Guía Docente

DATOS DE IDENTIFICACIÓN

Titulación:	Grado en Ingeniería Matemática
Rama de Conocimiento:	Ingeniería y Arquitectura
Facultad/Escuela:	Escuela Politécnica Superior
Asignatura:	Criptografía
Tipo:	Obligatoria
Créditos ECTS:	6
Curso:	3
Código:	4970
Periodo docente:	Sexto semestre
Materia:	Ingeniería Matemática Aplicada
Módulo:	Proyectos de Aplicación
Tipo de enseñanza:	Presencial
Idioma:	Castellano
Total de horas de dedicación del alumno:	150

Equipo Docente	Correo Electrónico
Adrián Jesús Trejo Gil	adrian.trejo@ufv.es

DESCRIPCIÓN DE LA ASIGNATURA

La asignatura Criptografía quiere profundizar con el alumno en una de las aplicaciones más relacionadas con el mundo de la ingeniería de las Matemáticas siendo éste clave para la seguridad informática, los códigos de comunicación y los algoritmos de cifrado y descifrado. Esta asignatura contribuye al desarrollo de la capacidad de razonamiento matemático, la abstracción y la aplicación de los conocimientos a ámbitos de la ingeniería, pilares fundamentales para la formación del matemático y para el ejercicio de su profesión.

OBJETIVO

El objetivo de la asignatura de Criptografía será conocer las matemáticas que hay detrás de los algoritmos más conocidos de seguridad en las comunicaciones a distancia. Para ello se requerirá de unas nociones básicas de Teoría de Grupos, Teoría de Cuerpos y Aritmética Modular.

Es también necesario conocer nociones básicas sobre Análisis Complejo para conocer los algoritmos de cifrado mediante Curvas Elípticas.

También será imprescindible tener nociones básicas de programación y conocer el programa Matlab debido a que ciertas prácticas grupales se harán en Matlab.

CONOCIMIENTOS PREVIOS

Se recomienda al alumno que conozca Aritmética Modular, Teoría de Grupos y Cuerpos, análisis complejo y programación en Matlab.

CONTENIDOS

Tema 1. Introducción a la aritmética modular:
*Números primos y factorización
*Espacio cociente
*Aritmética Modular
*Máximo Común Divisor y Algoritmo de Euclides
*Identidad de Bezout
*Teorema Chino del Resto y Función de Contar de Euler

Tema 2. Álgebra Abstracta:
*Teoría de Grupos
*Grupos cíclicos y abelianos
*Teoría de Cuerpos
*Teorema Fundamental del Álgebra
*Extensiones algebraicas y trascendentes
*Irreducibilidad de polinomios

Tema 3. Cifrado de códigos:
*Introducción y distancia de Hamming
*Codificación y descodificación
*Operaciones con códigos lineales

Tema 4. Cifrado de clave pública y clave privada:
*Función de Hash
*Cifrado RSA
*Seguridad del cifrado RSA
*Búsqueda de números primos y problema de factorización de enteros

Tema 5. Análisis complejo y espacio proyectivo
*Repaso de números complejos
*Espacio proyectivo
*Funciones holomorfas
*Ceros y polos de una función, funciones meromorfas
*Series de Laurent y Teorema de Cauchy
*Teorema de los Residuos y funciones elípticas

Tema 6. Cifrado de curvas elípticas:
*Función de Weierstrass y latices
*Mapa entre el Toro y Curvas Elípticas
*Teorema de Uniformización
*Aplicación del cifrado en curvas elípticas

ACTIVIDADES FORMATIVAS

Las actividades formativas, así como la distribución de los tiempos de trabajo, pueden verse modificadas y adaptadas en función de los distintos escenarios establecidos siguiendo las indicaciones de las autoridades sanitarias.

La metodología seguida en esta asignatura está dirigida a conseguir un aprendizaje significativo por parte del alumno de los conceptos y técnicas fundamentales de la materia. Por ese motivo se combinan sesiones "Lección Expositiva" con "Clases Prácticas" y "Presentación y Defensa de Trabajos", de manera que se favorezca la participación del alumno y la interacción alumno-profesor y alumno-alumno como vía para fomentar el aprendizaje colaborativo y la capacidad de autoaprendizaje, todo ello mediante estrategias de resolución de problemas y metodologías de intervención. Las actividades no presenciales, que pueden ser tanto de tipo individual como colectivo, serán supervisadas por el profesor en clases y "Tutorías", tanto individuales como de grupo, estando encaminadas a favorecer el aprendizaje autónomo y colaborativo.

