GUIA DOCENTE DE LA ASIGNATURA

Criptografía y Computación

Curso 2013-2014

MÓDULO	MATERIA	CURSO	SEMESTRE	CRÉDITOS	TIPO
Complementos de Computación y Sistemas Inteligentes	Complementos de Sistemas Inteligentes	4º	1º	6	Optativa

PROFESOR(ES)	DIRECCIÓN COMPLETA DE CONTACTO PARA TUTORÍAS (Dirección postal, teléfono, correo electrónico, etc.)
• Pedro A. García Sánchez (a) • Jesús García Miranda (b)	(a) Despacho 39, Departamento de Álgebra, Facultad de Ciencias, Campus Fuentenueva, Teléfono 958243375 pedro@ugr.es (b) Despacho 2.14, Departamento de Álgebra, Escuela de Ingeniería Informática y Telecomunicaciones Teléfono 958240824 jesusgm@ugr.es
	HORARIO DE TUTORÍAS
	(a) www.ugr.es/local/pedro/tutorias.html (b) algebra.ugr.es/pages/personal/fichas_profesores/jesusgm/profesor
GRADO EN EL QUE SE IMPARTE	OTROS GRADOS A LOS QUE SE PODRÍA OFERTAR
Grado en Ingeniería Informática	Grado en Matemáticas, Grado en Telecomunicaciones, Doble grado en Matemáticas e Informática

PRERREQUISITOS Y/O RECOMENDACIONES (si procede)
No es necesario que los alumnos tengan aprobadas asignaturas, materias o módulos previos como requisito indispensable para cursar este módulo. No obstante se recomienda la superación de los contenidos y adquisición de competencias de las materias de formación básica y de rama, en particular de las asignaturas

- Álgebra y Estructuras Matemáticas,
- Lógica y Métodos Discretos.

BREVE DESCRIPCIÓN DE CONTENIDOS (SEGÚN MEMORIA DE VERIFICACIÓN DEL GRADO)

Introducción a la criptografía: Descripción, problemas y métodos. Criptografía clásica. Paradigmas de cómputo en criptografía: Algoritmos y complejidad. Aritmética de precisión múltiple entera y modular. Implementación eficiente. Criptografía de llave secreta. Criptografía de llave pública. Ataques sobre algoritmos. Ataques Fuerza Bruta. Capacidad de cálculo. Protocolos criptográficos y aplicaciones.

COMPETENCIAS GENERALES Y ESPECÍFICAS

- Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado
.
- Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía
.
- Capacidad para resolver problemas con iniciativa, toma de decisiones, autonomía y creatividad. Capacidad para saber comunicar y transmitir los conocimientos, habilidades y destrezas de la profesión de Ingeniero Técnico en Informática.

- Capacidad para el uso y aplicación de las TIC en el ámbito académico y profesional.

OBJETIVOS (EXPRESADOS COMO RESULTADOS ESPERABLES DE LA ENSEÑANZA)

- Conocer el recorrido histórico de los principales criptosistemas empleados en la antigüedad y sus ataques más efectivos.
- Repasar la aritmética necesaria para definir y conocer los algoritmos criptográficos.
- Conocer la complejidad algorítmica de las herramientas que se aplicarán posteriormente en la definición de los algoritmos criptográficos. Fundamentalmente los cálculos de potencias y logaritmos, el cálculo de raíces cuadradas y los algoritmos de factorización de enteros.
- Diseñar estructuras de datos que nos permitan trabajar con enteros de precisión arbitraria.
- Analizar la complejidad de las operaciones aritméticas clásicas para los diseños anteriores.
- Conocer algoritmos de multiplicación rápida de enteros, como los originados en el algoritmo de Karatsuba y los basados en aritmética modular y FFT, así como sus respectivas complejidades.
- Conocer los algoritmos de aritmética de precisión múltiple enteros y modulares: Reducciones de Montgomery y Barret, algoritmos de Lehmer y Garner y algoritmos de exponenciación rápida.
- Conocer los aspectos de implementación eficiente de los algoritmos anteriores y su repercusión en el funcionamiento de los mismos.
- Conocer los principales algoritmos de clave secreta, sus especificaciones y algunos criterios

de diseño. Capacidad para medir comparativamente la velocidad de proceso de los mismos.
- Distinguir claramente los conceptos de algoritmo por bloque y algoritmo de flujo. Conocer las fortalezas de cada uno de ellos.
- Conocer el paradigma de algoritmo criptográfico de clave pública.
- Describir los principales algoritmos de clave pública basados en problemas de aritmética entera.
- Abstraer algunos de los conocimientos anteriores para diseñar algoritmos en estructuras algebraicas más complejas.
- Entender las fortalezas y debilidades comparadas de los criptosistemas de clave secreta y los criptosistemas de clave pública.
- Enumerar los principales ataques a cada algoritmo.
- Capacidad para realizar un ataque a Fuerza Bruta sobre un algoritmo, teniendo en cuenta las disponibilidades de cómputo, y de realizar una estimación sobre su coste.
- Estimar el coste de uso de los distintos algoritmos criptográficos y de sus ataques.
- Capacidad para poner en funcionamiento un ataque al algoritmo basado en criterios de complejidad en casos de muestra: factorización, logaritmo discreto u otros.
- Distinguir entre ataques a los algoritmos criptográficos y ataques al uso de los mismos.
- Conocer el problema de la distribución de claves y algunas de sus soluciones.
- Enumerar distintos métodos de certificación digital y conocer sus estándares.
- Describir el uso de los algoritmos criptográficos para situaciones concretas en las que se hace necesario proteger la confidencialidad de la información y la privacidad en las comunicaciones.

TEMARIO DETALLADO DE LA ASIGNATURA

TEMARIO TEÓRICO
- Tema 1. Introducción y revisión histórica.
- Tema 2. Aritmética de múltiple precisión. Aritmética modular. Primalidad.
- Tema 3. Cifrado en flujo.
- Tema 4. Cifrado por bloques simétrico. Redes de Feistel. DES. AES.
- Tema 5. Cifrado por bloques asimétrico. RSA. El Gammal.
- Tema 6. Aplicaciones criptográficas. Autentificación y firmas digitales. Protocolos criptográficos.

TEMARIO PRÁCTICO
Prácticas de Ordenador
- Práctica 1. Aritmética modular. Primalidad.
- Práctica 2. Secuencias pseudo-aleatorias.
- Práctica 3. Funciones de un solo sentido. Firmas digitales.

BIBLIOGRAFÍA

BIBLIOGRAFÍA FUNDAMENTAL

- O. Geddes, S. R. Czapor, G. Labahn, Algorithms for Computer Algebra, Springer, 1992.
- P. Caballero, Introducción a la criptografía. 2ª edición, RA-MA 2002.
- G. Brassard, Moderm Cryptography, a tutorial, Springer-Verlag, 1988.
- G. Dawson, Cryptography: policy and algorithms, 1996.

- N. Koblitz, A course in number theory and cryptography, Springer-Verlag, 1979.
- A. Fúster ,Técnicas cirptográficas de protección de datos. 3ª ed. Actualizada, Ed. RA-MA 2004.
- D.R. Stinson , Cryptography: Theory & Practice, CRC 1995.
- J. Pastor Franco, M.A. Sarasa López, J.L. Salazar Riaño, Criptografía Digital: Fundamentos y aplicaciones. Prensas Universitarias de Zaragoza.
- J. Ortega, M.A. López Guerrero, Eugenio C. García del Castillo, Introducción a la criptografía: Historia y actualidad, Universidad de Castilla la Mancha.
- J. Gutiérrez, J. Tena, Protocolos criptográficos y seguridad en redes, Universidad de Cantabria.

BIBLIOGRAFÍA QUE SE PUEDE ENCONTRAR EN INTERNET

- P. J. Cameron, Notes on cryptography
  http://www.maths.qmul.ac.uk/~pjc/notes/crypt.pdf
- S. Goldwasser, M. Bellare, Lecture notes on cryptography
  http://cseweb.ucsd.edu/~mihir/papers/gb.pdf
- A. J. Menezes, P. van Oorschot, S. A. Vaustone, HAC
  http://www.cacr.math.uwaterloo.ca/hac/
- N. Smart, Cryptography: An introduction
  http://www.cs.bris.ac.uk/~nigel/Crypto_Book/book.ps
- Criptografia y Seguridad en Computadores de Manuel Lucena López, Universidad de Jaén
  http://wwwdi.ujaen.es/local/mlucena/lcripto.html
- Fundamentals of Cryptology, A professional reference and interactive manual, Henk C. A. van Tilborg
  http://www.win.tue.nl/~henkvt/cryptobook/cryptodict.pdf

ENLACES RECOMENDADOS

- N. Smart slides
  http://www.cs.bris.ac.uk/Teaching/Resources/COMS30124/Lec...
- Jorge Ramió Aguirre's notes on security and cryptography
  http://www.criptored.upm.es/guiateoria/gt_m001a_en.htm
- Proyecto TEAS
  http://proyectoteas.blogspot.com/
- Stick figures to explain AES
  http://www.moserware.com/2009/09/stick-figure-guide-to-ad...
- Apuntes de Matemática Discreta
  http://ocw.ugr.es/course/view.php?id=20

METODOLOGÍA DOCENTE

- **Lecciones magistrales**: 3 créditos.
- **Acontecimientos científicos o divulgativos**: Asistencia a posibles conferencias sobre temas relacionados con el curso.
- **Prácticas de laboratorio**: 3 créditos, implementación de algoritmos en un lenguaje de programación elegido por el alumno bajo el asesoramiento del profesor.

- **Prácticas autónomas**: Realización de un trabajo personal sobre un tema elegido por el alumno sobre los tópicos del curso. Revisión bibliográfica de antecedentes, metodología y recursos.

EVALUACIÓN (INSTRUMENTOS DE EVALUACIÓN, CRITERIOS DE EVALUACIÓN Y PORCENTAJE SOBRE LA CALIFICACIÓN FINAL, ETC.)

- Un cincuenta por ciento de la evaluación se basará en las prácticas entregadas y defendidas por los alumnos dentro de los plazos que se fijarán a lo largo del curso.
- El resto de la evaluación se basará en presentaciones sobre temas propuestos y en un examen teórico práctico.
- Para los estudiantes que se acojan a la evaluación única final, esta modalidad de evaluación estará formada por todas aquellas pruebas que el profesor estime oportunas, de forma que se pueda acreditar que el estudiante ha adquirido la totalidad de las competencias generales y específicas descritas en el apartado correspondiente de esta Guía Docente.
- Todo lo relativo a la evaluación se regirá por la Normativa de evaluación y calificación de los estudiantes vigente en la Universidad de Granada, que puede consultarse en: http://secretariageneral.ugr.es/bougr/pages/bougr71/ncg712/

RÉGIMEN DE ASISTENCIA

- La asistencia a las clases teóricas no será obligatoria, aunque la participación activa en clase y la entrega de ejercicios planteados por el profesor se tendrá en cuenta dentro del sistema de evaluación continua de la asignatura.
- La asistencia a las clases prácticas no será obligatoria. En cualquier caso, la asistencia y participación activa en clase se tendrá en cuenta dentro del sistema de evaluación continua de la asignatura.