Universidad de Alcalá

GUÍA DOCENTE

Criptografía aplicada

Master Universitario en Ciberseguridad
Universidad de Alcalá

Curso Académico 2019/20

GUíA DOCENTE

Nombre de la asignatura:	**Criptografía aplicada**
Código:	202553
Titulación en la que se imparte:	**Master Universitario en Ciberseguridad**
Departamento y Área de Conocimiento:	**Departamento de Automática** **Área de Arquitectura y Tecnología de Computadores**
Carácter:	**Obligatorio**
Créditos ECTS:	**4,5**
Curso y cuatrimestre:	**Primer curso**
Profesorado:	Raúl Durán Díaz
Horario de Tutoría:	
Idioma en el que se imparte:	Español

1. PRESENTACIÓN

La asignatura *Criptografía aplicada*, que se enmarca dentro de la materia *Seguridad de la Información y Comunicaciones*, tiene por objetivo fundamental analizar los mecanismos básicos que permiten garantizar la confidencialidad y la integridad de la información, evitar su repudio ilegítimo y asegurarse de su autoría. Se estudiarán las primitivas criptográficas básicas con sus fundamentos matemáticos, pues realmente es el único modo de comprender cómo funcionan y cuáles son sus puntos débiles.

El sesgo aplicado de la asignatura nos llevará a prestar atención a las bibliotecas de programación orientadas a criptografía que resulten más modernas en cada momento. Los conceptos fundamentales permitirán al alumno utilizar esas bibliotecas con seguridad y eficiencia tanto a la hora de diseñar aplicaciones con necesidades criptográficas como para el criptoanálisis y la auditoría de las ya existentes.

2. COMPETENCIAS

Competencias Generales (CG)

Esta asignatura contribuye a adquirir las siguientes competencias generales:

CG1	Capacidad para aplicar conocimientos y técnicas de seguridad de la información a la gestión, evaluación, cumplimiento de normativas y diseño de departamentos, programas y proyectos.
CG2	Capacidad para seleccionar y aplicar técnicas, métodos y tecnologías de protección de la información y las comunicaciones en contextos complejos y cambiantes.
CB6	Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación
CB7	Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio

Competencias específicas (CESP)

Esta asignatura contribuye a adquirir las siguientes competencias específicas:

CE5	Capacidad para aplicar los fundamentos y las técnicas de ingeniería criptográfica a la selección, diseño y evaluación de la seguridad de la información y las comunicaciones.
CE7	Capacidad para aplicar técnicas avanzadas de ocultación de información sobre diferentes soportes, así como para analizar la presencia de esas informaciones ocultas.

Resultados del aprendizaje

Al término de la asignatura, el alumno habrá alcanzado los siguientes resultados de aprendizaje:

RA1	Utilización de mecanismos criptográficos para gestionar riesgos de seguridad de la información, evaluando las implicaciones de uso de los diferentes mecanismos disponibles.
RA2	Construcción de soluciones de seguridad aceptables en escenarios concretos, utilizando diferentes mecanismos criptográficos.
RA3	Aplicación de técnicas avanzadas de ocultación de información sobre diferentes soportes.

3. CONTENIDOS

Bloques de contenido (se pueden especificar los temas si se considera necesario)	Total de clases, créditos u horas
Introducción a la criptografía. Fundamentos. Objetivos y servicios esperables: confidencialidad, integridad, autenticación. Modelos de seguridad y modelos de ataques. Secreto perfecto. Criptografía simétrica y asimétrica. Primitivas criptográficas, funciones resumen, autenticación de mensajes, gestión de claves. Dispositivos criptográficos. Conceptos matemáticos básicos.	1,5 horas
Números aleatorios y pseudo-aleatorios. Aleatoriedad y pseudo-aleatoriedad. Baterías de pruebas. Generadores de números y sucesiones aleatorias. Generadores de números y sucesiones pseudo-aleatorias criptográficamente seguros.	1,5 horas
Criptografía simétrica: cifrado en flujo. Generadores de secuencias cifrantes: FSR y sus variantes. Generadores software y hardware: RC4, Trivium. Criptoanálisis.	3 horas
Criptografía simétrica: cifrado en bloque. Arquitectura general de los cifradores en bloque: esquema de Feistel y su uso en DEA. Interludio: estructura algebraica de cuerpos finitos primos y sus extensiones. Estructura del AES (*advanced encryption standard*). Modos de operación.del cifrado en bloque. Funciones resumen. Códigos de autenticación de mensajes. Cifrado autenticado. Criptoanálisis.	12 horas
Criptografía asimétrica. Fundamentos matemáticos de la criptografía asimétrica: funciones unidireccionales basadas en problemas difíciles. Criptografía basada en el Problema del la Factorización: criptosistema RSA. Criptografía basada en el Problema del Logaritmo Discreto en un cuerpo primo: criptosistema de ElGamal. Criptografía basada en el Problema del Logaritmo Discreto sobre curvas elípticas. Criptoanálisis.	12 horas
Firmas digitales. Esquemas de firma digital y sus propiedades. Tipos de firmas: ordinarias, en grupo, ciegas, en anillo, multifirmas. Implementación con los distintos criptosistemas asimétricos. Criptoanálisis.	3 horas
Criptografía cuántica y post-cuántica. Fundamentos de la computación cuántica. Impacto de la criptografía cuántica. Algoritmos criptográficos cuánticos. Algoritmos criptográficos «post-cuánticos». Criptoanálisis.	3 horas

