UNIVERSIDAD COMPLUTENSE DE MADRID

FACULTAD DE INFORMATICA

Ficha del curso: 2015-2016

Grado: GRADO EN INGENIERÍA INFORMÁTICA		**Curso**: Optativas generales 3º y 4º **(** 2C **)**
Asignatura: 803305 - Criptografía y teoría de códigos **Asignatura en Inglés**:	**Abrev:** CTC	6 **ECTS**
Materia: Complementos de matemáticas e investigación operativa		12 **ECTS**
Otras asignaturas en la misma materia: Investigación Operativa		6 ECTS
Módulo: Optativo		
Departamento: Algebra **Coordinador:** Alonso García, Mª Emilia		

Descripción de contenidos mínimos:

Criptografía y Teoría de Códigos

Programa detallado:

1. Algoritmos básicos de la aritmética de enteros y anillos de polinomios con coeficientes en un cuerpo. Complejidad binaria.
2. Cuerpos finitos. Caracterización y representación.
3. Códigos correctores de errores. Distancia de Hamming y cotas.
4. Códigos lineales.Algunas familias de códigos, Problema de la decodificación de códigos lineales.
5. Códigos cíclicos. Construcción de códigos cíclicos : códigos BCH y de Reed Salomón. Decodificación de BCH con algoritmo Berlekamp-Massey.
6. Conceptos básicos y tareas de la Criptografía de Clave Pública. Criptografía clásica.
7. Cifrado en flujo, LFSR's y ataques.
8. Funciones de una dirección. Funciones resumen (" hash"). Complejidad de problemas , P y NP , en la aritmética de enteros. Criptografía de Clave Pública. Autentificación. Firma digital.
9. Sistemas criptográficos basados en el problema del logaritmo discreto (DLP). Protocolo de Diffie-Hellmann-Meckle. Sistema "El Gamal ", DSS y otros protocolos basados en DLP. Ataques a DLP.
10. Sistemas criptográficos basados en el problema de la factorización de enteros. RSA. Protocolos basados en RSA. Ataques a RSA. Algoritmo "Rho" de Pollard y algoritmo QS.
12. Otros protocolos: Prueba sin conocimiento, votación electrónica, dinero digital.

Programa detallado en inglés:

First part:

Elementary algorithms for integer arithemtic and polynomials arithmetic over a field.
Binary complexity of EEA. Finite fields: characterization and representation.
Libraries in Maple and SAGE.Error-correcting codes. Hamming distance. Some bounds.
Linear codes, cyclic codes, BCH codes, Reed Salomon codes. The problem of de-codification.

Second part:

Basic concepts on Cryptography and its history. Symetric Cryptography versus public Cryptography. Stream Ciphers. Complexity of problems in Arithmetic and Combinatorics: P and NP. One way functions, hash functions.
Public key Cryptography based on DLP. Some attacks and protocols: DSS.
Public key Cryptography based on the factorization problem: RSA. Attacks:
modern integer factorization algorithms. Zero knowledge protocols. Electronic voting, digital cash.

Competencias de la asignatura:

Generales:

CG1-Capacidad para la resolución de los problemas matemáticos que puedan plantearse en la ingeniería. Aptitud para aplicar los conocimientos sobre: álgebra lineal; cálculo diferencial e integral; métodos numéricos; algorítmica numérica; estadística y optimización.

Específicas:

No tiene

Básicas y Transversales:

CT1-Capacidad de comunicación oral y escrita, en inglés y español utilizando los medios audiovisuales habituales, y para trabajar en equipos multidisciplinares y en contextos internacionales.

CT2-Capacidad de análisis y síntesis en la resolución de problemas.

CT3-Capacidad para gestionar adecuadamente la información disponible integrando creativamente conocimientos y aplicándolos a la resolución de problemas informáticos utilizando el método científico.

CT4-Capacidad de organización, planificación, ejecución y dirección de recursos humanos.

Fecha: ____ de _____ de _____

Firma del Director del Departamento:

CT5-Capacidad para valorar la repercusión social y medioambiental de las soluciones de la ingeniería, y para perseguir objetivos de calidad en el desarrollo de su actividad profesional.

