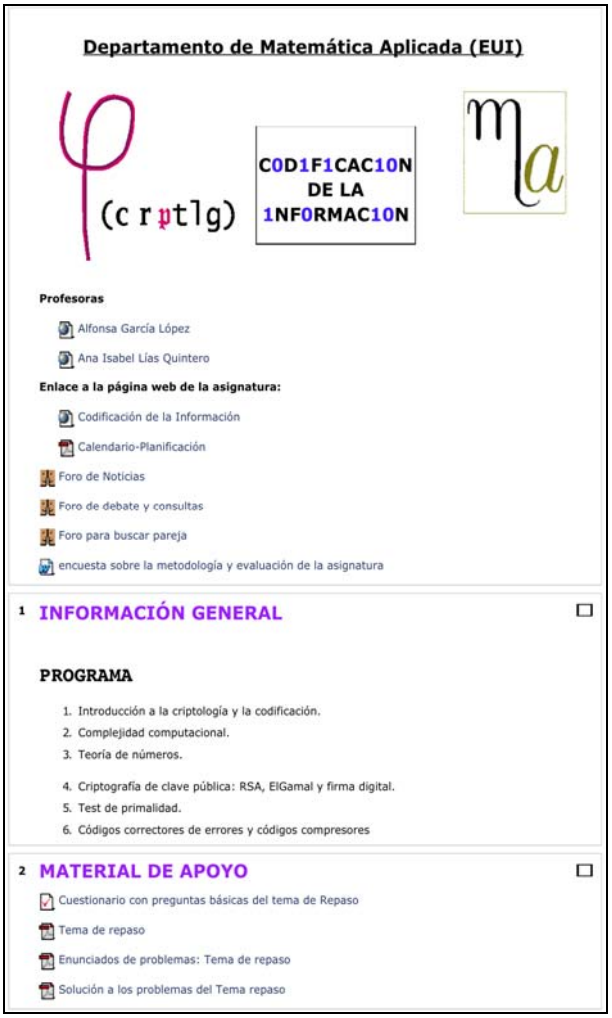

Fig. 1. Pantalla Inicial

b) unas notas y un cuestionario de repaso, que cubre todos los conceptos relativos a aritmética entera y modular que se les supone conocidos en la carrera pero que, dadas las circunstancias de este tipo de estudiantes, es altamente probable que hayan olvidado.

c) un foro de *Noticias*, para ir anunciando las distintas actividades, otro de *Debate y consultas* y otro para establecer los grupos de trabajo.

A lo largo del curso se va poniendo a disposición de los alumnos el material y las tareas correspondientes a cada tema. A continuación describimos los diferentes tipos de actividades clasificadas en presenciales y no presenciales.

ACTIVIDADES PRESENCIALES:

Las actividades presenciales se realizan en bloques de tres horas semanales, en las que se usa el método expositivo, salvo 5 sesiones de dos horas de prácticas de laboratorio. Para desarrollar las actividades, los alumnos disponen previamente del material adecuado.

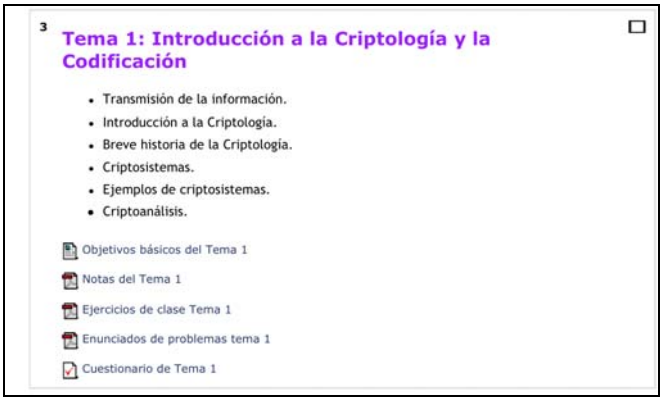

Fig. 2. Ejemplo de material de un tema.

