Guía didáctica

ASIGNATURA: *Criptografía y Teoría de Códigos*

Título: *Grado en Ingeniería Informática*
Materia: *Optativas*
Créditos: *6 ECTS*
Código: *73GIIN*

Índice

1. Organización general

1.1. Datos de la asignatura

MÓDULO	***Formación Optativa***
MATERIA	***Optativas***
ASIGNATURA	*Criptografía y Teoría de Códigos* **6 ECTS**
Carácter	Optativa
Curso	Cuarto
Cuatrimestre	Segundo
Idioma en que se imparte	Castellano
Requisitos previos	No existen
Dedicación al estudio por ECTS	**25 horas**

1.2. Equipo docente

Profesor	**Dr. Juan Vera del Campo** juan.vera@professor.universidadviu.com

1.3. Introducción a la asignatura

En esta asignatura estudiaremos los mecanismos de seguridad necesarios para mantener nuestras comunicaciones seguras: historia de la criptografía, criptografía simétrica y asimétrica, protocolos criptográficos y firma digital. Los protocolos se analizarán a bajo nivel y se hará especial hincapié en aquellos aspectos que los hacen inseguros, para evitar errores en la implementación de la seguridad en un proyecto.

1.4. Competencias y resultados de aprendizaje

COMPETENCIAS GENERALES

CG.3.- Capacidad para diseñar, desarrollar, evaluar y asegurar la accesibilidad, ergonomía, usabilidad y seguridad de los sistemas, servicios y aplicaciones informáticas, así como de la información que gestionan.

CG.4.- Capacidad para definir, evaluar y seleccionar plataformas hardware y software para el desarrollo y la ejecución de sistemas, servicios y aplicaciones informáticas, de acuerdo con los conocimientos adquiridos según lo establecido en la resolución.

CG.5.- Capacidad para concebir, desarrollar y mantener sistemas, servicios y aplicaciones informáticas empleando los métodos de la ingeniería del software como instrumento para el aseguramiento de su calidad, de acuerdo con los conocimientos adquiridos según lo establecido en la resolución.

CG.9.- 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.

CG.11.- Capacidad para analizar y valorar el impacto social y medioambiental de las soluciones técnicas, comprendiendo la responsabilidad ética y profesional de la actividad del Ingeniero Técnico en Informática.

CG.12.- Conocimiento y aplicación de elementos básicos de economía y de gestión de recursos humanos, organización y planificación de proyectos, así como la legislación, regulación y normalización en el ámbito de los proyectos informáticos, de acuerdo con los conocimientos adquiridos según lo establecido en la resolución.

RESULTADOS DE APRENDIZAJE

Al finalizar esta asignatura se espera que el estudiante sea capaz de:

RA.1.- Distinguir los criptosistemas seguros de los que no son fiables.

RA.2.- Diferenciar entre criptografía de clave secreta y clave pública.

RA.3.- Identificar los fundamentos en los que se basan los criptosistemas de clave pública y privada.

RA.4.- Determinar el concepto de firma digital y su importancia.

2. Contenidos/temario

- Tema 1: Conceptos básicos
  - Servicios de seguridad
  - Protocolos de seguridad

- Tema 2: Criptografía clásica
  - Historia de la criptograma

- Cifrado César
- Cifrado Vigenère
- Máquina Enigma
- Confidencialidad perfecta: cifrado Vernam

- Tema 3: Criptografía de clave simétrica
  - Seguridad computacional
  - Cifrado simétrico de flujo
  - Cifrado simétrico de bloque
  - Cifrado AES
  - Cifrado ChaCha

- Tema 4: Teoría de la información y de la complejidad
  - Teoría de números
  - Teoría de complejidad
  - Acuerdo de claves Diffie-Hellman

- Tema 5: Criptografía de clave pública
  - Cifrado RSA
  - Curvas Elípticas

- Tema 6: Funciones de hash y blockchain
- Tema 7: Protocolo TLS y sistemas PKI
- Tema 8: Criptografía ofensiva
- Tema 9: Esteganografía

3. Metodología

La metodología de la Universidad Internacional de Valencia (VIU) se caracteriza por una apuesta decidida en un modelo de carácter e-presencial. Así, siguiendo lo estipulado en el calendario de actividades docentes del Título, se impartirán en directo un conjunto de sesiones, que, además, quedarán grabadas para su posterior visionado por parte de aquellos estudiantes que lo necesitasen. En todo caso, se recomienda acudir, en la medida de lo posible, a dichas sesiones, facilitando así el intercambio de experiencias y dudas con el docente.

En lo que se refiere a las metodologías específicas de enseñanza-aprendizaje, serán aplicadas por el docente en función de los contenidos de la asignatura y de las necesidades pedagógicas de los estudiantes. De manera general, se impartirán contenidos teóricos y, en el ámbito de las clases prácticas se podrá realizar la resolución de problemas, el estudio de casos y/o la simulación.

Por otro lado, la Universidad y sus docentes ofrecen un acompañamiento continuo al estudiante, poniendo a su disposición foros de dudas y tutorías para resolver las consultas de carácter académico que el estudiante pueda tener. Es importante señalar que resulta fundamental el trabajo autónomo del estudiante para lograr una adecuada consecución de los objetivos formativos previstos para la asignatura.

4. Actividades formativas

Durante el desarrollo de cada una de las asignaturas se programan una serie de actividades de aprendizaje que ayudan a los estudiantes a consolidar los conocimientos trabajados.