Resultados de aprendizaje:

No tiene

Evaluación:

Todas las pruebas realizadas en cada asignatura serán comunes a todos los grupos de la misma.
Al tener las materias optativas muy diversas características la calificación de las mismas podrá ser muy variada, por lo que los rangos se dejan muy abiertos:

- Exámenes sobre la materia: 0-60%
- Otras actividades: 100-40%

En el apartado "Otras actividades" se podrá valorar la participación activa en el proceso de aprendizaje, la realización de prácticas y ejercicios y la realización de otras actividades dirigidas. La realización de las prácticas de laboratorio y del resto de las actividades evaluables será obligatoria.
Antes del comienzo de cada curso escolar se concretarán en las fichas docentes los porcentajes exactos que se utilizarán durante ese curso para la evaluación de la materia, siendo comunes estos criterios para todos los grupos de una misma asignatura.
La calificación reflejará los resultados de aprendizaje de las diferentes competencias que se adquieren en el módulo o materia.

Evaluación detallada:

La evaluación de la asignatura se realizará vía : examen, entrega de ejercicios y práctica de programación. Con los porcentajes que se expresan a continuación:
- La práctica de programación se realizará en grupos de 2 a 4 alumnos cuyo número de integrantes dependerá del número de alumnos que asistan asiduamente a clase y deseen realizarla. Ésta constituirá un 40% de la calificación final.
La evaluación de dicha práctica se hará vía su presentación en grupo a la profesora, y durante la realización de la misma los integrantes del grupo deben demostrar conocer los algoritmos en que dicha práctica se basa y no solo la correcta ejecución del programa. La calificación de la práctica será individual.
- La entrega de ejercicios asidua durante el correspondiente cuatrimestre constituirá un 10% de la calificación total.
- El examen se valorará en el 50% de la calificación total.

Exámenes: En Lab Final Jun y Final Sep .
En el caso en que el alumno por circunstancias especiales no pueda asistir asiduamente a clase, no tendrá opción arealizar la práctica de programación por considerar que su realización requiere una tutorización continua por parte del profesor, y se le calificará únicamente el examen y la entrega de ejercicios siempre que se asista a corregirlos personalmente a las tutorías.
Las calificaciones serán sobre 10.

Exámenes:

☑ En Aula	☐ En Lab
☐ Final Feb	☐ Parcial Feb
☑ Final Jun	☐ Parcial Jun
☑ Final Sep	☐ Sin Examen

Actividades formativas:

Las actividades formativas que se van a realizar para esta materia se dividen en tres grupos:
Actividades presenciales: 30-40% de la dedicación del alumno. Estas actividades podrán incluir:
Clases teóricas magistrales.
Clases de problemas.
Laboratorios.
Seminarios.
Actividades dirigidas: 10-15% de la dedicación del alumno. Estas actividades podrán incluir:
Trabajos dirigidos.
Tutorías dirigidas.
Trabajo personal: 50-55% de la dedicación del alumno. Estas actividades podrán incluir:
Trabajo personal no dirigido: Estudio, preparación de exámenes, realización de ejercicios.
Realización de exámenes.

Actividades docentes:

Reparto de créditos:	Otras actividades:
Teoria: 4,00	--Clases magistrales, apoyadas por herramienta informática de cálculo simbólico .
Problemas: 2,00	
Laboratorios: 0,00	--Resolución de problemas individual y presentación de estos en clase.

Fecha: ____ de _____ de _____

Firma del Director del Departamento:

Bibliografía:

- Buchmann, J.A. : "Introduction to Cryptography". Undergraduate Texts in Maths. Springer- Verlag 2nd. de. (2004).
- Gómez-Pardo, J.L.: "Introduction to Cryptography with Maple". Springer-Verlag, 2013.
- Koblitz, N.: "A course in Number Theory and Cryptography". Springer- Verlag 2nd. ed., 1994. (GTM 1149.
- Lidl, R., Gunter, P.: "Applied Abstract Algebra". 2nd. ed. Springer 1997.
- Stinson D. R. : "Cryptography Theory and Practice. 3rd. Ed . In "Discrete Mathematics and its Applications". Taylor&Francis, LLC, CRC Press (2005).
- Trappe W. Washington L.: "Cryptography with Coding Theory". Prentice Hall; 2nd. ed. (2005)

Ficha docente guardada por última vez el **02/07/2015 9:37:00** por el usuario: **Secretaría Administrativa de Decanato**

Fecha: ____ de _____ de _____

Firma del Director del Departamento:

UNIVERSIDAD COMPLUTENSE DE MADRID

FACULTAD DE INFORMATICA

Fecha: ____ de _____ de _____

Firma del Director del Departamento: