GUIA DOCENTE DE LA ASIGNATURA (∾)

Criptografía y Computación

(Fecha última actualización: 02/07/2020)
(Fecha de aprobación en Consejo de Departamento: 14/07/2020)

MÓDULO	MATERIA	CURSO	SEMESTRE	CRÉDITOS	TIPO
Complementos de computación y sistemas inteligentes	Complementos de sistemas inteligentes	4º	2º	6	Optativa

PROFESORES[1]	DIRECCIÓN COMPLETA DE CONTACTO PARA TUTORÍAS (Dirección postal, teléfono, correo electrónico, etc.)
Pedro A. García Sánchez	Departameto de Álgebra, Facultad de Ciencias, Despacho 39. Correo electrónico: pedro@ugr.es
	HORARIO DE TUTORÍAS Y/O ENLACE A LA PÁGINA WEB DONDE PUEDAN CONSULTARSE LOS HORARIOS DE TUTORÍAS[1]
	www.ugr.es/local/pedro/tutorias.html

GRADO EN EL QUE SE IMPARTE	OTROS GRADOS A LOS QUE SE PODRÍA OFERTAR
Grado en Ingeniería Informática	Grado en Matemáticas

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 la asignatura de Álgebra Lineal y Estructuras Matemáticas.

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

Introducción a la criptografía: Descripción, problemas y métodos. Criptografía clásica. Paradigmas

[1] Consulte posible actualización en Acceso Identificado > Aplicaciones > Ordenación Docente
(∾) Esta guía docente debe ser cumplimentada siguiendo la "Normativa de Evaluación y de Calificación de los estudiantes de la Universidad de Granada" (http://secretariageneral.ugr.es/pages/normativa/fichasugr/ncg7121/!)

Firma (1): LUIS MIGUEL MERINO GONZALEZ
En calidad de: Director/a de Departamento

Este documento firmado digitalmente puede verificarse en https://sede.ugr.es/verifirma/
Código seguro de verificación (CSV): 9828BBA38B7E513561739FD0CC87FC2F

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

El título de Graduado/a en Ingeniería Informática de la Universidad de Granada ha obtenido, con fecha 5 de junio de 2019, el sello Euro-Inf, otorgado por ANECA en colaboración con el Consejo General de Colegios Profesionales de Ingeniería en Informática (CCII) y con el Consejo General de Colegios Oficiales de Ingeniería Técnica en Informática (CONCITI). Esta acreditación garantiza el cumplimiento de criterios y estándares reconocidos por los empleadores españoles y del resto de Europa, de acuerdo con los principios de calidad, relevancia, transparencia, reconocimiento y movilidad contemplados en el Espacio Europeo de Educación Superior.

Competencias básicas y generales

CB4: Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado.

CB5: Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía

E4: Capacidad para definir, evaluar y seleccionar plataformas hardware y software para el desarrollo y la ejecución de sistemas, servidios y aplicaciones informáticas.

E8: Conocimiento de las materias básicas y tecnologías, que capaciten para el aprendizaje y desarrollo de nuevos métodos y tecnologías, así como las que les doten de una gran versatilidad para adaptarse a nuevas situaciones.

E9: 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.\\

Competencias transversales

T2: Capacidad para tomar decisiones basadas en criterios objetivos (datos experimentales, científicos o de simulación disponibles) así como capacidad de argumentar y justificar lógicamente dichas decisiones, sabiendo aceptar otros puntos de vista.

T3: 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.

Firma (1): LUIS MIGUEL MERINO GONZALEZ
En calidad de: Directo/a de Departamento

Este documento firmado digitalmente puede verificarse en https://sede.ugr.es/verifirma/
Código seguro de verificación (CSV): 9828BBA38B7E513561739FD0CC87FC2F

- Analizar la complejidad de las operaciones aritméticas clásicas para los diseños anteriores.
- 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.

Firma (1): LUIS MIGUEL MERINO GONZALEZ
En calidad de: Director/a de Departamento

UNIVERSIDAD DE GRANADA
INFORMACIÓN SOBRE TITULACIONES DE LA UGR
grados.ugr.es

Este documento firmado digitalmente puede verificarse en https://sede.ugr.es/verifirma/
Código seguro de verificación (CSV): **9828BBA38B7E513561739FD0CC87FC2F**

- 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.

ENLACES RECOMENDADOS

- 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 https://www.cs.umd.edu/~waa/414-F11/IntroToCrypto.pdf
- Editor Henk C. A. van Tilborg , Encyclopedia of Cryptography and Security https://link.springer.com/referencework/10.1007/0-387-23483-7

METODOLOGÍA DOCENTE

Lección Magistral: Presentación en el aula de los conceptos propios de la materia haciendo uso de metodología expositiva con lecciones magistrales participativas ilustradas con variedad de ejemplos.

Resolución de problemas: Realización en el aula de distintos ejercicios donde se abordan los diferentes tópicos de la asignatura.

Prácticas en Laboratorio: En el laboratorio probaremos diferentes formas de resolver problemas criptográficos y analizaremos la eficiencia de éstas.

Exposición de Trabajos Tutelados: Los estudiantes deberán realizar un trabajo en grupos (2-4 personas) sobre un tema elegido por ellos. Este trabajo deberán exponerlo ante los demás estudiantes, que podrán preguntar y debatir sobre el tema.

Tutorías académicas: En el horario establecido, los estudiantes podrán realizar consultas personalizadas al profesor, así como exponer los distintos trabajos prácticos que hayan realizado.

