Guía Docente: Criptografía y Criptoanálisis

DATOS GENERALES	
Facultad	Facultad de Ciencias y Tecnología
Titulación	Grado en Ingeniería Informática
Plan de estudios	2012
Especialidad/Mención	Mención en Criptología y Seguridad de la Información
Materia	Criptología y Seguridad de la Información
Carácter	Optativo
Período de impartición	Primer Trimestre
Curso	Cuarto
Nivel/Ciclo	Grado
Créditos ECTS	6
Lengua en la que se imparte	Castellano
Prerrequisitos	No se precisa

DATOS DEL PROFESORADO			
Profesor Responsable	Cristina Romero Tris	**Correo electrónico**	cristina.romero.tris@ui1.es
Área		**Facultad**	Facultad de Ciencias y Tecnología
Perfil Profesional 2.0	LinKedin		

CONTEXTUALIZACIÓN Y JUSTIFICACIÓN DE LA ASIGNATURA	
Asignaturas de la materia	• Auditoría y seguridad avanzada de sistemas y redes de comunicaciones • Autenticación y Sistemas Biométricos • Criptografía y Criptoanálisis • Dirección de Proyectos de Seguridad Corporativos • Técnicas de Análisis Forense • Técnicas de auditoría, ataque y programación segura de aplicaciones web
Contexto y sentido de la asignatura en la titulación y perfil profesional	Esta asignatura forma parte de las asignaturas optativas del itinerario de Criptología y Seguridad de la Información del último año del Grado en Ingeniería Informática. En esta asignatura se estudian técnicas criptográficas que constituyen un pilar fundamental para entender cómo funciona la seguridad informática en la actualidad. Durante la asignatura, además de conceptos básicos de criptografía, también se explican herramientas matemáticas que son esenciales para comprender cómo funcionan los sistemas criptográficos. Se analizan en profundidad los algoritmos más utilizados, como el RSA y se estudia cómo los nuevos avances en computación cuántica afectan a la criptografía. Además, se tratarán las numerosas aplicaciones del mundo cotidiano que utilizan la criptografía.

COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE Y RESULTADOS DE APRENDIZAJE	
Competencias de la asignatura	• CR06: Conocimiento y aplicación de los procedimientos algorítmicos básicos de las tecnologías informáticas para diseñar soluciones a problemas, analizando la idoneidad y complejidad de los algoritmos propuestos. • CMC01: Conocimiento de los métodos matemáticos básicos sobre los que se fundamentan las principales primitivas criptológicas y procedimientos de criptoanálisis. • CMC02: Capacidad para conocer, comprender y utilizar las principales primitivas criptográficas, identificar la más adecuada para cada uso y aplicarlas adecuadamente para garantizar la seguridad del procedimiento. • CMC03: Comprensión y capacidad de utilización de los principales métodos y procedimientos de criptoanálisis, aplicando los mismos para la identificación y recuperación de textos cifrados con algoritmos clásicos o débiles. • CT01: Capacidad de análisis y síntesis: encontrar, analizar, criticar (razonamiento crítico), relacionar, estructurar y sintetizar información proveniente de diversas fuentes, así como integrar ideas y conocimientos • CT04: Capacidad para la resolución de problemas
Resultados de aprendizaje de la asignatura	• Conoce el recorrido histórico de los principales criptosistemas empleados en la antigüedad y sus ataques más efectivos. • Conoce los aspectos básicos de la teoría de la información y de complejidad necesarios para definir cualidades en un buen criptosistema. • Distingue claramente los conceptos de criptosistema de bloque y de flujo, y conoce las fortalezas y debilidades de cada uno de ellos. • Distingue entre ataques a los algoritmos criptográficos y ataques al uso de los mismos. • Conoce el problema de la distribución de claves y algunas de sus soluciones. • Enumera distintos métodos de certificación digital y conoce sus estándares. • Conoce los principales algoritmos de clave secreta y pública, sus especificaciones y algunos criterios de diseño. • Decide sobre el uso y la aplicación de los algoritmos criptográficos más adecuados, en situaciones donde es necesario proteger la confidencialidad de la información y la privacidad en las comunicaciones.

