Escuela de Doctorado
y Estudios de Posgrado
Universidad de La Laguna

Escuela de Doctorado y Estudios de Posgrado

Máster Universitario en Ciberseguridad e Inteligencia de Datos

GUÍA DOCENTE DE LA ASIGNATURA :

Criptografía de Clave Secreta
(2022 - 2023)

1. Datos descriptivos de la asignatura

Asignatura: Criptografía de Clave Secreta	Código: 835870901

- Centro: **Escuela de Doctorado y Estudios de Postgrado**
- Lugar de impartición: **-**
- Titulación: **Máster Universitario en Ciberseguridad e Inteligencia de Datos**
- Plan de Estudios: **2018 (Publicado en 2018-09-19)**
- Rama de conocimiento: **Ingeniería y Arquitectura**
- Itinerario / Intensificación:
- Departamento/s:
  Ingeniería Informática y de Sistemas
- Área/s de conocimiento:
  Ciencia de la Computación e Inteligencia Artificial
- Curso: **1**
- Carácter:
- Duración: **Primer cuatrimestre**
- Créditos ECTS: **3,0**
- Modalidad de impartición: **Semipresencial**
- Horario: **Enlace al horario**
- Dirección web de la asignatura: **http://www.campusvirtual.ull.es**
- Idioma: **Castellano e Inglés (0,15 ECTS en Inglés)**

2. Requisitos para cursar la asignatura

3. Profesorado que imparte la asignatura

Profesor/a Coordinador/a: PINO TERESA CABALLERO GIL

- Grupo: **C1 y L1**

General
- Nombre: **PINO TERESA**
- Apellido: **CABALLERO GIL**
- Departamento: **Ingeniería Informática y de Sistemas**
- Área de conocimiento: **Ciencia de la Computación e Inteligencia Artificial**

Contacto
- Teléfono 1: **922 31 8176**
- Teléfono 2:
- Correo electrónico: **pcaballe@ull.es**
- Correo alternativo: **pcaballe@ull.edu.es**
- Web: **https://pcaballe.webs.ull.es/PCG.htm**

Tutorías primer cuatrimestre:

Desde	Hasta	Día	Hora inicial	Hora final	Localización	Despacho
Todo el cuatrimestre		Lunes	09:00	12:00	Escuela Superior de Ingeniería y Tecnología - Módulo A - AN.4A ESIT	P2.035
Todo el cuatrimestre		Miércoles	11:30	14:30	Escuela Superior de Ingeniería y Tecnología - Módulo A - AN.4A ESIT	P2.035

Observaciones: Este horario es orientativo. Prevalecerá el que se ponga en las aulas virtuales de las asignaturas. Es recomendable reservar cita para las tutorías enviando mail a la profesora. Las tutorías podrán realizarse en modalidad presencial o telemática a través de Google Meet.

Tutorías segundo cuatrimestre:

Desde	Hasta	Día	Hora inicial	Hora final	Localización	Despacho
Todo el cuatrimestre		Lunes	09:00	12:00	Escuela Superior de Ingeniería y Tecnología - Módulo A - AN.4A ESIT	P2.035
Todo el cuatrimestre		Miércoles	11:30	14:30	Escuela Superior de Ingeniería y Tecnología - Módulo A - AN.4A ESIT	P2.035

Observaciones: Este horario es orientativo. Prevalecerá el que se ponga en las aulas virtuales de las asignaturas. Es recomendable reservar cita para las tutorías enviando mail a la profesora. Las tutorías podrán realizarse en modalidad presencial o telemática a través de Google Meet.

