Guía docente de la asignatura

Criptografía y Computación (Especialidad Computación y Sistemas Inteligentes)

Fecha última actualización: 15/06/2021
Fecha de aprobación: 15/06/2021

Grado	Grado en Ingeniería Informática	**Rama**	Ingeniería y Arquitectura
Módulo	Complementos de Computación y Sistemas Inteligentes	**Materia**	Complementos de Sistemas Inteligentes

Curso	4º	**Semestre**	2º	**Créditos**	6	**Tipo**	Optativa

PRERREQUISITOS Y/O RECOMENDACIONES

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 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 ASOCIADAS A MATERIA/ASIGNATURA

COMPETENCIAS GENERALES

- CG04 - Capacidad para definir, evaluar y seleccionar plataformas hardware y software para el desarrollo y la ejecución de sistemas, servicios y aplicaciones informáticas.
- CG08 - 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.
- CG09 - Capacidad para resolver problemas con iniciativa, toma de decisiones, autonomía y creatividad. Capacidad para saber comunicar y transmitir los conocimientos,

Firma (1): Universidad de Granada
CIF: Q1818002F

Firmado electrónicamente según artículo 41.1.j) del Reglamento de Adm. Electrónica de la Universidad de Granada (BOJA nº 85 de 6 de mayo de 2021)
Este documento firmado digitalmente puede verificarse en https://sede.ugr.es/verifirma/ 21/02/2022 - 09:00:35
Código seguro de verificación (CSV): 401755ED0E0140B18A42A4F944394A5A Pág. 1 de 5

habilidades y destrezas de la profesión de Ingeniero Técnico en Informática.

RESULTADOS DE APRENDIZAJE (Objetivos)

- 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 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.

PROGRAMA DE CONTENIDOS TEÓRICOS Y PRÁCTICOS

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

Firma (1): Universidad de Granada
CIF: Q1818002F

Firmado electrónicamente según artículo 41.1.j) del Reglamento de Adm. Electrónica de la Universidad de Granada (BOJA nº 85 de 6 de mayo de 2021)
Este documento firmado digitalmente puede verificarse en https://sede.ugr.es/verifirma/ 21/02/2022 - 09:00:35
Código seguro de verificación (CSV): 401755ED0E0140B18A42A4F944394A5A Pág. 2 de 5

criptográficos.

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 COMPLEMENTARIA

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

Firma (1): Universidad de Granada
CIF: Q1818002F

Firmado electrónicamente según artículo 41.1.j) del Reglamento de Adm. Electrónica de la Universidad de Granada (BOJA nº 85 de 6 de mayo de 2021)
Este documento firmado digitalmente puede verificarse en https://sede.ugr.es/verifirma/ 21/02/2022 - 09:00:35
Código seguro de verificación (CSV): 401755ED0E0140B18A42A4F944394A5A Pág. 3 de 5

METODOLOGÍA DOCENTE

- MD01 Lección Magistral (Clases Teóricas-Expositivas)
- MD02 Actividades Prácticas (Resolución de Problemas, Resolución de Casos Prácticos, Desarrollo de Proyectos, Prácticas en Laboratorio, Taller de Programación, Aula de Informática, Prácticas de Campo).
- MD03 Seminarios (Debates, Demos, Exposición de Trabajos Tutelados, Conferencias, Visitas Guiadas, Monografías).
- MD04 Actividades no presenciales Individuales.
- MD05 Actividades no presenciales Grupales.
- MD06 Tutorías Académicas.

EVALUACIÓN (instrumentos de evaluación, criterios de evaluación y porcentaje sobre la calificación final)

EVALUACIÓN ORDINARIA

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 este enlace.

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 una o varias pruebas teórico-prácticas que se realizarán durante el curso o tras su finalización.

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.

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

Firma (1): Universidad de Granada
CIF: Q1818002F

Firmado electrónicamente según artículo 41.1.j) del Reglamento de Adm. Electrónica de la Universidad de Granada (BOJA nº 85 de 6 de mayo de 2021)
Este documento firmado digitalmente puede verificarse en https://sede.ugr.es/verifirma/ 21/02/2022 - 09:00:35
Código seguro de verificación (CSV): 401755ED0E0140B18A42A4F944394A5A Pág. 4 de 5

se tendrá en cuenta dentro del sistema de evaluación continua de la asignatura.

EVALUACIÓN EXTRAORDINARIA

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

EVALUACIÓN ÚNICA FINAL

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.

Firma (1): Universidad de Granada
CIF: Q1818002F

Firmado electrónicamente según artículo 41.1.j) del Reglamento de Adm. Electrónica de la Universidad de Granada (BOJA nº 85 de 6 de mayo de 2021)
Este documento firmado digitalmente puede verificarse en https://sede.ugr.es/verifirma/ 21/02/2022 - 09:00:35
Código seguro de verificación (CSV): **401755ED0E0140B18A42A4F944394A5A** Pág. 5 de 5