PROGRAMACION DE CONTENIDOS	
Breve descripción de la asignatura	El conocimiento y correcta aplicación de técnicas criptográficas se ha convertido en una habilidad muy preciada para cualquier graduado en Informática, dado que éstas se encuentran presentes en multitud de áreas. Esta asignatura introduce, primero, los grandes paradigmas de computación criptográfica, de clave secreta y pública, analizando los algoritmos y su complejidad algorítmica. A continuación, se analizan algunos de los principales esquemas de criptoanálisis, como el criptoanálisis diferencial. Por último, se analizan una serie de protocolos criptográficos del más alto nivel, así como su aplicación a problemas y situaciones reales.
Contenidos	**Unidad Didáctica 1: Conceptos básicos de criptografía** - Definiciones iniciales básicas - Historia de la criptografía - La criptografía moderna

Unidad Didáctica 2: Fundamentos matemáticos de la criptografía

- Aritmética modular

- Tests de primalidad

- Algoritmos de factorización

Unidad Didáctica 3: Métodos clásicos de cifrado

- Criptosistemas

- Algoritmos clásicos de cifrado

- Cifrado por desplazamiento

- Cifrados de flujo

Unidad Didáctica 4: Criptografía de clave simétrica

- Cifrados por bloques

- Tiny Encryption Algorithm (TEA)

- Data Encryption Standard (DES)

- Advanced Encryption Standard (AES)

Unidad Didáctica 5: Criptografía de clave pública

- Algoritmo de Diffie y Hellman

- El criptosistema RSA

- El criptosistema ElGammal

- Firmas digitales

- Certificados digitales

Unidad Didáctica 6: Aplicaciones de la criptografía

- Criptomonedas: Bitcoin

- Cifrado de mensajes en Whatsapp

- Votación electrónica segura

- Criptografía en smart cards

- Nuevos avances en criptografía

METODOLOGÍA	
Actividades formativas	El alumno dispondrá de un espacio dentro del aula virtual, organizado en seis unidades didácticas. Cada unidad didáctica estará organizada en las siguientes estructuras: • **Contenidos:** Conceptos teóricos sobre la temática de la asignatura. • **Cuestionario de autoevaluación:** Todas las unidades didácticas tendrán un cuestionario donde el alumno podrá comprobar si ha asimilado los contenidos explicados en esa unidad. • **Actividades prácticas:** En cada unidad el alumno será evaluado de la forma más adecuada al contenido. En algunas unidades habrá foros de debate, donde los alumnos expresarán sus opiniones sobre temas de actualidad relacionados con la unidad. En otras unidades habrá laboratorios criptográficos, con actividades prácticas y problemas para comprobar que el alumno ha asimilado los conceptos explicados. Por último, los alumnos tendrán un trabajo colaborativo en el que implementarán alguna actividad práctica en grupos.

EVALUACIÓN	
Sistema evaluativo	*En caso de que la situación sanitaria impida la realización presencial de los exámenes con todas las garantías, la Universidad Isabel I celebrará dichas pruebas en modalidad online. Para la realización de dichos exámenes, la universidad incorporará la herramienta de proctoring a nuestra plataforma tecnopedagógica, con el objetivo de garantizar los procesos de autentificación del alumno, como el control del entorno durante el desarrollo de las pruebas de evaluación. A su vez, la Universidad Isabel I pondrá a disposición del alumnado una Unidad de Exámenes Online específica para ofrecer apoyo técnico durante todo el proceso y así solventar todas las incidencias que se puedan presentar.* El sistema de evaluación se basará en una selección de las pruebas de evaluación más adecuadas para el tipo de competencias que se trabajen. El sistema de calificaciones estará acorde con la legislación vigente *(Real Decreto 1125/2003, de 5 de septiembre, por el que se establece el sistema europeo de créditos y el sistema de calificaciones en las titulaciones universitarias de carácter oficial y de validez en todo el territorio nacional)*. El sistema de evaluación de la Universidad Isabel I queda configurado de la siguiente manera: **Sistema de evaluación convocatoria ordinaria** **Opción 1. Evaluación continua** Los estudiantes que opten por esta vía de evaluación deberán realizar el **seguimiento de la evaluación continua (EC)** y podrán obtener hasta un **60 %** de la calificación final a través de las actividades que se plantean en la evaluación continua. Además, deberán realizar un **examen final presencial (EX)** que supondrá el **40 %** restante. Esta prueba tiene una parte dedicada al control de la identidad de los estudiantes que consiste en la verificación del trabajo realizado durante la evaluación continua y otra parte en la que realizan diferentes pruebas teórico-prácticas para evaluar las competencias previstas en cada asignatura. Para la aplicación de los porcentajes correspondientes, el estudiante debe haber obtenido una nota mínima de un 4 en cada una de las partes de las que consta el sistema de evaluación continua.