Profesor/a: **MARIA CANDELARIA HERNANDEZ GOYA**

- Grupo: **C1 y L1**

General
- Nombre: **MARIA CANDELARIA**
- Apellido: **HERNANDEZ GOYA**
- Departamento: **Ingeniería Informática y de Sistemas**
- Área de conocimiento: **Ciencia de la Computación e Inteligencia Artificial**

Contacto
- Teléfono 1: **922 316 502 Ext 6827**
- Teléfono 2: **922 316 502 Ext 6827**
- Correo electrónico: **mchgoya@ull.es**
- Correo alternativo:
- Web: **http://www.campusvirtual.ull.es**

Tutorías primer cuatrimestre:

Desde	Hasta	Día	Hora inicial	Hora final	Localización	Despacho
Todo el cuatrimestre		Martes	10:00	12:00	Escuela Superior de Ingeniería y Tecnología - Módulo A - AN.4A ESIT	P2.026
Todo el cuatrimestre		Jueves	10:00	12:00	Escuela Superior de Ingeniería y Tecnología - Módulo A - AN.4A ESIT	P2.026
Todo el cuatrimestre		Miércoles	10:00	12:00	Escuela Superior de Ingeniería y Tecnología - Módulo A - AN.4A ESIT	P2.026

Observaciones: Las modificaciones de este horario por causas sobrevenidas se comunicarán a través del campus virtual. Las tutorías de los jueves, de 10:00 a 12:00, serán en línea. Para llevar a cabo la tutoría en línea se hará uso del Google Meet https://meet.google.com/rii-asrj-dxt

Tutorías segundo cuatrimestre:

Desde	Hasta	Día	Hora inicial	Hora final	Localización	Despacho
Todo el cuatrimestre		Martes	12:00	14:00	Escuela Superior de Ingeniería y Tecnología - Módulo A - AN.4A ESIT	P2.026

Todo el cuatrimestre		Miércoles	12:00	14:00	Escuela Superior de Ingeniería y Tecnología - Módulo A - AN.4A ESIT	P2.026
Todo el cuatrimestre		Viernes	10:00	12:00	Escuela Superior de Ingeniería y Tecnología - Módulo A - AN.4A ESIT	P2.026

Observaciones: Las modificaciones de este horario por causas sobrevenidas se comunicarán a través del campus virtual. Las tutorías de los viernes, de 10:00 a 12:00, serán en línea. Para llevar a cabo la tutoría en línea se hará uso del Google Meet https://meet.google.com/bfv-ajyu-xhe.

Profesor/a: **CARLOS BENJAMÍN ROSA REMEDIOS**

- Grupo: **C1 y L1**

General
- Nombre: **CARLOS BENJAMÍN**
- Apellido: **ROSA REMEDIOS**
- Departamento: **Ingeniería Informática y de Sistemas**
- Área de conocimiento: **Ciencia de la Computación e Inteligencia Artificial**

Contacto
- Teléfono 1:
- Teléfono 2:
- Correo electrónico: **crosarem@ull.es**
- Correo alternativo:
- Web: **http://www.campusvirtual.ull.es**

Tutorías primer cuatrimestre:

Desde	Hasta	Día	Hora inicial	Hora final	Localización	Despacho
01-10-2022	30-10-2022	Martes	16:00	18:00	Escuela Superior de Ingeniería y Tecnología - Módulo C - AN.4A ESIT	

01-10-2022	30-10-2022	Miércoles	16:00	17:00	Escuela Superior de Ingeniería y Tecnología - Módulo C - AN.4A ESIT	
01-10-2022	30-10-2022	Miércoles	18:00	20:00	Escuela Superior de Ingeniería y Tecnología - Módulo C - AN.4A ESIT	
01-10-2022	30-10-2022	Jueves	15:30	16:30	Escuela Superior de Ingeniería y Tecnología - Módulo C - AN.4A ESIT	
31-10-2022	11-12-2022	Lunes	15:30	18:00	Escuela Superior de Ingeniería y Tecnología - Módulo C - AN.4A ESIT	
31-10-2022	11-12-2022	Jueves	15:30	17:00	Escuela Superior de Ingeniería y Tecnología - Módulo C - AN.4A ESIT	
31-10-2022	11-12-2022	Jueves	18:00	20:00	Escuela Superior de Ingeniería y Tecnología - Módulo C - AN.4A ESIT	
12-12-2022	31-01-2023	Martes	15:30	19:00	Escuela Superior de Ingeniería y Tecnología - Módulo C - AN.4A ESIT	