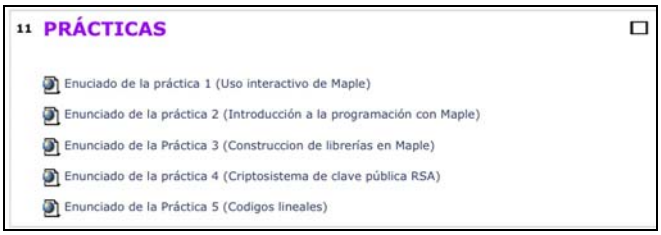

Fig. 3. Sección de prácticas.

Para cada tema hemos puesto a disposición de los estudiantes (ver Fig. 2): una lista de los objetivos básicos del tema, las notas teóricas, hojas de ejercicios básicos (de respuesta corta o aplicación directa de algún algoritmo o propiedad), hojas de problemas más elaborados y un cuestionario. En las horas presenciales se explica la teoría, se resuelven dudas de partes teóricas cuya lectura se hubiera encargado, se hacen problemas de respuesta corta intercalada con la teoría, para afianzar conceptos y finalizado el tema se realizan los problemas elaborados y globalizadores.

Para las sesiones de prácticas se usa el sistema Maple de cálculo matemático ([14]). Hemos elegido dicho sistema porque sus prestaciones lo hacen especialmente adecuado para los protocolos criptográficos: tiene implementada la aritmética entera modular y el cálculo matricial, dispone de un lenguaje de programación de alto nivel, cuenta con funciones de teoría de números, permite manejar con facilidad cadenas de caracteres y permite la creación de librerías que completan el sistema.

En las sesiones de prácticas (ver Fig. 3), el alumno se familiariza con el sistema y con su lenguaje de programación al mismo tiempo que define funciones para resolver ejercicios y problemas propios de la asignatura. Se insiste en la esquematización de procesos algorítmicos, con el fin de desarrollar la competencia G4 y se trabajan también las competencias G3 y G5.

También se incluye la realización en horario presencial de dos pruebas escritas, que incluyen preguntas teóricas y resolución de ejercicios.

ACTIVIDADES NO PRESENCIALES:

Como actividades de trabajo autónomo establecemos la lectura de documentación (desarrollo de la competencia G1), resolución de ejercicios que se envían por correo, resolución de cuestionarios on-line y realización de trabajos en grupo dirigidos (mini-proyectos). Para estas actividades hemos diseñado o utilizado las siguientes herramientas Moodle:

- Un *Foro* de *Consulta y Debate* para tutorías on-line.
- Un repositorio de documentación con material teórico, enunciados de ejercicios y prácticas y especificaciones de los proyectos.
- *Tareas* de subida avanzada de archivos para gestionar las entregas.
- *Cuestionarios* Moodle de aprendizaje y evaluación.
- *Mensajería* para el envío de ejercicios.

En cuanto al material disponible en el Moodle, se ha evitado poner una cantidad de información excesiva, una de las tentaciones en la que solemos caer los profesores y que dificulta la organización de los estudiantes ([15]). Así, las referencias bibliográficas específicas se encuentran en las notas de cada tema.

A continuación se describen las distintas actividades de aprendizaje no presenciales.

A. Mini-Proyectos

Los alumnos realizan cuatro mini-proyectos a lo largo del curso, en grupos de dos personas (ver Fig. 4). En cada uno de estos proyectos los alumnos han de estudiar algunos algoritmos, definir funciones Maple que los implementen, crear páginas de ayuda al usuario para estas funciones, hacer pruebas y ejemplos de uso de las funciones programadas y resolver con ellas algún ejercicio. En estas actividades se desarrollan las competencias G1, G2, G3 y G5.

Para cada proyecto se estima una dedicación entre 10 y 15 horas de trabajo del alumno, que se contrasta recabando los datos de dedicación real. Además se les facilita una rúbrica para que conozcan los criterios de calificación y los trabajos se les devuelven corregidos y comentados en el plazo más breve posible, para que las sugerencias de cada proyecto puedan ser usadas como mejoras para el siguiente. Los estudiantes pueden consultar las dudas presencialmente o en el foro de debate.