A continuación, se relacionan las actividades que forman parte de la asignatura:

1. **Actividades de carácter teórico**

Se trata de un conjunto de actividades guiadas por el profesor de la asignatura destinadas a la adquisición por parte de los estudiantes de los contenidos teóricos de la misma. Estas actividades, diseñadas de manera integral, se complementan entre sí y están directamente relacionadas con los materiales teóricos que se ponen a disposición del estudiante (manual, SCORM y material complementario). Estas actividades se desglosan en las siguientes categorías:

a. Clases expositivas

b. Sesiones con expertos en el aula

c. Observación y evaluación de recursos didácticos audiovisuales

d. Estudio y seguimiento de material interactivo

2. **Actividades de carácter práctico**

Se trata de un conjunto de actividades guiadas y supervisadas por el profesor de la asignatura vinculadas con la adquisición por parte de los estudiantes de los resultados de aprendizaje y competencias de carácter más práctico. Estas actividades, diseñadas con visión de conjunto, están relacionadas entre sí para ofrecer al estudiante una formación completa e integral.

3. **Tutorías**

Se trata de sesiones, tanto de carácter síncrono como asíncrono (e-mail), individuales o colectivas, en las que el profesor comparte información sobre el progreso académico del estudiante y en las que se resuelven dudas y se dan orientaciones específicas ante dificultades concretas en el desarrollo de la asignatura.

4. **Trabajo autónomo**

Se trata de un conjunto de actividades que el estudiante desarrolla autónomamente y que están enfocadas a lograr un aprendizaje significativo y a superar la evaluación de la asignatura. La realización de estas actividades es indispensable para adquirir las competencias y se encuentran entroncadas en el aprendizaje autónomo que consagra

la actual ordenación de enseñanzas universitarias. Esta actividad, por su definición, tiene carácter asíncrono.

5. **Prueba objetiva final**

Como parte de la evaluación de cada una de las asignaturas (a excepción de las prácticas y el Trabajo fin de título), se realiza una prueba (examen final). Esta prueba se realiza en tiempo real (con los medios de control antifraude especificados) y tiene como objetivo evidenciar el nivel de adquisición de conocimientos y desarrollo de competencias por parte de los estudiantes. Esta actividad, por su definición, tiene carácter síncrono.

5. Evaluación

5.1. Sistema de evaluación

El Modelo de Evaluación de estudiantes en la Universidad se sustenta en los principios del Espacio Europeo de Educación Superior (EEES), y está adaptado a la estructura de formación virtual propia de esta Universidad. De este modo, se dirige a la evaluación de competencias.

Sistema de Evaluación	Ponderación	
	mínima	**máxima**
Entrega de informes de problemas y ejercicios	10	15
Planteamiento, estudio, análisis y resolución de casos	0	25
Informes o memorias de prácticas de laboratorio	0	15
Trabajos o proyectos desarrollados en grupo o de forma individual	0	30
Participación activa en los debates, foros y otros medios	5	5
Sistema de Evaluación	**mínima**	**máxima**
Evaluación final: Se podrán realizar exámenes finales o parciales (que incluyan ítems de alternativas, de asociación,multi-ítems, interpretativos, preguntas de desarrollo breve o extenso), supuestos prácticos y/o análisis de casos, sobre el desarrollo y los resultados de las actividades propuestas.	40	60

***Es requisito indispensable para superar la asignatura aprobar cada apartado (portafolio y prueba final)** con un mínimo de 5 para ponderar las calificaciones.

Los enunciados y especificaciones propias de las distintas actividades serán aportados por el docente, a través del Campus Virtual, a lo largo de la impartición de la asignatura.

Atendiendo a la Normativa de Evaluación de la Universidad, se tendrá en cuenta que la utilización de **contenido de autoría ajena** al propio estudiante debe ser citada adecuadamente en los trabajos entregados. Los casos de plagio serán sancionados con suspenso (0) de la actividad en la que se detecte. Asimismo, el uso de **medios fraudulentos durante las pruebas de evaluación** implicará un suspenso (0) y podrá implicar la apertura de un expediente disciplinario.

5.2. Sistema de calificación

La calificación de la asignatura se establecerá en los siguientes cómputos y términos:

Nivel de aprendizaje	Calificación numérica	Calificación cualitativa
Muy competente	9,0 - 10	Sobresaliente
Competente	7,0 - 8,9	Notable
Aceptable	5,0 -6,9	Aprobado
Aún no competente	0,0 -4,9	Suspenso

Sin detrimento de lo anterior, el estudiante dispondrá de una **rúbrica simplificada** en el aula que mostrará los aspectos que valorará el docente, como así también los **niveles de desempeño que tendrá en cuenta para calificar las actividades vinculadas a cada resultado de aprendizaje.**

La mención de «**Matrícula de Honor**» podrá ser otorgada a estudiantes que hayan obtenido una calificación igual o superior a 9.0. Su número no podrá exceder del cinco por ciento de los estudiantes matriculados en una materia en el correspondiente curso académico, salvo que el número de estudiantes matriculados sea inferior a 20, en cuyo caso se podrá conceder una sola «Matrícula de Honor.

6. Bibliografía

6.1. Bibliografía de referencia

Juan Vera “Criptografía y Teoría de Códigos”. http://juanvvc.github.io/crypto/ También disponible en enlace entre los recursos del aula. En navegadores como Chrome puedes “imprimirse a PDF” ara obtener la versión en PDF.

Atención: las transparencias tienen “Notas del profesor” que pueden verse pulsando la tecla “P” (en el formato HTML) o viendo notas adicionales (en los visores PDFs que lo soporten)

6.2. Bibliografía complementaria

Boneh D., Shoup V. ”A Graduate Course in Applied Cryptography”. http://toc.cryptobook.us/

“The Joy of Cryptography” by Mike Rosulek: https://joyofcryptography.com/ Knospe H.

“A course in Cryptography”, Ed. American Mathematical Society

Muñoz A. “Criptografía ofensiva. Atacando y defendiendo organizaciones”. Amazon.