Guía Didáctica - GRADO

ASIGNATURA: Criptografía y Teoría de Códigos

Título: Grado en Ingeniería Informática
Módulo: Optativa
Créditos: 6 ECTS
Código: 73GIIN

viu | Universidad Internacional de Valencia

1. Organización general

1.1. Datos de la asignatura

MÓDULO	**Optativas**
MATERIA	**Seguridad de la información**
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 recomendada por ECTS	**25 horas**

1.2. 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.

1.3. Competencias y resultados de aprendizaje

COMPETENCIAS GENERALES

- CG.1.- 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.

- CG.2.- Que los estudiantes hayan demostrado poseer y comprender conocimientos en un área de estudios 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, incluyen también algunos aspectos que implican conocimientos procedentes de la vanguardia de su campo de estudio.
- CG.3.- 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.
- CG.4.- 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.
- CG.5.- Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado.
- CG.6.- Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía.

COMPETENCIAS ESPECÍFICAS DE LA ASIGNATURA

- CE.1.- Comprensión y dominio de los conceptos básicos de criptografía, cifrados simétricos y asimétricos, intercambios de claves, parámetros que hacen seguro un algoritmo y protocolos criptográficos.

RESULTADOS DE APRENDIZAJE

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

RA1. Distinguir los criptosistemas seguros de los que no son fiables.

RA2. Diferenciar entre criptografía de clave secreta y clave pública.

RA3. Identificar los fundamentos en los que se basan los criptosistemas de clave pública y privada.

RA4. 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

Unidad Competencial 4: Teoría de la información y de la complejidad

- Teoría de números
- Teoría de complejidad

Tema 5: Criptografía de clave asimétrica

- Intercambio de claves Diffie-Hellman
- Cifrado RSA
- El Gamal
- Curva Elíptica

Tema 6: Firma digital

- Firma Digital
- Sistemas PKI

Tema 7: Protocolos

- TLS
- Amenazas

3. Actividades Formativas

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Clases expositivas	75	60
Resolución de ejercicios prácticos	100	30
Prácticas de laboratorios virtuales	100	20
Tutorías	75	0
Trabajo Autónomo	400	0

4. Metodologías Docentes

4.1 Clases teóricas impartidas como lecciones magistrales o exposiciones, en las que además de presentar el contenido de la asignatura, se explican los conceptos fundamentales y se desarrolla el contenido teórico.

4.2 Colección de tareas que el alumnado llevará a cabo a lo largo de toda la asignatura, entre las que podemos encontrar: análisis de casos, resolución de problemas, prácticas de laboratorios, comentarios críticos de textos, análisis de lecturas, etc.

4.3 Sesiones periódicas entre el profesorado y el alumnado para la resolución de dudas, orientación, supervisión, etc.

4.4 Trabajo tanto individual como grupal para la lectura crítica de la bibliografía, estudio sistemático de los temas, reflexión sobre problemas planteados, resolución de actividades propuestas, búsqueda, análisis y elaboración de información, investigación e indagación, así como trabajo colaborativo basado en principios constructivistas.

5. Evaluación

1.1. 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
Portafolio*	**40-60 %**
Colección de tareas realizadas por el alumnado y establecidas por el profesorado. La mayoría de las tareas aquí recopiladas son el resultado del trabajo realizado dirigido por el profesorado en las actividades, tutorías, etc. Esto permite evaluar, además de las competencias conceptuales, otras de carácter más práctico, procedimental o actitudinal.	

Sistema de Evaluación	Ponderación
Prueba final*	**40-60 %**
Realización de una prueba cuyas características son definidas en cada caso por el correspondiente profesorado.	

1.2. Sistema de Calificación

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

Nivel de Competencia	Calificación Oficial	Etiqueta Oficial
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

El nivel de competencia en cada una de las actividades realizadas se medirá, teniendo en cuenta **criterios generales derivados de la consecución de los resultados de aprendizaje**, que en términos generales y en función de la adecuación en el planteamiento de los contenidos generales y contenidos específicos, valorarán por norma general y en trabajos escritos, la corrección de la estructura formal y organización del discurso (semántica, sintaxis y léxico) valorándose además la originalidad, creatividad y argumentación de las intervenciones utilizando referencias bibliográficas.

Sin detrimento de lo anterior, el alumnado dispondrá de una rúbrica simplificada (CAMPUS) 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.

6. Bibliografía

Referencias básicas

- Griesa, J.I, Vera J. “Criptografía y Teoría de Códigos”. http://juanvvc.github.io/crypto/slides También disponible en formato PDF en los recursos del aula.
- Boneh D., Shoup V. ”A Graduate Course in Applied Cryptography”. http://toc.cryptobook.us/
- FIPS 186-4. “Digital Signature Standard (DSS)”. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf
- NIST SP 800-57. “Recommendation for Key Management”. https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final

Otra bibliografía recomendada

- Knospe H. “A course in Cryptography”, Ed. American Mathematical Society
- Muñoz A. “Criptografía ofensiva. Atacando y defendiendo organizaciones”. Amazon.