El trabajo presencial se completará con trabajo autónomo por parte del alumno, en algunos casos desarrollados en grupo, de manera que se fomente el aprendizaje cooperativo. Las actividades de carácter no presencial previstas incluyen el "Estudio y Trabajo Individual", que permitirá trabajar en la fijación de los conceptos teóricos abordados en las sesiones de "Lección Expositivas" correspondientes a todas las materias del módulo y adquirir la destreza práctica que se persigue con las clases prácticas, que aplicarán el aprendizaje por descubrimiento basado en problemas. Para el desarrollo de las competencias y habilidades en esta asignatura es igualmente importante el "Trabajo en Grupo". Todo el estudio y trabajo realizado por el alumno será supervisado y guiado por el profesor mediante "Tutorías", individuales o en grupo. En algunos casos, el alumno tendrá que realizar en clase la exposición de las principales conclusiones de su estudio o trabajo, lo que permitirá el intercambio de conocimientos y experiencias entre alumnos.

Finalmente, con el fin de facilitar al alumno el acceso a los materiales y la planificación de su trabajo, así como la comunicación con el profesor y el resto de alumnos, se empleará el Aula Virtual, que es una plataforma de aprendizaje que ofrece diferentes recursos electrónicos para complementar, de forma muy positiva, el aprendizaje del alumno.

DISTRIBUCIÓN DE LOS TIEMPOS DE TRABAJO

ACTIVIDAD PRESENCIAL	TRABAJO AUTÓNOMO/ACTIVIDAD NO PRESENCIAL
60 horas	90 horas
Clase expositiva participativa 13h Tutorías en pequeños grupos con el fin de profundizar en contenidos didácticos específicos, tutorías individuales o grupales 5h Clases prácticas 10h Laboratorio 26h Evaluación 6h	Estudio teórico y práctico 38h Trabajos individuales o en grupo 47h Trabajo virtual en red 5h

COMPETENCIAS

Competencias básicas

Que los estudiantes hayan demostrado poseer y comprender conocimientos en un área de estudio que parte de la base de la educación secundaria general, y se suele encontrar a un nivel que, si bien se apoya en libros de texto avanzados, incluye también algunos aspectos que implican conocimientos procedentes de la vanguardia de su campo de estudio

Que los estudiantes sepan aplicar sus conocimientos a su trabajo o vocación de una forma profesional y posean las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro de su área de estudio

Que los estudiantes tengan la capacidad de reunir e interpretar datos relevantes (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética

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

Competencias generales

Capacidad para aplicar técnicas, modelos y herramientas matemáticas y computacionales, así como las metodologías de gestión y planificación, a la resolución de proyectos en entornos reales, en diferentes ámbitos de aplicación.

Competencias específicas

Capacidad para diseñar y descifrar códigos que oscurezcan o clarifiquen la información recogida por los sistemas informáticos utilizando herramientas matemáticas y modelos de representación del lenguaje.

Capacidad para modelar y resolver matemática y algorítmicamente problemas en el ámbito de la industria conectada.

RESULTADOS DE APRENDIZAJE

Entender y modelar problemas asociados a criptografía

Comprender y ser capaz de demostrar proposiciones y teoremas elementales de aritmética modular

Comprender conceptos elementales de Teoría de Grupos y Cuerpos y saber aplicarlos a la criptografía

Comprender el cifrado de códigos y sus resultados más elementales

Conocer el sistema clave pública y clave privada y aplicarlo

Comprender conceptos claves del análisis complejo y saber demostrar los teoremas clásicos

Comprender el cifrado de curvas elípticas y saber aplicarlo

SISTEMA DE EVALUACIÓN DEL APRENDIZAJE

SISTEMA DE EVALUACIÓN:

El sistema de evaluación consiste en tres partes fundamentales para la convocatoria Ordinaria:

-Exámenes escritos de carácter teórico-práctico (70%). Se harán dos exámenes escritos agrupados por temas durante el cuatrimestre para evaluar el aprendizaje de los contenidos expuestos en las clases teóricas y de problemas. Los exámenes presenciales son liberatorios para el examen final siempre y cuando la nota de cada parcial sea igual o mayor de 5 puntos sobre 10. Si no se supera esta nota, en el examen final el alumno se examinará de todos los contenidos teóricos y prácticos de la parte correspondiente de la asignatura. Para superar con éxito la asignatura, se debe obtener al menos una nota de 5 sobre 10 en esta parte.

-Preparación y presentación de trabajos de carácter individual y/o colectivo (20%). Se evaluará la presentación tanto oral como escrita de los trabajos realizados en grupo y tutelados por el profesor, así como la evaluación de problemas propuestos y resueltos de manera individual por parte de los alumnos. La evaluación de los problemas propuestos permite evaluar los conocimientos del alumnado de una forma constante. Se debe obtener al menos una nota de 5 sobre 10 en esta parte.

-Participación en el desarrollo de las clases y asistencia (10%): La participación activa, el interés mostrado durante las clases magistrales y la intervención durante los problemas propuestos en clase serán evaluadas positivamente. En esta parte de la calificación no hay recuperación ni nota mínima.

