21-22

MÁSTER UNIVERSITARIO EN
CIBERSEGURIDAD

GUÍA DE ESTUDIO PÚBLICA

CRIPTOGRAFÍA APLICADA

CÓDIGO 31109010

UNED

21-22

CRIPTOGRAFÍA APLICADA

CÓDIGO 31109010

ÍNDICE

Nombre de la asignatura	CRIPTOGRAFÍA APLICADA
Código	31109010
Curso académico	2021/2022
Título en que se imparte	MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD
Tipo	CONTENIDOS
Nº ETCS	6
Horas	150.0
Periodo	SEMESTRE 1
Idiomas en que se imparte	CASTELLANO

PRESENTACIÓN Y CONTEXTUALIZACIÓN

La asignatura Criptografía Aplicada tiene como objetivo presentar los fundamentos criptográficos básicos que todo profesional de la seguridad de los sistemas de información debe conocer. No se pretende que al final de la misma los estudiantes sean expertos criptógrafos de manera que sean capaces de diseñar algoritmos de cifrado o descifrarlos pero si es importante que los estudiantes entiendan cuáles son los fundamentos de los más relevantes en la actualidad, dónde deben ser considerados en los sistemas de información y cuáles son las consecuencias de que se utilice un algoritmo de cifrado u otro. Por ello, la asignatura está orientada hacia la aplicación concreta en los sistemas de información.

REQUISITOS Y/O RECOMENDACIONES PARA CURSAR ESTA ASIGNATURA

Además de los requisitos propios del acceso a la titulación es recomendable que los estudiantes tengan conocimientos de algunas materias que en los Grados relacionados pueden haberse cursado de manera optativa. En concreto conocimientos de aritmética modular pueden facilitar el aprovechamiento completo de la asignatura.
Se recomienda que los interesados en cursar el Máster tengan un nivel de lectura en inglés suficiente como para entender contenidos técnicos en dicha lengua.
Gran parte de la bibliografía, así como los recursos proporcionados al estudiante en el curso virtual pueden estar únicamente en inglés.
Se procurará el uso de software libre siempre y cuando sea posible para la realización de las actividades y las practicas propuestas.
El estudiante deberá tener en cuenta que parte de los materiales estarán en inglés.

EQUIPO DOCENTE

Nombre y Apellidos	ROBERTO HERNANDEZ BERLINCHES (Coordinador de asignatura)
Correo Electrónico	roberto@scc.uned.es
Teléfono	91398-7196
Facultad	ESCUELA TÉCN.SUP INGENIERÍA INFORMÁTICA
Departamento	SISTEMAS DE COMUNICACIÓN Y CONTROL

Nombre y Apellidos	LUIS GRAU FERNANDEZ
Correo Electrónico	lgrau@scc.uned.es
Teléfono	91398-7153
Facultad	ESCUELA TÉCN.SUP INGENIERÍA INFORMÁTICA
Departamento	SISTEMAS DE COMUNICACIÓN Y CONTROL

COLABORADORES DOCENTES EXTERNOS

Nombre y Apellidos	JESUS SALVADOR CANO CARRILLO
Correo Electrónico	jcano@scc.uned.es
Nombre y Apellidos	ANTONIO JUANO AYLLÓN
Correo Electrónico	ajuano@scc.uned.es
Nombre y Apellidos	ANTONIO JUANO AYLLÓN
Correo Electrónico	antjuano@calatayud.uned.es

HORARIO DE ATENCIÓN AL ESTUDIANTE

Martes de 15.00 h a 19.00 h
Las comunicaciones deberán realizarse preferentemente a través del curso virtual

COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE

COMPETENCIAS BÁSICAS

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

CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios

CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades

CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

COMPETENCIAS GENERALES

CG1 - Analizar métodos y técnicas de ciberataques.

CG2 - Diseñar, poner en marcha y mantener un sistema de ciberseguridad.

CG4 - Identificar, gestionar y desarrollar medidas y protocolos de seguridad en la operación y gestión de sistemas informáticos.

COMPETENCIAS TRANSVERSALES

CT1 - Ser capaz de abordar y desarrollar proyectos innovadores en entornos científicos, tecnológicos y multidisciplinares.
CT2 - Ser capar de tomar decisiones y formular juicios basados en criterios objetivos (datos experimentales, científicos o de simulación disponibles).

COMPETENCIAS ESPECÍFICAS

CE1 - Utilizar mecanismos criptográficos avanzados para garantizar los requisitos de seguridad en un sistema, así como el acceso y seguridad en las comunicaciones.

RESULTADOS DE APRENDIZAJE

Los resultados básicos más relevantes que se pretenden alcanzar con el estudio de esta asignatura son los siguientes:

·Comprender los fundamentos matemáticos que sustentan la criptología.
·Elegir entre los diversos algoritmos de criptografía existentes aquellos más adecuados a los escenarios de la ciberseguridad.
·Desarrollar la implementación de algoritmos criptográficos en entornos de programación real.
·Analizar un texto cifrado utilizando diversas técnicas de criptoanálisis con el fin de determinar cuál es el texto plano asociado.
·Comprender la criptología post computacional-cuántica.
·Analizar el papel de la criptología en las diversas aplicaciones actuales.

