Proyecto docente de la asignatura

Proyecto/Guía docente de la asignatura para el curso 2021-2022

Asignatura	SEGURIDAD Y CRIPTOGRAFÍA		
Materia	INGENIERÍA DE SISTEMAS TELEMÁTICOS		
Módulo	BLOQUE DE ITINERARIOS TECNOLÓGICOS EN TIC (BI)		
Titulación	MÁSTER UNIVERSITARIO DE INVESTIGACIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES		
Plan	624	**Código**	54630
Periodo de impartición	2º CUATRIMESTRE	**Tipo/Carácter**	OPTATIVA
Nivel/Ciclo	MÁSTER	**Curso**	1º
Créditos ECTS	5 ECTS		
Lengua en que se imparte	CASTELLANO INGLÉS (materiales de lectura y charlas complementarias)		
Profesor/es responsable/s	JUAN CARLOS GARCÍA ESCARTÍN		
Departamento(s)	TEORÍA DE LA SEÑAL Y COMUNICACIONES E INGENIERÍA TELEMÁTICA		
Datos de contacto (E-mail, teléfono…)	E-mail: juagar@tel.uva.es		

1. Situación / Sentido de la Asignatura

1.1 Contextualización

Los sistemas electrónicos e informáticos están presentes en un número creciente de actividades y tareas cotidianas. Los sistemas de comercio electrónico, telefonía móvil e internet de las cosas han aumentado su complejidad y su implantación de forma notable en las últimas décadas.

Una parte fundamental de todos estos sistemas es la necesidad de seguridad en sentido amplio: garantizar que los usuarios legítimos pueden acceder a los servicios que se ofrecen sin temor a que se suplante su identidad o se roben sus datos.

En esta asignatura se discutirán los principios de los diferentes sistemas criptográficos que permiten implementar sistemas resistentes a diferentes ataques.

1.2 Relación con otras materias

Se trata de una asignatura de carácter generales relevante para redes de ordenadores y sistemas informáticos generales. Por su importancia en el diseño, se relaciona particularmente con las asignaturas del bloque del itinerario en Ingeniería de Sistemas Telemáticos, aunque los contenidos son aplicables al diseño de redes y la creación de sistemas de biomedicina seguros y que preserven la privacidad de los pacientes.

1.3 Prerrequisitos

La asignatura será autocontenida. Se supondrán unos conocimientos matemáticos e informáticos básicos correspondientes a un graduado en Ingenería de Telecomunicación o estudios afines.

2. Competencias

2.1 Generales

1. Capacidad crítica hacia el conocimiento actual como medio imprescindible para la detección de nuevos retos a resolver y por eso evaluar crítica y constructivamente resultados de investigación de otros [CG 1].

2. Capacidad de entender las implicaciones éticas y sociales de las decisiones adoptadas durante el ejercicio de las labores profesionales y de investigación [CG 6].

3. Capacidad de ser creativo en la concepción, formulación y resolución de preguntas de investigación [CG 15].

4. Capacidad de emplear una metodología adecuada de investigación adaptada en cada contexto con énfasis en el método científico [CG 16].

2.2 Específicas

5. Capacidad de entender las principales tecnologías emergentes de la Internet de Futuro y plantear preguntas de investigación sobre su idoneidad y sostenibilidad [CE-IST 5].

6. Capacidad de diseñar sistemas seguros usando criptografía y siguiendo las prácticas de seguridad aceptadas en la industria [CE-IST 13].

7. Capacidad de detectar las posibles vulnerabilidades de los sistemas informáticos y de proteger los datos de los usuarios [CE-IST 14].

8. Capacidad de descubrir problemas de seguridad en sistemas informáticos y comunicarlos de forma responsable a la industria y la sociedad [CE-IST 15].

9. Capacidad de usar las diferentes fuentes de datos en seguridad informática (archivos de preprints, repositorios de vulnerabilidades, RFCs...) [CE-IST 16].

3. Objetivos

1. Conocer las primitivas básicas disponibles en sistemas de seguridad.
2. Comprender las ventajas e inconvenientes de diferentes sistemas de cifrado.
3. Comprender la importancia de seguir las prácticas recomendables en la implementación de sistemas de seguridad.
4. Conocer las herramientas matemáticas básicas detrás de los sistemas de cifrado y seguridad más habitual.
5. Conocer los programas informáticos utilizados en tareas de ciberseguridad.
6. Ser capaz de evaluar la aleatoriedad de una secuencia binaria.
7. Conocer los protocolos de divulgación responsable de vulnerabilidades y problemas de seguridad.
8. Ser capaz de presentar de forma clara resultados de investigación.
9. Ser capaz de analizar la seguridad de un sistema informático.
10. Ser capaz de evaluar críticamente los resultados de investigación, los artículos y exposiciones de otros.