El último porcentaje solo será evaluado cuando la asistencia registrada del alumno sea de al menos el 80%. (Excepto faltas justificadas)

Para superar la asignatura con éxito, se deberá alcanzar un mínimo de 5 puntos sobre 10, una vez sumadas todas las partes. No se redondearán notas.

Convocatoria Extraordinaria:

Se realizará una única prueba teórico-práctica correspondiente al 70% de la calificación final. Para superar con éxito la asignatura, se debe obtener al menos una nota de 5 sobre 10 en esta parte.

Las prácticas y trabajos (20%) podrán recuperarse, presentando ejercicios a determinar por el profesor, siempre antes de la fecha de examen de la convocatoria extraordinaria. Para superar con éxito la asignatura, se debe obtener al menos una nota de 5 sobre 10 en esta parte.

La parte correspondiente a la participación en clase (10%) no se recuperará, salvo dispensa expresa de la Dirección del Grado, en cuyo caso, podrá recuperarse asistiendo a un número variable de tutorías con el/los profesor/profesores responsable/s de la asignatura.

Para superar la asignatura con éxito, se deberá alcanzar un mínimo de 5 puntos sobre 10, una vez sumadas todas las partes.

SISTEMA DE EVALUACIÓN ALTERNATIVO en caso de no poder realizar los exámenes presenciales por causas de fuerza mayor (SITUACIÓN COVID-19):

- CONVOCATORIA ORDINARIA:

En caso de confinamiento total o imposibilidad de realizar los exámenes de manera presencial, el sistema de evaluación consistirá en la realización de uno o más exámenes en remoto a través del aula virtual (70% de la nota final) y a través de boletines de problemas propuestos, prácticas de programación o trabajos grupales que serán resueltos individualmente por los alumnos (20% de la nota final), realizando una grabación de vídeo explicando el procedimiento y demostrando sus conocimientos. La participación activa en las clases online, interés por la asignatura determinará el 10% restante de la nota final.

En caso de que algún alumno sea positivo en COVID-19 pero no haya confinamiento total aparte de seguir todos los protocolos se aplazará la convocatoria presencial de su examen para su posterior realización de manera presencial, entendiendo que un alumno con COVID-19 no debería realizar un examen mientras dure su situación y será tratado como situación de fuerza mayor.

El profesor podrá llamar a examen oral a cualquier alumno después de los exámenes y/o prácticas y antes de la firma de actas, haya sospecha o no de haber infringido alguna norma según el reglamento de la UFV. Podrá alterarse la nota de la prueba escrita en su totalidad según los conocimientos y competencias que el alumno demuestre en dicha prueba oral, que será grabada y archivada. Si el alumno rechazase acudir al examen oral en la cita propuesta, se considerará como "no presentado" y se podrá calificar la prueba con una nota de 0 sobre 10, anulando la nota obtenida en la prueba escrita. Este procedimiento será especialmente utilizado en casos de sospecha de copia o actividades fraudulentas.

Para superar la asignatura con éxito, se deberá alcanzar un mínimo de 5 puntos sobre 10, una vez sumadas todas las partes.

- CONVOCATORIA EXTRAORDINARIA:

Se repetirá el procedimiento de la convocatoria ordinaria.

* Si los exámenes no se pudieran realizar de forma presencial ni de la forma alternativa anteriormente detallada, se realizarán de forma remota mediante las herramientas que determine la Universidad Francisco de Vitoria, garantizando siempre la evaluación de las competencias y resultados de aprendizaje de la asignatura.

Notas de carácter general:

El alumno dispone de 6 convocatorias para superar esta asignatura. La Normativa de Evaluación de la UFV recoge todo lo relativo a los procesos de evaluación y consumo de convocatorias.

Cualquier fraude o plagio (*) por parte del alumno en una actividad evaluable será comunicado a la Dirección del Grado y sancionado según se recoge en la Normativa de Convivencia de la Universidad Francisco de Vitoria.

(*) Se considera "plagio" cualquier tipo de copia de cuestiones o ejercicios de examen, memorias de trabajos, prácticas, etc., ya sea de manera total o parcial, de trabajos ajenos al alumno con el engaño de hacer creer al profesor que son propios.

BIBLIOGRAFÍA Y OTROS RECURSOS

Básica

Rubinstein-Salzedo, Simon, Cryptography REVERTE, ISBN: 978-3-319-94818-8. Año de edición: 2018

J.F. Fernando, J.M Gamboa: Ecuaciones Algebraicas. Extensiones de cuerpos y teoría de Galois. Editorial Sanz y Torres. ISBN: 9788416466528. Año de edición: 2017

Complementaria

J.F. Fernando, J.M Gamboa: Estructuras Algebraicas, ISBN: 978-8416466511. Año de edición: 2018

Lang, Serge, Complex Analysis ISBN: 978-1-4757-3083-8. Año de edición: 1999

David Loeffler, Elliptic Curves Lecture Notes. Año de edición: 2015

Andrew V. Sutherland, Lecture Notes 15, 16. Año de publicación 2017