Se considerará que el estudiante supera la asignatura en la convocatoria ordinaria por el sistema de evaluación continua, siempre y cuando al aplicar los porcentajes correspondientes se alcance una calificación mínima de un 5.

Opción 2. Prueba de evaluación de competencias

Los estudiantes que opten por esta vía de evaluación deberán realizar una **prueba de evaluación de competencias (PEC)** y un **examen final presencial (EX)**.

La **PEC** se propone como una prueba que el docente plantea con el objetivo de evaluar en qué medida el estudiante adquiere las competencias definidas en su asignatura. Dicha prueba podrá ser de diversa tipología, ajustándose a las características de la asignatura y garantizando la evaluación de los resultados de aprendizaje definidos. Esta prueba supone el 50 % de la calificación final.

El **examen final presencial**, supondrá el **50 %** de la calificación final. Esta prueba tiene una parte dedicada al control de la identidad de los estudiantes que consiste en la verificación del seguimiento de las actividades formativas desarrolladas en el aula virtual y otra parte en la que realizan diferentes pruebas teórico-prácticas para evaluar las competencias previstas en cada asignatura.

Al igual que con el sistema de evaluación anterior, para la aplicación de los porcentajes correspondientes el estudiante debe haber obtenido una puntuación mínima de un 4 en cada una de las partes de las que consta la opción de prueba de evaluación de competencias.

Se considerará que el estudiante supera la asignatura en la convocatoria ordinaria por el sistema de la prueba de evaluación de competencias siempre y cuando al aplicar los porcentajes correspondientes se alcance una calificación mínima de un 5.

Sistema de evaluación convocatoria extraordinaria

Todos los estudiantes, independientemente de la opción seleccionada, que no superen las pruebas evaluativas en la convocatoria ordinaria tendrán derecho a una convocatoria extraordinaria.

La convocatoria extraordinaria completa consistirá en la realización de una **prueba de evaluación de competencias** que supondrá el **50 %** de la calificación final y un **examen final presencial** cuya calificación será el **50 %** de la calificación final.

Para la aplicación de los porcentajes correspondientes, el estudiante debe haber obtenido una nota mínima de un 4 en cada una de las partes de las que consta el sistema de evaluación de la convocatoria extraordinaria.

Los estudiantes que hayan suspendido todas las pruebas evaluativas en convocatoria ordinaria (evaluación continua o prueba de evaluación de competencias y examen final) o no se hayan presentado deberán realizar la convocatoria extraordinaria completa, como se recoge en el párrafo anterior.

En caso de que hayan alcanzado una puntuación mínima de un 4 en alguna de las pruebas evaluativas de la convocatoria ordinaria (evaluación continua o prueba de evaluación de competencias y examen final), se considerará su calificación para la convocatoria extraordinaria, debiendo el estudiante presentarse a la prueba que no haya alcanzado dicha puntuación o que no haya realizado.

