1. DATOS BÁSICOS

Asignatura	Criptografía
Titulación	Grado en Ingeniería de la Ciberseguridad
Escuela/ Facultad	Escuela de Arquitectura, Ingeniería y Diseño
Curso	Segundo
ECTS	6
Carácter	Obligatoria
Idioma/s	Castellano
Modalidad	Online
Semestre	Tercer Semestre
Curso académico	2024/2025
Docente coordinador	JOSE JAVIER RUIZ COBO
Docente	ALBERTO LOPEZ GONZALEZ

2. PRESENTACIÓN

La materia denominada criptografía comprende un vasto campo de elementos relacionados con:

- La matemática.
- La algorítmica.
- Los sistemas de tratamiento de información.
- La comunicación, el intercambio y el almacenamiento de información.
- La ingeniería de software.
- La ingeniería de (ciber)seguridad de la información y la seguridad informática.

La criptografía presenta múltiples ramas, siendo el denominador común convertir información en ininteligible y tal que pueda recuperarse pero solo bajo ciertas condiciones. La materia, criptografía, comprenderá los métodos empleados para el tratamiento y resolución de problemas de dicha amplia naturaleza, incluyendo, todas las técnicas que resuelven problemas empleando técnicas de ocultar información.

El alumno deberá ser capaz de comprender los conceptos, protocolos y algoritmos tanto de la criptografía simétrica como de la criptografía asimétrica.

3. RESULTADOS DE APRENDIZAJE

Conocimientos

CON07. Reconocer los algoritmos criptográficos de clave pública y de clave privada más importantes, así como sus aplicaciones en ciberseguridad.

- Explicar el concepto de criptografía y la teoría de la complejidad

- Describir las bases y aplicaciones de las técnicas de criptografía avanzada

Habilidades
HAB06 Aplicar las arquitecturas y modelos de ciberseguridad.

- Aplicar las técnicas de criptografía simétrica.
- Desarrollar un sistema de intercambio y comprobación de hash
- Aplicar las técnicas de criptografía asimétrica
- Desarrollar un sistema de firma digital basado en cifrado asimétrico

Competencias
CP05. Diseñar, desarrollar y mantener técnicas y soluciones para la protección de los datos (almacenados, procesados o en tránsito), considerando en todo momento la privacidad de éstos.
CP10. Aplicar y analizar los principios y técnicas basadas en la criptografía que permiten garantizar la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos y de la información, así como la autenticación y autorización de sus entidades.
CP14. Utilizar las tecnologías de la información y de la comunicación para la búsqueda y análisis de datos, la investigación, la comunicación y el aprendizaje.
CP16. Cooperar con otros en la consecución de un objetivo compartido, participando de manera activa, empática y ejerciendo la escucha activa y el respeto a todos los integrantes.
CP17. Integrar el análisis con el pensamiento crítico en un proceso de evaluación de distintas ideas o posibilidades y su potencial de error, basándose en evidencias y datos objetivos que lleven a una toma de decisiones eficaz y válida.

4. CONTENIDOS

- Introducción a la criptografía. Teoría de Complejidad
- Criptografía clásica. Cifrado simétrico.
- Funciones Hash.
- Cifrado asimétrico. Intercambio de clave. Firma digital.
- Criptografía cuántica
- Esquemas de compromiso.
- Compartición de secretos

5. METODOLOGÍAS DE ENSEÑANZA-APRENDIZAJE

A continuación, se indican los tipos de metodologías de enseñanza-aprendizaje que se aplicarán:

- Clase magistral/ web conference
- Aprendizaje cooperativo
- Aprendizaje basado en problemas
- Aprendizaje basado en enseñanzas de taller virtual
- Entornos de simulación

6. ACTIVIDADES FORMATIVAS

A continuación, se identifican los tipos de actividades formativas que se realizarán y la dedicación en horas del estudiante a cada una de ellas:

Modalidad virtual:

Actividad formativa	Número de horas
Clases magistrales	8
Clases virtuales	26
Resolución de problemas	30
Laboratorios Virtuales	12
Estudios de contenidos y documentación complementaria	50
Foro virtual	4
Tutoría virtual	18
Pruebas de evaluación virtuales	2
TOTAL	**150**

7. EVALUACIÓN

A continuación, se relacionan los sistemas de evaluación, así como su peso sobre la calificación total de la asignatura:

Modalidad virtual:

Sistema de evaluación	Peso
Pruebas de evaluación virtuales	60 %

Caso/ Problema. Proyecto grupal	20 %
Cuaderno de prácticas	20%

En el Campus Virtual, cuando accedas a la asignatura, podrás consultar en detalle las actividades de evaluación que debes realizar, así como las fechas de entrega y los procedimientos de evaluación de cada una de ellas.