12-12-2022	31-01-2023	Miércoles	15:30	17:00	Escuela Superior de Ingeniería y Tecnología - Módulo C - AN.4A ESIT	
12-12-2022	31-01-2023	Miércoles	19:00	20:00	Escuela Superior de Ingeniería y Tecnología - Módulo C - AN.4A ESIT	
Observaciones: Atendiendo a las medidas referentes a la prevención del contagio del virus SARS-CoV-2, todas las tutorías deben solicitarse previamente por correo electrónico para evitar aglomeraciones. En la medida de lo posible, se recomienda consultar las dudas a través de correo electrónico o realizar las tutorías a través de Google Meet.						
Tutorías segundo cuatrimestre:						
Desde	**Hasta**	**Día**	**Hora inicial**	**Hora final**	**Localización**	**Despacho**
Todo el cuatrimestre		Martes	15:30	17:00	Escuela Superior de Ingeniería y Tecnología - Módulo C - AN.4A ESIT	
Todo el cuatrimestre		Martes	19:00	20:00	Escuela Superior de Ingeniería y Tecnología - Módulo C - AN.4A ESIT	
Todo el cuatrimestre		Miércoles	15:30	18:00	Escuela Superior de Ingeniería y Tecnología - Módulo C - AN.4A ESIT	
Todo el cuatrimestre		Miércoles	19:00	20:00	Escuela Superior de Ingeniería y Tecnología - Módulo C - AN.4A ESIT	

Observaciones: Atendiendo a las medidas referentes a la prevención del contagio del virus SARS-CoV-2, todas las tutorías deben solicitarse previamente por correo electrónico para evitar aglomeraciones. En la medida de lo posible, se recomienda consultar las dudas a través de correo electrónico o realizar las tutorías a través de Google Meet.

4. Contextualización de la asignatura en el plan de estudio

Bloque formativo al que pertenece la asignatura:
Perfil profesional:

5. Competencias

Generales

CG1 - Ser capaces de aplicar los conocimientos adquiridos para resolver problemas en entornos nuevos o poco conocidos dentro de contextos relacionados con seguridad informática o inteligencia de datos
CG3 - Mantener una actitud de permanente actualización, que les permita estudiar de manera autónoma mediante formación continua en su futuro desempeño profesional como expertos en seguridad informática e inteligencia de datos
CG4 - Diseñar y elaborar planes de intervención profesional o proyectos de investigación relacionados con el entorno de seguridad informática, e implementarlos y desarrollarlos mediante los métodos y procesos adecuados
CG5 - Adquirir el grado de especialización necesario para ejercer las funciones profesionales de experto en seguridad informática e inteligencia de datos, en el seno de entidades de TIC
CG6 - Evaluar los recursos necesarios, planificar y organizar las actividades, sin olvidar la continua revisión del proceso que conlleva la seguridad informática y la inteligencia de datos
CG9 - Manejar adecuadamente información relativa al sector de la seguridad informática atendiendo a la legislación vigente, estándares, certificaciones, documentos internos, etc.

Básicas

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
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

Específicas

CE1 - Capacidad de seleccionar y aplicar adecuadamente diferentes mecanismos de cifrado y autenticación para garantizar la confidencialidad, integridad y autenticidad de los datos
CE2 - Capacidad de verificar el funcionamiento correcto de las medidas de seguridad, y el cumplimiento de las normas y las leyes que corresponden

6. Contenidos de la asignatura

Contenidos teóricos y prácticos de la asignatura

Temas:

1. El concepto de clave secreta.
2. Confidencialidad: algoritmos de cifrado.
3. Cifrado en bloque.
4. Cifrado en flujo.
5. Modos de cifrado.
6. Protocolos para la gestión y distribución de claves.
7. Protocolos de autenticación con clave secreta.
8. Integridad de datos con clave secreta.

Actividades a desarrollar en otro idioma

En esta asignatura se impartirán 1,5 horas de clases en inglés.
Además se trabajará preferentemente sobre bibliografía en inglés, y el alumnado deberá ser capaz de extraer la información necesaria para seguir la asignatura a partir de dicha documentación, junto con los apuntes del profesorado.

