Guía Docente

DATOS DE IDENTIFICACIÓN

Titulación:	Grado en Ingeniería Matemática
Ámbito	Ingeniería Informática y de Sistemas.
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
Jorge Andrés Plazas Vargas	jorge.plazas@ufv.es
Ernesto Correa Velandia	ernesto.correa@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.

En la asignatura se desarrollan de manera paralela y complementaria los resultados matemáticos subyacentes a la criptografía moderna junto con sus fundamentales.
Para afianzar el conocimiento de los resultados el curso tiene una fuerte componente práctica basada en problemas concretos, ejemplos y aplicaciones. Dichos problemas y ejemplos se trabajarán a mano en algunos casos y serán implementados computacionalmente en otros. Para el curso se utilizará el software para matemáticas Sage, el cual se basa sobre el lenguaje de programación Python extendiendo este a un entorno algebraico computacional robusto y de fácil uso.

OBJETIVO

El objetivo final de esta asignatura es que el alumno obtenga una profunda comprensión de los algoritmos y rutinas fundamentales de la criptografía moderna, basando dicha comprensión en un sólido entendimiento de las matemáticas subyacentes a algoritmos y rutinas.

CONOCIMIENTOS PREVIOS

Conocimiento de los contenidos de las asignaturas correspondientes al ciclo básico del grado en Ingeniería Matemática. En particular se requieren las destrezas propias de los cursos “Matemáticas Discretas” y “Álgebra II”. Conocimientos básicos de programación en Python.

CONTENIDOS

Los contenidos del curso cubren los resultados matemáticos sobre los cuales se basa la criptografía moderna, así como sus protocolos y algoritmos fundamentales de esta. La temática se divide en las siguientes secciones:

- Esquemas de cifrado simétrico y criptoanálisis básico.
- Teoría de números elemental: Teorema del resto, teorema fundamental de la aritmética y algoritmo de Euclides.
- Aritmética modular y cuerpos finitos. Teorema chino del residuo y teorema de Fermat.
- Esquemas de cifrado por substitución. Cifrado de clave privada.
- Protocolo de intercambio de claves de Diffie-Hellman.
- El problema del logaritmo discreto en cuerpos finitos.
- Cifrado de clave pública.
- Esquema de cifrado de ElGamal.
- Anillos y factorización. Formula de Euler.
- Sistema de cifrado RSA.
- Grupos cíclicos.
- Problema del logaritmo discreto para grupos cíclicos.
- Curvas elípticas sobre cuerpos finitos.
- Cifrado basado en curvas elípticas.

ACTIVIDADES FORMATIVAS

La metodología a seguir consistirá en la exposición de contenidos, ejercicios y problemas por parte del profesor con participación activa de los estudiantes durante las sesiones. Se usará el modelo de exposición activa y participativa por parte de los alumnos. Las prácticas en el aula se desarrollan mediante las siguientes actividades:

- Resolución de problemas de manera escrita con distintos grados de complejidad.
- Resolución de problemas utilizando Sage.
- Exposición en el aula por parte del alumno de problemas/ejercicios que implique la aplicación de los conocimientos fundamentales de la asignatura así como la asimilación por parte del alumno de dichos conceptos.

Estas actividades tendrán contrapartes de trabajo autónomo fuera del aula para así afianzar los conocimientos adquiridos. También se asignarán lecturas para ahondar en distintos aspectos del área.
En las pruebas de evaluación de la adquisición de contenidos (exámenes), se podrá evaluar la capacidad de aprendizaje autónomo y los resultados de aprendizaje.
Se realizarán tutorías con atención individual al alumno con el objetivo de revisar y debatir los temas presentados en clase y aclarar dudas. Los horarios de tutorías son flexibles a la necesidad del alumno por lo que debe enviar un mail al profesor. Las citas serán fijadas por el profesor y comunicadas a los 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 Canvas, la plataforma de aprendizaje online que ofrece diferentes recursos electrónicos para complementar el aprendizaje del alumno. Allí se dispondrá de los materiales de la asignatura, se plantearán las tareas que deben entregar los alumnos, se añadirán enlaces de interés sobre la asignatura y se podrá habilitar un foro de comunicación entre el profesor y los alumnos.