4. METODOLOGÍAS DE ENSEÑANZA-APRENDIZAJE. ACTIVIDADES FORMATIVAS

4.1. Distribución de créditos (especificar en horas)

Número de horas presenciales:	Clases presenciales teórico prácticas, incluyendo trabajo en ordenador: 31,5 horas Tutorías: 9 horas Seminarios temáticos y conferencias: 4,5 horas Total: 45 horas presenciales
Número de horas del trabajo propio del estudiante:	Trabajo personal del estudiante: 45 horas Trabajo en grupos de estudiantes: 22,5 horas
Total horas	112,5 horas.

4.2. Estrategias metodológicas, materiales y recursos didácticos

Clases Presenciales	• Exposiciones en clase, de carácter teórico práctico. • Resolución de problemas. • Sesiones prácticas de laboratorio: orientadas a consolidar los conceptos presentados previamente, así como a familiarizar al estudiante con las herramientas y metodologías de apoyo al estudio de la materia y futuro desempeño profesional (mejorar la comprensión de los conceptos de seguridad, detección de intrusiones, análisis de vulnerabilidades y puesta en marcha de medidas de seguridad). • Presentaciones orales y otras actividades. • Actividades de trabajo en grupo.
Tutorías individuales, grupales y vía web (foro, correo, etc.)	• Resolución de dudas. • Apoyo al aprendizaje autónomo.
Trabajo autónomo	• Lectura crítica de recursos docentes. • Resolución de ejercicios, prácticas o casos, de manera individual o colaborativa • Elaboración de trabajos e informes

5. EVALUACIÓN: Procedimientos, criterios de evaluación y de calificación[1]

Procedimientos

El alumno dispone de dos convocatorias, una ordinaria y otra extraordinaria para la superación de la asignatura.

Convocatoria Ordinaria (Evaluación Continua y Examen Final)

En la convocatoria ordinaria, se distinguen dos posibles vías para la evaluación: Evaluación Continua (EC) y Examen Final (EF). El alumno será evaluado preferentemente mediante el proceso de evaluación continua. Para acogerse al proceso de examen final, el alumno debe solicitarlo por escrito al Director del máster en las dos primeras semanas de su incorporación, indicando las razones que le impiden seguir el sistema de evaluación continua. El Director del máster comunicará la resolución en un máximo de 15 días. En caso de no haber recibido respuesta, se considera estimada esta solicitud.

Convocatoria Extraordinaria

La convocatoria extraordinaria consistirá en una prueba similar al examen final.

Instrumentos de evaluación en Convocatoria Ordinaria

Para el caso de la evaluación continua, se plantea un seguimiento continuo del rendimiento del estudiante mediante trabajos programados y la realización de una prueba parcial a mitad de cuatrimestre, más una prueba de conjunto a realizar al final del cuatrimestre. El caso de examen final considera una única prueba y la realización de un trabajo de la asignatura.

Actividades de seguimiento entregables (E): El seguimiento del trabajo del estudiante permite que el profesor conozca el grado de dedicación del estudiante respecto a las distintas actividades propuestas. A su vez, a los estudiantes les sirve para conocer si van alcanzando los objetivos marcados a lo largo del curso. Las actividades de seguimiento podrán plantearse para hacer en clase, o como trabajo personal para el alumno, y podrán tener carácter individual o grupal. Las actividades de seguimiento suponen un 40% de la calificación final.

Prueba de evaluación Intermedia (PEI): La prueba de Evaluación Intermedia tiene un peso del 30% sobre la calificación final.

Prueba de Evaluación Final (PEF): La Prueba de Evaluación Final tiene un peso del 30% de la calificación final, y persigue un doble objetivo: evaluar la capacidad de relación de los conceptos aprendidos y revisar los conceptos evaluados en la prueba parcial.

Examen Final (EF): El Examen Final consiste en una prueba que incluye cuestiones teóricas y la realización de uno o más ejercicios, con un peso del 60% de la calificación final.

Trabajo de la Asignatura (TA): Supone la realización de un trabajo propuesto por el profesor que supondrá un 40% de la calificación final.