En el caso de que el alumno obtenga una puntuación que oscile entre el 4 y el 4,9 en las dos partes de que se compone la convocatoria ordinaria (EC o PEC y examen), solo se considerará para la convocatoria extraordinaria la nota obtenida en la evaluación continua

	o prueba de evaluación de competencias ordinaria (en función del sistema de evaluación elegido), debiendo el alumno realizar el examen extraordinario para poder superar la asignatura. Al igual que en la convocatoria ordinaria, se entenderá que el alumno ha superado la materia en convocatoria extraordinaria si, aplicando los porcentajes correspondientes, se alcanza una calificación mínima de un 5.

BIBLIOGRAFÍA Y OTROS RECURSOS	
Bibliografía básica	• Lucena López. M. *Criptografía y Seguridad en Computadores* (4º ed). Creative Commons (online) http://www.grc.upv.es/biblioteca/cripto.pdf Libro abierto y en castellano que recoge los aspectos básicos de la asignatura, así como algunas aplicaciones de la criptografía. Destacar que este manual ofrece una gran cantidad de algoritmos presentados en pseudocódigo para facilitar la implementación de los mismos. Destacar los capítulos 4, 5 y 6 para los fundamentos matemáticos y los capítulos 7, 8 y 9 para la criptografía de clave pública y privada • Cabellero Gil, P. (2002). *Introducción a la criptografía* (2ºed.). Madrid: Editorial RA-MA. Presenta un recorrido introductorio por los aspectos más destacables de cada una de las facetas de la Criptografía. Se reúnen aquí tanto los fundamentos de la base teórica y las descripciones de varios cifrados clásicos, como el análisis de los sistemas de clave secreta y de clave pública más difundidos actualmente. Se presta especial atención a las aplicaciones criptográficas de mayor relevancia, como son la firma digital y la identificación de usuarios para el control de accesos. Finalmente, se describen diversos protocolos criptográficos que permiten resolver en el mundo de las telecomunicaciones situaciones habituales tan simples como lanzar una moneda o guardar un mensaje dentro de un sobre, y tan complejas como firmar un contrato o llevar a cabo unas elecciones seguras.
Bibliografía complementaria	Stinson, D.R. (2005). *Cryptography: Theory & Practice* (3ª ed.). Chapman and Hall Menezes, A. J. Van Oorschot P.C.& Vanstone, S.A. (2001). *Handbook of Applied Criptography*. CRC Press. Pastor Franco, J. Sarasa López, M. y Salazar Riaño, J.L. (2001). Criptografía Digital: Fundamentos y aplicaciones. Zaragoza: Prensas Universitarias de Zaragoza. Gutiérrez, J. y Tena, J. (2003). *Protocolos criptográficos y seguridad en redes.* Servicio de publicaciones Universidad de Cantabria. Tilborg, V. (2000). *Fundamentals of cryptology*. Kluver Academic Plublishers.

Otros recursos	Resumen histórico sobre los hitos de la criptografía http://world.std.com/~cme/html/timeline.html Web de la agencia del departamento de comercio de EEUU del Instituto Nacional de Estándares y Tecnología http://www.nist.gov/itl/ y de la división de seguridad informática http://csrc.nist.gov/groups/STM/ Servidor de Claves Públicas del MIT https://pgp.mit.edu/ Artículo original del algoritmo RSA https://people.csail.mit.edu/rivest/Rsapaper.pdf Web para generar el par de claves (pública y privada) de cifrado https://gnupg.org/ Cómo enviar correos encriptados mediante Gmail http://www.enlanubetic.com.es/2012/11/enviar-correos-encriptados-en-gmail.html Información y algoritmo HASH http://www.secure-hash-algorithm-md5-sha-1.co.uk/ El algoritmo de encriptación Blowfish https://www.schneier.com/cryptography/blowfish/ Información sobre criptografía cuántica https://uwaterloo.ca/institute-for-quantum-computing/research/areas-research/quantum-cryptography Centro Criptológico Nacional donde indica el nivel de alerta de ciberataques https://www.ccn-cert.cni.es/ Instituto Nacional de Seguridad de España https://www.incibe.es/ Revista de interés sobre criptografía a nivel internacional http://www.insaonline.org/ La Fábrica Nacional de Moneda y Timbre emite el certificado electrónico que se puede utilizar para gestiones online http://www.cert.fnmt.es/