B. Cuestionarios on line

Para cada tema, los estudiantes deben responder a las preguntas de un cuestionario de objetivos básicos. La realización de estos cuestionarios es una actividad de aprendizaje, con una pequeña recompensa en la evaluación. Se contemplan como una innovación pedagógica de evaluación formativa ya que el entorno on-line favorece la retroalimentación y permite a los estudiantes detectar sus puntos fuertes y débiles.

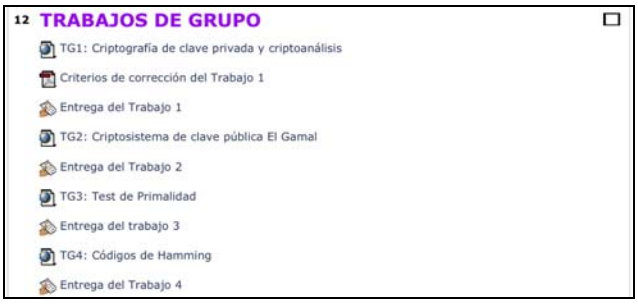

Fig. 4. Sección de mini-proyectos.

Cada cuestionario tiene diez preguntas tipo test que barren todos los aspectos básicos del tema. Para ello, hemos creado colecciones de preguntas referentes a un mismo objetivo del tema. Cuando un alumno accede a un cuestionario, éste se confecciona eligiendo aleatoriamente una pregunta de cada colección. El alumno resuelve el cuestionario en modo on-line sobre la plataforma Moodle y puede hacer varios intentos de entrenamiento durante unos días, la corrección es automática y sirve como retroalimentación, sin repercusión en la nota. Al resolver el cuestionario el estudiante dispone de toda la documentación de la asignatura y su tarea se centra en la labor de sintetizar ideas y aplicar conceptos (competencia G4).

La idea es que al hacer varios cuestionarios diferentes, pero relativos a los mismos resultados de aprendizaje, tenga oportunidad de corregir sus errores. En estos entrenamientos el profesor tutoriza la labor de los alumnos y, según convenga, puede comentar los fallos de los cuestionarios vía el foro de consulta y debate o vía correos individuales.

Después, en una fecha concreta, y tras un día sin acceso al cuestionario, los alumnos han de hacer, simultáneamente conectados on-line, el cuestionario definitivo, que es distinto para cada alumno pues se genera aleatoriamente. Deben acertar 8 de las 10 preguntas para que se les reconozca el porcentaje de nota asignado.

C. Resolución de ejercicios

Algunos ejercicios se pautan para ser realizados en horario no presencial y se envían al profesor por correo. Además del estudio del tema, esta actividad pretende desarrollar las competencias de resolución de problemas y la comunicación escrita. Los ejercicios se corrigen, aunque no puntúan para la evaluación, y el mejor ejercicio resuelto (ya corregido) se publica en la plataforma, como ejemplo motivador.

TUTORÍAS:

La labor de tutela es fundamental en un modelo de enseñanza b-learning. En la asignatura CI los estudiantes pueden acudir libremente a tutorías presenciales en los espacios y horarios habilitados al efecto. Por otra parte, se realiza una interesante labor tutorial on-line, mediante correo electrónico y en los foros de la asignatura. Lo interesante de

esta tutoría on–line es que fuerza al estudiante a plantear su duda por escrito, lo que no siempre les resulta fácil, pero es altamente formativo. Como curiosidad, cabe señalar que se registra un elevado número de consultas fuera del horario laboral y lectivo (en horario nocturno o fines de semana).

V. Modelo de evaluación

El aprendizaje basado en competencias requiere un nuevo modelo de evaluación, con una alta componente formativa. Cuando evaluamos estamos señalando al alumno lo que es importante, le guiamos en el proceso de aprendizaje y le indicamos si ha alcanzado el objetivo. Por tanto, si queremos desarrollar las competencias, hay que evaluarlas. Siguiendo criterios comúnmente admitidos como buenos para un programa de evaluación de competencias (ver [16]), hemos diseñado un modelo de evaluación continua para la asignatura CI. El porcentaje total sobre la calificación final para cada tipo de actividad es el siguiente:

- Trabajos Dirigidos: 50% (la nota de cada mini-proyecto supone un 12.5% de la nota final de la asignatura).
- Cuestionarios de Objetivos Básicos: 10% (cada cuestionario básico contribuye entre 1% y 2%).
- Pruebas escritas: 40%.