---

[1] *Es importante señalar los procedimientos de evaluación: por ejemplo evaluación continua, final, autoevaluación, co-evaluación. Instrumentos y evidencias: trabajos, actividades. Criterios o indicadores que se van a valorar en relación a las competencias: dominio de conocimientos conceptuales, aplicación, transferencia conocimientos. Para el sistema de calificación hay que recordar la* ***Normativa del Consejo de Gobierno del 16 de julio de 2009****: la calificación de la evaluación continua representará****, al menos, el 60%.*** *Se puede elevar este % en la guía.*

Criterios de Calificación en Evaluación Continua

Competencias	Resultados de Aprendizaje	Instrumento de Evaluación	Peso en la calificación
CG1, CG2, CB6, CB7, CE5, CE7	RA1-RA3	E	40%
CG1, CG2, CB6, CB7, CE5, CE7	RA1-RA3	PEI	30%
CG1, CG2, CB6, CB7, CE5, CE7	RA1-RA3	PEF	30%

Criterios de Calificación en Examen Final

Competencias	Resultados de Aprendizaje	Instrumento de Evaluación	Peso en la calificación
CG1, CG2, CB6, CB7, CE5, CE7	RA1-RA3	EF	60%
CG1, CG2, CB6, CB7, CE5, CE7	RA1-RA3	TA	40%

Instrumentos de evaluación en Convocatoria Extraordinaria

La convocatoria extraordinaria plantea una única prueba de evaluación extraordinaria (PEE), análogo al EF e incorpora cuestiones teóricas junto a la resolución de uno o más ejercicios, con un peso del 60% de la calificación final. Asimismo, deberán entregar un Trabajo de la Asignatura (TA), que supondrá un 40% de la calificación final.

Criterios de Calificación en Evaluación Extraordinaria

Competencias	Resultados de Aprendizaje	Instrumento de Evaluación	Peso en la calificación
CG1, CG2, CB6, CB7, CE5, CE7	RA1-RA3	PEE	60%
CG1, CG2, CB6, CB7, CE5, CE7	RA1-RA3	TA	40%

6. BIBLIOGRAFÍA

Básica

- Amparo Fúster Sabater, Luis Hernández Encinas, Agustín Martín Muñoz, Fausto Montoya Vitini, Jaime Muñoz Masqué, *Criptografía, protección de datos y aplicaciones. Guía para estudiantes y profesionales*. Ra-Ma, Madrid, España, 2012.
- Christof Paar, Jan Pelzl, *Understanding Cryptography. A Textbook for Students and Practitioners*. Springer, Heidelberg, Alemania, 2010.
- Jean-Philippe Aumasson, *Serious Cryptography: A Practical Introduction to Modern Encryption*. No Starch Press, San Francisco, EEUU, 2017.
- Douglas R. Stinson, Maura Paterson, *Cryptography: Theory and Practice*. Chapman and Hall/CRC, Boca Raton, EEUU, 2019.
- Jonathan Katz, Yehuda Lindell, *Introduction to Modern Cryptography*. Chapman and Hall/CRC, Boca Raton, EEUU, 2015.
- Niels Ferguson, Bruce Schneier, Tadayoshi Kohno, *Cryptography Engineering: Design Principles and Practical Applications*. Wiley Publishing, Inc, EEUU, 2010.

Complementaria

- Alfred Menezes, Paul van Oorschot, Scott Vanstone, *Handbook of Applied Cryptography*. CRC Press, Inc, EEUU, 1997.
- Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman, *An Introduction to Mathematical Cryptography*, Springer, EEUU, 2008.
- Antoine Joux, *Algorithmic Cryptanalysis*. Chapman and Hall/CRC, EEUU, 2009.
- Víctor Gayoso Martínez, Luis Hernández Encinas, Agustín Martín Muñoz, *Criptografía con curvas elípticas*. Biblioteca de Ciencias, Consejo Superior de Investigaciones Científicas, Madrid, España, 2018.
- Henri Cohen, Gerhard Frey (eds.), *Handbook of Elliptic and Hyperelliptic Curve Cryptography*. Chapman and Hall/CRC, Boca Raton, EEUU, 2006.
- Raúl Durán Díaz, Luis Hernández Encinas, Jaime Muñoz Masqué, *El criptosistema RSA*. Ra-Ma, Madrid, España, 2005.
- Kenneth H. Rosen, *Elementary Number Theory and its applications*. Pearson, EEUU, 2011.
- Çetin Kaya Koç (ed.), *Cryptographic Engineering*. Springer, EEUU, 2009.
- Daniel J. Bernstein, Johannes Buchmann, Erik Dahmen (eds.), *Post-Quantum Cryptography*. Springer, Berlín, Alemania, 2009.