Guía docente de la asignatura

Criptografía y Computación (Especialidad Computación y Sistemas Inteligentes) (29611AF)

Fecha de aprobación: **20/06/2022**

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.
- 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 FB.
- 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, habilidades y destrezas de la profesión de Ingeniero Técnico en Informática.

COMPETENCIAS TRANSVERSALES

- CT02 - 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.
- CT03 - Capacidad para el uso y aplicación de las TIC en el ámbito académico y profesional.

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. Aritmética de múltiple precisión. Aritmética modular. Primalidad.
- Tema 2. Criptografía simétrica.
- Tema 3. Criptografía asimétrica.
- Tema 4. Aplicaciones criptográficas. Autentificación y firmas digitales. Protocolos criptográficos.

PRÁCTICO

Prácticas de Ordenador

- Práctica 1. Aritmética modular. Primalidad.
- Práctica 2. Secuencias pseudo-aleatorias.
- Práctica 3. Criptosistemas simétricos.
- Práctica 4. RSA
- Práctica 5. Hash.
- Práctica 6. DH, DSA
- Práctica 7. ECDH, ECDSA

BIBLIOGRAFÍA

BIBLIOGRAFÍA FUNDAMENTAL

- O. Geddes, S. R. Czapor, G. Labahn, Algorithms for Computer Algebra, Springer, 1992.
- J. von zur Gathen, J. Gerhard. Modern Computer Algebra. Cambridge University Press, 2003.
- H. Delfs and H. Knebl. Introduction to Cryptography. Information Security and Cryptography. Springer-Verlag Berlin Heidelberg, 2015.
- N. P. Smart. Cryptography Made Simple. Information Security and Cryptography. Springer International Publishing, 2016.
- J. von zur Gathen. CryptoSchool. Springer-Verlag Berlin Heidelberg, 2015.

BIBLIOGRAFÍA COMPLEMENTARIA

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).

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 cincuenta por ciento de la nota vendrá dado por una o varias pruebas teórico-prácticas que se realizarán durante el curso o tras su finalización.

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.

EVALUACIÓN EXTRAORDINARIA

La evaluación será de la siguiente forma

- Un cincuenta por ciento de la evaluación se basará en las prácticas. El alumno podrá decidir mantener la calificación de la parte correspondiente realizadas a lo largo del curso, o entregar y defender aquellas prácticas que determine el profesor en la convocatoria.
- Un cincuenta por ciento de la nota vendrá dado por una prueba teórico-práctica realizada en la fecha acordada por la Junta de Centro.

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.