7. Metodología y volumen de trabajo del estudiante

Descripción

La metodología docente de las clases teóricas consistirá en sesiones en las que el profesorado explicará los conceptos fundamentales de cada tema que deben ser asimilados por el alumnado, bien presencialmente, o no presencialmente mediante retransmisión online, en directo usando videoconferencia o en diferido a través de grabaciones colgadas en el entorno virtual.
La metodología docente de las clases prácticas consistirá en sesiones supervisadas en grupos reducidos en el laboratorio en las que se realizarán diversas prácticas informáticas de dificultad creciente aplicando los conceptos expuestos en las clases de teoría. Además, el alumnado aprenderá a usar diversas herramientas, en entornos reales o de simulación, así como metodologías relacionadas con el contexto de la materia.
La metodología docente de los informes consistirá en el desarrollo por parte del alumnado de su capacidad para la aplicación de los conocimientos adquiridos y la resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios y multidisciplinares, siendo capaces de integrar estos conocimientos.
Se plantea una metodología docente para los seminarios que consistirá en sesiones donde se llevará a cabo una explicación más detallada de determinados aspectos concretos de algunos temas teóricos o prácticos especialmente relevantes. Se ofrecerán seminarios donde profesionales de esta materia harán charlas debates con el alumnado de los temas relacionados con el mundo profesional.
Las tutorías individuales ayudarán a reforzar los diferentes aspectos de la materia y ayudarán al alumnado en la comprensión de la teoría y la realización de las prácticas.

Actividades formativas en créditos ECTS, su metodología de enseñanza-aprendizaje y su relación con las competencias que debe adquirir el estudiante

Actividades formativas	Horas presenciales	Horas de trabajo autónomo	Total horas	Relación con competencias
Clases teóricas	5,00	5,00	10,0	[CE2], [CE1], [CG3]
Clases prácticas (aula / sala de demostraciones / prácticas laboratorio)	8,00	8,00	16,0	[CE2], [CE1], [CG5], [CG4], [CG1]
Realización de seminarios u otras actividades complementarias	1,00	1,00	2,0	[CE2], [CE1]
Estudio/preparación de clases teóricas	0,00	10,00	10,0	[CE2], [CE1], [CG3]
Estudio/preparación de clases prácticas	0,00	6,00	6,0	[CE2], [CE1], [CG5], [CG4], [CG1]
Realización de exámenes	1,00	0,00	1,0	[CG6]
Asistencia a tutorías	0,00	6,00	6,0	[CE2], [CE1], [CG9], [CG6]
Informes, trabajos y proyectos	0,00	24,00	24,0	[CB10], [CB8], [CB7], [CG5], [CG4], [CG3], [CG1]
Total horas	15,00	60,00	75,00	
		Total ECTS	3,00	

8. Bibliografía / Recursos

Bibliografía Básica

Smart, Nigel Paul. Cryptography made simple (2016). ISBN:9783319219356978331921963
Paar, Christof. Understanding cryptography : a textbook for students and practitioners. Editorial:Springer, 2010.
Caballero Gil, Pino. Introducción a la criptografía (2002) 2 ed. actualizada. Editorial: Madrid : RA-MA, 2002. ISBN: 84-7897-520-9

Bibliografía Complementaria

Otros Recursos

9. Sistema de evaluación y calificación

Descripción

La evaluación de la teoría contribuirá a la evaluación de la asignatura con un 40%, mientras que la evaluación de la práctica lo hará con un 60%.
Las herramientas utilizadas en la evaluación continua serán las siguientes.
La Calificación de Teoría (CT) se obtendrá mediante participación en clases de teoría, tareas y pruebas escritas (40%), mientras que la Calificación de Prácticas (CP) mediante participación en clases de prácticas, informes y memorias de prácticas (20%) + seminarios con tareas reales y/o simuladas (20%) + trabajos y proyectos (20%).
Ambas calificaciones serán valores entre 0 y 10, de forma que la Calificación Final (CF) se obtendrá mediante la fórmula: CF= 0,40*CT + 0,60*CP, si y solo si CT>=5 y CP>=5. En otro caso, CF= min(CT, CP)
El alumnado que no supere la evaluación continua podrá participar en la evaluación única participando en las diferentes convocatorias con pruebas de evaluación destinadas a evaluar las mismas competencias y resultados de aprendizaje de la asignatura.