4. Contenidos

Los contenidos se estructurarán en 12 temas de 3 a 5 horas con una introducción teórica y cerca de dos tercios de ejemplos prácticos.

1. Introducción: primitivas en seguridad. Consejos generales.

Descripción de las primitivas de seguridad más importantes. Consejos de diseño.

2. Funciones hash:Funciones de un sentido. Autenticación y comprobación de la integridad. Colisiones.

Definición de función hash. Aplicaciones. Ejemplos en autenticación y comprobación de la integridad. Ejemplos prácticos de evaluación de diferentes funciones hash.

3. Aplicaciones de las funciones hash (I): gestión de contraseñas.

Sistemas de gestión de contraseñas. Establecimiento de sesión con cadenas de hashes. Ejemplos prácticos de almacenamiento y uso de sal.

4. Aplicaciones de las funciones hash (II): Blockchain. Bitcoin (I).

Uso de funciones hash en cuadernos públicos. Blockchain: fundamentos generales. Ejemplos prácticos con Bitcoin.

5. Criptografía simétrica: Cifrado por bloques. Modos de operación. DES. AES.

Criptografía simétrica: fundamentos. Modos de funcionamiento ECB y CBC. Ejemplos prácticos con DES y AES.

6. Criptografía asimétrica: RSA y curvas elípticas. Distribución de claves. Infraestructura de clave pública. Certificados.

Fundamentos de Teoría de Números. El sistema RSA. Curvas elípticas. Aplicaciones en distribución de claves. PKI. Cadenas de confianza y certificados.

7. Generación de números aleatorios.

Números aleatorios y pseudoaleatorios. Aplicaciones. Generación de números aleatorios con uso criptográfico. Tests de aleatoriedad.

8. Conferencias y temas avanzados en seguridad y criptografía.

Charlas invitadas y trabajos personalizados para los alumnos.

5. Métodos docentes y principios metodológicos

Clase magistral y ejercicios prácticos ilustrativos mediante problemas y demostraciones con ordenador.

6. Tabla de dedicación del estudiante a la asignatura

ACTIVIDADES PRESENCIALES	HORAS	ACTIVIDADES NO PRESENCIALES	HORAS
Clases teórico – prácticas	20	Estudio y trabajo autónomo individual	55
Laboratorios	24	Estudio y trabajo autónomo grupal	20
Seminarios	6		
Total presencial	**50**	**Total no presencial**	**75**

7. Sistema y características de la evaluación

INSTRUMENTO/PROCEDIMIENTO	PESO EN LA NOTA FINAL	OBSERVACIONES
Evaluación continua (voluntaria): Entrega de trabajos, exposición en clase, trabajos de programación...	0-100%	
Examen final	0-100%	- Supondrá el total de la nota final para los alumnos que no se acojan a la evaluación continua.

CRITERIOS DE CALIFICACIÓN

- **Convocatoria ordinaria:**

  Se ofrecerá a los alumnos la opción de ser evaluados de forma continua mediante trabajos y presentaciones, con un examen final voluntario en caso de llegar al 5.

  El examen final será el 100% de la nota de los alumnos que no se acojan a la evaluación continua y será necesario para obtener las notas más altas (sobresaliente y matrícula de honor

- **Convocatoria extraordinaria:**

El examen final será el 100% de la nota, salvo que el alumno haya realizado actividades de evaluación continua (en ese caso se ponderará la nota obtenida durante la convocatoria ordinaria en la evaluación continua sin posibilidad de entregar nuevos trabajos o prácticas).

8. Bibliografía

Se proporcionarán artículos y materiales sobre cada tema. Además, como bibliografía general se recomienda:

[1] N. Ferguson, B. Schneier y T. Kohno, *Cryptography Engineering Design Principles and Practical Applications*, (John Wiley & Sons, 2010).

[2] A. J. Menezes, S. A. Vanstone y P. C. van Oorschot, *Handbook of Applied Cryptography*, 1st ed. (CRC Press, Inc., Boca Raton, FL, USA, 1996).

[3] D. M. Burton, *Elementary Number Theory*, 6th ed. (McGraw-Hill Higher Education, 2005).

9. Consideraciones finales

Este programa es orientativo. Dependiendo de la formación previa de los alumnos matriculados y los intereses que éstos expresen, los contenidos concretos podrán variar, previo acuerdo con los matriculados.