Las pruebas escritas son la única actividad de evaluación 100% presencial. Se realizan tres a lo largo del curso y contienen cuestiones teóricas, ejercicios y algún problema.

Los contenidos de cada actividad de evaluación se diseñan de acuerdo con las competencias específicas y los resultados de aprendizaje que se pretenden conseguir con el módulo correspondiente. A los alumnos se les facilita información sobre estos objetivos y aprecian bastante la mejora en su nivel de competencia.

Respecto a las competencias genéricas no se ha hecho una evaluación separada pero está claro que el modelo b-learning permite evaluar el Aprendizaje autónomo y el Uso de tecnología. Por otra parte los Mini-Proyectos nos informan de la evolución a lo largo del curso del desarrollo de las competencias Análisis y Síntesis, Resolución de problemas y Comunicación escrita.

VI. Resultados y conclusiones

Tras las primeras experiencias de impartir la asignatura CI en modalidad b-learning, y comparando los resultados con los que se tenían en la asignatura de Fundamentos de Criptología del plan de estudios anterior, se puede concluir que la modalidad de enseñanza b-learning no ha sido menos efectiva que la tradicional.

Fig. 5. Calificaciones de la promoción 11-12.

Los resultados académicos son bastante satisfactorios. La asignatura se ha impartido en los cursos 10-11 y 11-12. En el primero se matricularon 8 alumnos, todos ellos del curso de adaptación que compatibilizaban el estudio con un trabajo a jornada completa. Hubo 6 aprobados y dos personas abandonaron la asignatura sin completar las actividades previstas. La segunda vez (curso 11-12) el número de alumnos matriculados fue 25, ya que además de alumnos de adaptación teníamos algunos estudiantes de tercer curso de la primera promoción del grado, que la eligieron como optativa. En la figura 5 se muestran los resultados de esta promoción.

En los dos cursos más del 80% de los alumnos matriculados en CI ha superado la asignatura por evaluación continua.

En el modelo de enseñanza b-learning, un aspecto a tener en cuenta es que prácticamente el 50% de la nota se obtiene de actividades de evaluación no presenciales. En la promoción del curso 11-12 la calificación media fue 6.57, la contribución a esta media de las actividades presenciales fue 3.1 y la de las no presenciales 3.47. Para analizar la fiabilidad de las calificaciones obtenidas en actividades no presenciales hemos hecho un análisis de varianza, que nos permite afirmar que no se aprecian diferencias estadísticamente significativas entre las medias de los dos tipos de actividades con un nivel de confianza del 95% y un p-valor de 0.122.

Dentro del protocolo de calidad también se contrasta el tiempo dedicado a cada mini-proyecto. La media de tiempo para los trabajos oscila entre las 10 y 15 horas pautadas, aunque algunos dedican más de 20 horas.

Para medir el grado de satisfacción de los estudiantes hemos usado las encuestas de evaluación de la actividad docente, que son anónimas y se hacen regularmente todos los cursos en la EU de Informática. En la TABLA I se muestran los resultados de los cursos 10-11 y 11-12. El rango para las respuestas es de 1 = totalmente desacuerdo a 6 = totalmente de acuerdo.

TABLA I . Encuesta de satisfacción (rango 1..6).

PREGUNTA	curso 10-11	curso 11-12
Las tareas programadas se adecúan a las competencias previstas	5.25	5.1
La coordinación entre teoría y práctica es adecuada	4.9	4.8
El volumen de contenidos es adecuado a los créditos	4.8	4.9
La dedicación se corresponde a la prevista	3.8	4.1
El modelo de evaluación es adecuado	5.1	5.2
He mejorado mi nivel en relación con las competencias previstas	5.2	5.1

LÍNEAS DE TRABAJO FUTURAS:

De cara al futuro, trasladando a nuestro contexto otras experiencias (ver [7]), hemos abierto una línea de ampliación en temas de Seguridad enfocada a la dirección de Proyectos Fin de Grado. La idea es ofrecer a los estudiantes la posibilidad de manejar otros protocolos y estrategias relacionadas con la Criptología y la Seguridad Informática, como es el caso de los Criptosistemas de Curvas Elípticas, que no podemos abarcar en el curso por falta de tiempo. En la actualidad ya estamos dirigiendo proyectos que, además, se podrán poner a disposición de futuros alumnos de la asignatura, con el fin de ofrecer una panorámica más amplia de la criptografía.