EVALUACIÓN (INSTRUMENTOS DE EVALUACIÓN, CRITERIOS DE EVALUACIÓN Y PORCENTAJE SOBRE

Firma (1): LUIS MIGUEL MERINO GONZALEZ
En calidad de: Directorla de Departamento

LA CALIFICACIÓN FINAL, ETC.)

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/bougr112/_doc/examenes/!

Preferentemente, la evaluación se ajustará al sistema de evaluación continua del aprendizaje del estudiante siguiendo el artículo 7 de la anterior Normativa.

El criterio de evaluación se especifica a continuación:

- 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.
- Un 20 por ciento de la evaluación se basará en la elaboración y presentación ante el profesor y el resto de estudiantes de un trabajo sobre un tema elegido por el estudiante.
- Un 30 por ciento de la nota vendrá dada por el examen teórico práctico que se realizará una vez finalizado el curso.

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.

En las convocatorias extraordinarias la evaluación consistirá en un examen general.

El sistema de calificaciones se expresará mediante calificación numérica de acuerdo con lo establecido en el art. 5 del R. D 1125/2003, de 5 de septiembre, por el que se establece el sistema europeo de créditos y el sistema de calificaciones en las titulaciones universitarias de carácter oficial y validez en el territorio nacional.

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, exceptuando las sesiones en las que se programen pruebas de evaluación. En cualquier caso, la asistencia y participación activa en clase se tendrá en cuenta dentro del sistema de evaluación continua de la asignatura.

DESCRIPCIÓN DE LAS PRUEBAS QUE FORMARÁN PARTE DE LA EVALUACIÓN ÚNICA FINAL ESTABLECIDA EN LA "NORMATIVA DE EVALUACIÓN Y DE CALIFICACIÓN DE LOS ESTUDIANTES DE LA UNIVERSIDAD DE GRANADA"

Según la normativa vigente, la evaluación única final, entendiendo por tal la que se realiza en un solo acto académico, podrá incluir cuantas pruebas sean necesarias para acreditar que el estudiante ha adquirido la totalidad de las competencias descritas en la Guía Docente de la asignatura.

ESCENARIO A (ENSEÑANZA-APRENDIZAJE PRESENCIAL Y NO PRESENCIAL)

ATENCIÓN TUTORIAL

HORARIO	HERRAMIENTAS PARA LA ATENCIÓN TUTORIAL

Firma (1): LUIS MIGUEL MERINO GONZALEZ
En calidad de: Director/a de Departamento

Este documento firmado digitalmente puede verificarse en https://sede.ugr.es/verifirma/
Código seguro de verificación (CSV): **9828BBA38B7E513561739FD0CC87FC2F**

(Según lo establecido en el POD)	(Indicar medios telemáticos para la atención tutorial)
www.ugr.es/local/pedro/tutorias.html	Mensajería, plataforma docente, videoconferencia.
MEDIDAS DE ADAPTACIÓN DE LA METODOLOGÍA DOCENTE	
De acuerdo con el modelo y horarios establecidos por el centro, se complementará la docencia presencial con el uso de plataforma docente y docencia online a través de videoconferencia.	
MEDIDAS DE ADAPTACIÓN DE LA EVALUACIÓN (Instrumentos, criterios y porcentajes sobre la calificación final)	
Convocatoria Ordinaria	
La evaluación será preferiblemente presencial, aunque no se descarta que alguna de las pruebas se lleve a cabo en modalidad online a través de plataforma docente o videoconferencia.	
Convocatoria Extraordinaria	
La evaluación será preferiblemente presencial, aunque no se descarta que alguna de las pruebas se lleve a cabo en modalidad online a través de plataforma docente o videoconferencia.	
Evaluación Única Final	
La evaluación será preferiblemente presencial, aunque no se descarta que alguna de las pruebas se lleve a cabo en modalidad online a través de plataforma docente o videoconferencia.	
ESCENARIO B (SUSPENSIÓN DE LA ACTIVIDAD PRESENCIAL)	
ATENCIÓN TUTORIAL	
HORARIO (Según lo establecido en el POD)	HERRAMIENTAS PARA LA ATENCIÓN TUTORIAL (Indicar medios telemáticos para la atención tutorial)
www.ugr.es/local/pedro/tutorias.html	Mensajería, plataforma docente, videoconferencia.
MEDIDAS DE ADAPTACIÓN DE LA METODOLOGÍA DOCENTE	
• Distribución de materiales teóricos y prácticos a través de plataforma docente. • Clases a través de videoconferencia.	
MEDIDAS DE ADAPTACIÓN DE LA EVALUACIÓN (Instrumentos, criterios y porcentajes sobre la calificación final)	
Convocatoria Ordinaria	
La evaluación será online mediante plataforma docente o videoconferencia.	

Firma (1): LUIS MIGUEL MERINO GONZALEZ
En calidad de: Directo/a de Departamento

Este documento firmado digitalmente puede verificarse en https://sede.ugr.es/verifirma/
Código seguro de verificación (CSV): 9828BBA38B7E513561739FD0CC87FC2F

Convocatoria Extraordinaria
La evaluación será online mediante plataforma docente o videoconferencia.
Evaluación Única Final
La evaluación será online mediante plataforma docente o videoconferencia.

Firma (1): **LUIS MIGUEL MERINO GONZALEZ**
En calidad de: **Director/a de Departamento**

Este documento firmado digitalmente puede verificarse en https://sede.ugr.es/verifirma/
Código seguro de verificación (CSV): **9828BBA38B7E513561739FD0CC87FC2F**