Estrategia Evaluativa

Tipo de prueba	Competencias	Criterios	Ponderación
Pruebas objetivas	[CG9], [CG6], [CG5], [CG4], [CG3], [CG1]	- Nivel de conocimientos adquiridos y nivel de comprensión alcanzado en la aplicación de los contenidos explicados. - Adecuación a lo solicitado.	40,00 %
Trabajos y proyectos	[CB10], [CB8], [CB7]	- Calidad del trabajo desarrollado y concreción en la redacción - Interés demostrado - Adecuación a lo solicitado.	20,00 %
Informes memorias de prácticas	[CE2], [CE1]	- Nivel de comprensión alcanzado en la aplicación de los contenidos explicados así como la destreza técnica desarrollada durante las prácticas. - Adecuación a lo solicitado.	20,00 %
Pruebas de ejecuciones de tareas reales y/o simuladas	[CE1], [CB8], [CB7], [CG1]	- Nivel de comprensión alcanzado en la aplicación de los contenidos explicados así como la destreza técnica desarrollada durante las prácticas. - Adecuación a lo solicitado.	20,00 %

10. Resultados de Aprendizaje

Al finalizar la asignatura el alumnado debe: conocer los conceptos básicos y fundamentos de los algoritmos criptográficos de clave secreta más utilizados y su aplicación en los protocolos de comunicación más habituales, saber analizar el nivel de seguridad de cada uno de los algoritmos, y resolver la problemática de la distribución de claves.

11. Cronograma / calendario de la asignatura

Descripción

Debido al carácter semipresencial del máster, está previsto que las clases presenciales se desarrollen de la forma siguiente: el alumnado tendrá 3 horas diarias las semanas 1 a 5 y 8 a 12 del primer cuatrimestre, y 3 o 4 horas diarias las semanas 1 a 5 del segundo cuatrimestre.
Todas las asignaturas se desarrollarán en bimestres, y concretamente esta asignatura se impartirá en el bimestre 1.
El cronograma que se presenta es a título estimativo, de modo que el profesorado podrá modificar dicha planificación temporal si así lo demanda el desarrollo de la asignatura.

Primer cuatrimestre					
Semana	Temas	Actividades de enseñanza aprendizaje	Horas de trabajo presencial	Horas de trabajo autónomo	Total
Semana 1:	1 y 2	Clases teóricas y prácticas y seminarios presenciales. Actividades con material disponible en el aula virtual.	2.00	8.00	10.00
Semana 2:	3	Clases teóricas y prácticas y seminarios presenciales. Actividades con material disponible en el aula virtual.	3.00	7.00	10.00
Semana 3:	4	Clases teóricas y prácticas y seminarios presenciales. Actividades con material disponible en el aula virtual.	3.00	7.00	10.00
Semana 4:	5	Clases teóricas y prácticas y seminarios presenciales. Actividades con material disponible en el aula virtual.	3.00	7.00	10.00
Semana 5:	6, 7 y 8	Clases teóricas y prácticas y seminarios presenciales. Actividades con material disponible en el aula virtual.	3.00	7.00	10.00
Semana 6:	6	Actividades con material disponible en el aula virtual. Seminarios utilizando el campus virtual y realización de cuestionarios on-line. Videotutoriales y foro para la resolución de dudas.	0.00	10.00	10.00

Semana 7:	7	Actividades con material disponible en el aula virtual. Seminarios utilizando el campus virtual y realización de cuestionarios on-line. Videotutoriales y foro para la resolución de dudas.	0.00	10.00	10.00
Semana 8:	8	Actividades con material disponible en el aula virtual. Seminarios utilizando el campus virtual y realización de cuestionarios on-line. Videotutoriales y foro para la resolución de dudas.	0.00	4.00	4.00
Semana 15:	Evaluación única	Evaluación del alumnado	1.00	0.00	1.00
		Total	15.00	60.00	75.00