Guía Docente

DATOS DE IDENTIFICACIÓN

Titulación:	Grado en Ingeniería Informática
Rama de Conocimiento:	Ingeniería y Arquitectura
Facultad/Escuela:	Escuela Politécnica Superior
Asignatura:	Criptografía
Tipo:	Optativa
Créditos ECTS:	3
Curso:	4
Código:	5656
Periodo docente:	Octavo semestre
Materia:	Tecnologías de la Información
Módulo:	Tecnología Específica
Tipo de enseñanza:	Presencial
Idioma:	Castellano
Total de horas de dedicación del alumno:	75

Equipo Docente	Correo Electrónico
José Luis de Miguel Álvarez	joseluis.demiguel@ufv.es
Javier Vázquez Pereda	j.vazquez.prof@ufv.es

DESCRIPCIÓN DE LA ASIGNATURA

La asignatura tiene como finalidad presentar los conceptos fundamentales y las técnicas de seguridad a través de los fundamentos matemáticos de la criptografía. Para ello se profundizará en la criptografía y el criptoanálisis. Se atenderán a los criptosistemas de clave privada y pública, cifrado simétrico, funciones Hash y Mac, así como los esquemas de establecimiento de clave, cifrado asimétrico y firma digital. Se finalizará la asignatura analizando los

protocolos criptográficos y estándares: transformaciones de cifrado, técnicas mixtas, esquemas y protocolos de identificación.

OBJETIVO

La asignatura persigue presentar los objetivos de seguridad de la información, y presentar, entender y aplicar los fundamentos matemáticos de la criptografía para dar solución a dichos objetivos.
Se atenderán a los criptosistemas de clave privada y pública, cifrado simétrico, funciones Hash y Mac, firma digital, certificados digitales, e Infraestructura de Clave Pública (PKI)
Se realizarán análisis de los protocolos criptográficos y estándares.

CONOCIMIENTOS PREVIOS

Se recomienda haber cursado y tener aprobado las asignaturas troncales de la rama de matemáticas.
Conocimientos deseables:
- Matemática discreta
- Programación
- Redes de Comunicaciones

CONTENIDOS

Tema 1: Introducción a la Criptografía
Tema 2: Criptografía clásica
Tema 3: Criptografía de clave simétrica
Tema 4: Criptografía de clave pública. PKI.
Tema 5: Aplicaciones de la Criptografía

ACTIVIDADES FORMATIVAS

La asignatura cuenta con:
- Lecciones expositivas
- Actividades prácticas
- Trabajos colaborativos en grupos

DISTRIBUCIÓN DE LOS TIEMPOS DE TRABAJO

ACTIVIDAD PRESENCIAL	TRABAJO AUTÓNOMO/ACTIVIDAD NO PRESENCIAL

40 horas	35 horas

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 concebir y desarrollar sistemas o arquitecturas informáticas centralizadas o distribuidas integrando hardware, software y redes, de acuerdo con los conocimientos adquiridos según lo establecido en el apartado 5 de esta memoria.

Competencias específicas

Comprender y aplicar los criptosistemas, sus características, principales arquitecturas y estándares más releventes.

RESULTADOS DE APRENDIZAJE

Conocer la historia de los principales criptosistemas empleados en la antigüedad y sus ataques más efectivos.

Conocer los aspectos básicos de la teoría de la información y de complejidad necesarios para definir un buen criptosistema

Conocer los principales algoritmos tanto basados en clave simétrica como los basados en clave pública, sus especificaciones, fortalezas y debilidades, y algunos criterios de diseño.

Conocer los diferentes campos de aplicación de la criptografía

SISTEMA DE EVALUACIÓN DEL APRENDIZAJE

CONVOCATORIA ORDINARIA
El sistema de evaluación contempla varios tipos de pruebas, distribuidos de la siguiente manera:
- [1] Examen teórico práctico: 60 %. Examen tipo test con contenidos teórico-prácticos de la asignatura. Pueden existir varias pruebas de este tipo a lo largo del curso.
- [2] Defensa escrita de trabajos: 30%. Documentos con la resolución de las prácticas. Puede solicitarse presentación presencial para revisar la autoría.
- [3] Participación e implicación en la asignatura: 10 %

Calificación_final** = [1] * 0,6 + [2] * 0,3 + [3] * 0,1

**Para superar la asignatura es necesario tener aprobadas las primeras dos partes que contempla el sistema de evaluación ([1], y [2]). En caso de suspender la asignatura por no haber superado alguna de dichas partes, la calificación máxima que podrá obtenerse en la convocatoria es 4,0 independientemente del valor que resultara del calculo de la calificación final.

En el caso de existir varias pruebas de [1] a lo largo del curso deben superarse todas ellas con calificación mayor o igual a 5,0. Para alumnos que no hayan obtenido calificación en [1] superior a 5,0 pero la media de los dos valores resulta superior a 5,0 se analizará su situación de manera individual por parte de los profesores de la asignatura.

En relación con las prácticas [2], deben obtenerse una media superior a 5,0. Para hacer media, debe alcanzarse en ellas una calificación de al menos 4,0.

Para puntuar en el apartado de participación en clase [3], es necesario asistir al menos a un 70% de las clases.

DISPENSA ACADÉMICA
Aquellos alumnos que estén exentos de la obligación de asistir a clase, bien por segunda matrícula en la asignatura o sucesivas, bien por contar con autorización expresa de la Dirección del Grado, serán evaluados por el mismo tipo de pruebas. El 10 % correspondiente a la participación e implicación se evaluará en base a la entrega de los ejercicios correspondientes en la fecha establecida.

CONVOCATORIA EXTRAORDINARIA
En el caso de no tener superada alguna de las dos primeras partes de la asignatura ([1], y [2]) en la convocatoria ordinaria, el alumno tendrá que presentarse a un examen final de aquellas partes que no haya superado en la convocatoria extraordinaria. En el caso de que sean las prácticas, deberá entregar aquellas no superadas.

LÍMITE DE CONVOCATORIAS
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.

PLAGIO
Cualquier tipo de fraude o plagio por parte del alumno en una actividad evaluable, será sancionado según se recoge en la Normativa de Convivencia de la UFV. A estos efectos, se considerará "plagio" cualquier intento de defraudar el sistema de evaluación, como copia en ejercicios, exámenes, prácticas, trabajos o cualquier otro tipo de entrega, bien de otro compañero, bien de materiales o dispositivos no autorizados, con el fin de hacer creer al profesor que son propios.

BIBLIOGRAFÍA Y OTROS RECURSOS

Básica

William Stallings Cryptography and Network Security: Principles and Practice 7ª