CONTENIDOS

Principios matemáticos de la criptografía

Criptología para la ciberseguridad

Criptoanálisis

Criptología y computación cuántica

Aplicaciones de la criptografía

METODOLOGÍA

Como todas las asignaturas que integran este Máster se impartirá conforme a la metodología no presencial que caracteriza a la UNED, en la cual prima el autoaprendizaje del estudiante, asistido por el profesor y articulado a través de diversos sistemas de comunicación docente-discente. Dentro de estos sistemas, el Máster en Ciberseguridad se imparte con apoyo en una plataforma virtual interactiva de la UNED donde el estudiante encuentra tanto materiales didácticos básicos como materiales didácticos complementarios, informaciones, noticias, ejercicios y también permite la evaluación correspondiente a las diferentes materias.

SISTEMA DE EVALUACIÓN

TIPO DE PRUEBA PRESENCIAL

Tipo de examen	Examen mixto
Preguntas test	8
Preguntas desarrollo	1
Duración del examen	120 (minutos)

Material permitido en el examen

Como ayuda para la resolución del problema, en el examen se perite el uso del texto Técnicas Criptográficas de Protección de Datos. FÚSTER, A. y Otros, Editorial RA-MA. **También está permitido el uso de calculadora.**

Criterios de evaluación

La calificación máxima del cuestionario test es 4. Cada pregunta se valora 0.5 si hay acierto, resta 0.25 si hay fallo. En blanco no resta. La calificación máxima del problema es 3

La calificación del Trabajo Práctico se sumará a la del examen si y sólo si la calificación del examen es mayor o igual que 4

% del examen sobre la nota final	70
Nota del examen para aprobar sin PEC	
Nota máxima que aporta el examen a la calificación final sin PEC	
Nota mínima en el examen para sumar la PEC	

Comentarios y observaciones

CARACTERÍSTICAS DE LA PRUEBA PRESENCIAL Y/O LOS TRABAJOS

Requiere Presencialidad	No

Descripción

El trabajo práctico será propuesto por el equipo docente y deberá comenzar a realizarse al inicio del segundo mes de la asignatura y deberá entregarse el viernes anterior a la primera semana de exámenes de la UNED.

Criterios de evaluación

En la evaluación del trabajo se tendrá en cuenta además de la corrección del mismo, su presentación, la claridad de la explicación y las aportaciones del estudiante.

Ponderación de la prueba presencial y/o los trabajos en la nota final: 70% prueba presencial 30% Trabajo Práctico

Fecha aproximada de entrega

Comentarios y observaciones

PRUEBAS DE EVALUACIÓN CONTINUA (PEC)

¿Hay PEC? No

Descripción

Criterios de evaluación

Ponderación de la PEC en la nota final

Fecha aproximada de entrega

Comentarios y observaciones

OTRAS ACTIVIDADES EVALUABLES

¿Hay otra/s actividad/es evaluable/s? No

Descripción

Criterios de evaluación

Ponderación en la nota final

Fecha aproximada de entrega

Comentarios y observaciones

¿CÓMO SE OBTIENE LA NOTA FINAL?

La calificación máxima del cuestionario test es 4. Cada pregunta se valora 0.5 si hay acierto, resta 0.25 si hay fallo. En blanco no resta. La calificación máxima del problema es 3. La calificación máxima de la prueba presencial es 7.0

La calificación del Trabajo Práctico se sumará a la de la prueba presencial si y sólo si la calificación del examen es mayor o igual que 4.

La calificación final será la suma de la calificación de la prueba presencial y la del trabajo

BIBLIOGRAFÍA BÁSICA

Para el estudio de la asignatura se utilizarán diversos materiales incluidos mayoritariamente en el curso virtual. Algunos de ellos serán textos de libre distribución, artículos, materiales preparados por el equipo docente, etc.

En concreto, se hará uso del texto “Criptografía y Seguridad en computadores”, Lucena y del texto permitido en la prueba presencial “Técnicas Criptográficas de Protección de Datos”. FÚSTER, A. y Otros, Editorial RA-MA.

BIBLIOGRAFÍA COMPLEMENTARIA

ISBN(13):9780387942933
Título:A COURSE IN NUMBER THEORY AND CRYPTOGRAPHY (2nd ed.)
Autor/es:
Editorial:Springer

ISBN(13):9780471128458
Título:APPLIED CRYPTOGRAPHY : (2nd ed.)
Autor/es:
Editorial:JOHN WILEY AND SONS

ISBN(13):9780521653749
Título:ELLIPTIC CURVES IN CRYPTOGRAPHY
Autor/es:Smart, Nigel P. ; Seroussi, Gadiel ;
Editorial:CAMBRIDGE UNIVERSITY PRESS..

ISBN(13):9783540613565
Título:PUBLIC-KEY CRYPTOGRAPHY (2nd enl. ed.)
Autor/es:
Editorial:Springer

Cryptography and Network Security Principles and Practice, 7th Edition, W. Stallings

RECURSOS DE APOYO Y WEBGRAFÍA

IGUALDAD DE GÉNERO

En coherencia con el valor asumido de la igualdad de género, todas las denominaciones que en esta Guía hacen referencia a órganos de gobierno unipersonales, de representación, o miembros de la comunidad universitaria y se efectúan en género masculino, cuando no se hayan sustituido por términos genéricos, se entenderán hechas indistintamente en género femenino o masculino, según el sexo del titular que los desempeñe.