DISTRIBUCIÓN DE LOS TIEMPOS DE TRABAJO

ACTIVIDAD PRESENCIAL	TRABAJO AUTÓNOMO/ACTIVIDAD NO PRESENCIAL
60 horas	90 horas
• Clases expositivas participativas 13h • Resolución de problemas o casos prácticos 10h • Actividades participativas grupales 5h • Prácticas en laboratorio 26h • Seguimiento académico y actividades de evaluación 6h	• Trabajo personal y estudio autónomo 85h • Aula virtual: trabajo virtual en red, revisión y visionado de material, chats 5h

RESULTADOS DE APRENDIZAJE

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

RESULTADOS DE APRENDIZAJE ESPECIFICOS

Entender y aplicar los resultados fundamentales de la teoría de números elemental y la aritmética modular.

Comprender distintos paradigmas de cifrado y su complejidad en relación con problemas como el problema de

factorización y el problema del logaritmo discreto.

Analizar e implementar los algoritmos y rutinas fundamentales de la criptografía moderna, entendiendo el papel que juegan en esta los esquemas de cifrado simétrico y los esquemas de cifrado de clave pública.

Conocer técnicas de cifrado basadas en curvas elípticas.

SISTEMA DE EVALUACIÓN DEL APRENDIZAJE

SISTEMAS DE EVALUACIÓN. Existen dos sistemas de evaluación:

- Evaluación continua: alumnos que asisten a clase y realizan las tareas y actividades solicitadas por el profesor junto con la asistencia a clase obligatoria al menos en un 80% de las sesiones.
- Sistema alternativo de evaluación: alumnos UFV en estancia de intercambio, para los que no es necesaria la asistencia y no tienen que solicitar la dispensa, y alumnos con dispensa académica aprobada. En cualquiera de los casos, es responsabilidad del alumno su conocimiento y seguimiento.

Los alumnos que matriculen la asignatura por segunda vez o sucesivas podrán acogerse al sistema de evaluación continua, en cuyo caso tendrán que cumplir con todos los requisitos, incluida la asistencia a clase, o acogerse al sistema alternativo de evaluación, siempre y cuando tengan concedida la dispensa académica.
CONVOCATORIA ORDINARIA. El sistema de evaluación que se realizará en la asignatura recoge los siguientes parámetros y ponderación en la calificación de la nota del cuatrimestre:

1. Pruebas teórico-prácticas: 70%.
2. Presentación y defensa de trabajos individuales o de equipo: 20%
3. Participación activa en las actividades presenciales en el aula: 10%. La participación en clase solo será evaluada cuando la asistencia registrada del alumno sea de al menos el 80%. Los alumnos sujetos al sistema alternativo de evaluación tendrán que asistir a 3 tutorías durante el periodo docente ordinario para completar el 10% asignado a la Participación.

Para poder ponderar los elementos detallados en la evaluación el alumno debe tener una calificación de al menos 4 en los exámenes escritos.
CONVOCATORIA EXTRAORDINARIA. En la convocatoria extraordinaria el alumno se examinará del contenido total de la asignatura. Además:

- Si el alumno se ha presentado al examen de Convocatoria ordinaria, se tendrá en cuenta el trabajo académico desarrollado durante el curso manteniendo los criterios descritos anteriormente, guardando las calificaciones asociadas. Se le dará la posibilidad de volver a examinarse del apartado 2 a través de las pruebas que establezca el profesor.
- Si el alumno no se ha presentado al examen de Convocatoria Ordinaria, tendrá que examinarse del apartado 2 a través de las pruebas que establezca el profesor.

NOTAS DE CARÁCTER GENERAL:

- Las conductas de plagio, así como el uso de medios ilegítimos en las pruebas de evaluación, serán sancionados conforme a lo establecido en la Normativa de Evaluación y la Normativa de Convivencia de la universidad.
- 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.

BIBLIOGRAFÍA Y OTROS RECURSOS

Básica

Jeffrey Hoffstein , Jill Pipher , Joseph H. Silverman An Introduction to Mathematical Cryptography 2
Springer 2014

William Stallings Cryptography and Network Security: Principles and Practice 8
Pearson 2020

Complementaria

Kenneth Rosen Discrete Mathematics and its Applications 8
McGraw Hill 2019