REFERENCIAS

[1] European Commission, Directorate-General for Education and Cultures (2009) "ECTS users' guide". Accesible (30 de mayo de 2012) en http://ec.europa.eu/dgs/education_culture/publ/educ-training_en.htm

[2] A. García; A. Lías, "Guía de aprendizaje de Codificación de la Información", 2011. Accesible en (30 de mayo de 2012) https://www.eui.upm.es/node/1331

[3] Moodle http://moodle.org (30 de mayo de 2012)

[4] P. Canto, I. Gallego, J. Manuel, J. Mora, A. Reyes, E. Rodríguez, K. Sanjeevan, E. Santamaría, y M. Valero, "Cómo usamos Moodle en nuestras asignaturas adaptadas al EEES" *IEEE-RITA*, 5, n.3, 2010, pp.75-85.

[5] M.T. Carracedo, C. Pérez, P. Ramírez, B. Salazar, "Implantación coordinada del entorno virtual Moodle y su utilización en la Escuela Universitaria de Informática de la Universidad Politécnica de Madrid". *Jornadas Internacionales de Innovación Educativa (INECE)*, 2009. Madrid. Proceedings en CD. ISBN 978-84-692-9417-8

[6] M.T. Pérez Rodríguez, "Innovación en docencia universitaria con Moodle. Casos prácticos". ECU, 2009.

[7] P. Alcover, J. Suardíaz, P. Navarro, "Adaptación de la docencia de una asignatura de criptografía a las recomendaciones del EEES". *IEEE-RITA*, 4, n.2, 2009, pp.95-101.

[8] A. Zabala, L. Arnau, "Cómo aprender y enseñar competencias". Grao, 2007. ISBN: 84-7827-500-7

[9] N. Koblitz, "A course in Number Theory and Cryptography" (2nd Ed.). Spriger Verlag, 1998.

[10] W. Trappe, L. Washington, "Introduction to Cryptography with Coding Theory". Prentice-Hall, 2002.

[11] C. Munuera, J.Tena, "Codificación de la Información". Universidad de Valladolid, 1997. ISBN:84-7762-764-9

[12] A. Bruen, M. Forcinito, "Cryptography, Information Theory and error-correction", Wiley-Interscience, 2005.

[13] R. Durán, L. Hernández, J. Muñoz, "El criptosistema RSA". RA-MA, 2005.

[14] García, A; Martínez, A; Rincón, F.: "Cálculo científico con Maple". RA-MA, 1995.

[15] S. Bemposta, M.J. García, J.J. Escribano, "El b-learning a examen: ventajas, desventajas y opiniones". *Higher Learning Reserch Communications*, 1, nº 1, 2011.

[16] L. Baartman, T. Bastiaens, P. Kirschner, and C. Van der Vleuten, "The Wheel of Competency Assessment: Presenting Quality Criteria for Competency Assessment Programs". Studies in Educational Evaluation, 32, 2006, pp. 153-170.

Alfonsa García López. Es doctora en Matemáticas por la Universidad Complutense de Madrid desde 1985 y Profesora Titular de Universidad de la Universidad Politécnica de Madrid desde 1987. Ha trabajado en Análisis Matemático y en Didáctica de la Matemáticas, sobre todo en relación con el uso de tecnologías. Es coordinadora del grupo de Innovación educativa GIEMATIC de la U.P.M.

Ana Isabel Lías Quintero. Es licenciada en Matemáticas por la Universidad Complutense de Madrid (1987) y Profesora Titular de Escuela Universitaria de la Universidad Politécnica de Madrid desde 1989. Es profesora de las asignaturas de Álgebra, Matemática Discreta y Codificación de la Información. Es miembro del grupo de Innovación educativa GIEMATIC de la U.P.M.