7.1. Convocatoria ordinaria

Para superar la asignatura en convocatoria ordinaria deberás obtener una calificación mayor o igual que 5,0 sobre 10,0 en la calificación final (media ponderada) de la asignatura.

En todo caso, será necesario que obtengas una calificación mayor o igual que 5,0 en la prueba final, para que la misma pueda hacer media con el resto de actividades.

7.2. Convocatoria extraordinaria

Para superar la asignatura en convocatoria extraordinaria deberás obtener una calificación mayor o igual que 5,0 sobre 10,0 en la calificación final (media ponderada) de la asignatura.

En todo caso, será necesario que obtengas una calificación mayor o igual que 5,0 en la prueba final, para que la misma pueda hacer media con el resto de actividades.

Se deben entregar las actividades no superadas en convocatoria ordinaria, tras haber recibido las correcciones correspondientes a las mismas por parte del docente, o bien aquellas que no fueron entregadas.

8. CRONOGRAMA

En este apartado se indica el cronograma con fechas de entrega de actividades evaluables de la asignatura:

Actividades evaluables	Fecha
1 y 2	1, 2 y 3
3 y 4	4, 5, 6, 7, 8, 9, 10, 11 y 12
5,6,7	13, 14, 15, 16 y 17
Prueba de conocimiento	18

Este cronograma podrá sufrir modificaciones por razones logísticas de las actividades. Cualquier modificación será notificada al estudiante en tiempo y forma.

9. BIBLIOGRAFÍA

La obra de referencia para el seguimiento de la asignatura es:

- Stallings, W. (2014). Cryptography and Network Security. Publisher: Prentice Hall.

A continuación, se indican referencias recomendadas:

- Schneier, B. (1996). *Applied Cryptography, Second Edition*. John Wiley & Sons
- Menezes, Alfred (1996). Handbook of Applied Cryptography. CRC.
- Pointcheval, D. (2022). Asymmetric Cryptography: Primitives and Protocols. Wiley.
- FIPS PUB 180-4, (2015). Secure Hash Standard (SHS), FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, NIST

10. UNIDAD DE ORIENTACIÓN EDUCATIVA Y DIVERSIDAD

Desde la Unidad de Orientación Educativa y Diversidad (ODI) ofrecemos acompañamiento a nuestros estudiantes a lo largo de su vida universitaria para ayudarles a alcanzar sus logros académicos. Otros de los pilares de nuestra actuación son la inclusión del estudiante con necesidades específicas de apoyo educativo, la accesibilidad universal en los distintos campus de la universidad y la equiparación de oportunidades.

Desde esta Unidad se ofrece a los estudiantes:

1. Acompañamiento y seguimiento mediante la realización de asesorías y planes personalizados a estudiantes que necesitan mejorar su rendimiento académico.
2. En materia de atención a la diversidad, se realizan ajustes curriculares no significativos, es decir, a nivel de metodología y evaluación, en aquellos alumnos con necesidades específicas de apoyo educativo persiguiendo con ello una equidad de oportunidades para todos los estudiantes.
3. Ofrecemos a los estudiantes diferentes recursos formativos extracurriculares para desarrollar diversas competencias que les enriquecerán en su desarrollo personal y profesional.
4. Orientación vocacional mediante la dotación de herramientas y asesorías a estudiantes con dudas vocacionales o que creen que se han equivocado en la elección de la titulación

Los estudiantes que necesiten apoyo educativo pueden escribirnos a:
orientacioneducativa@universidadeuropea.es

11. ENCUESTAS DE SATISFACCIÓN

¡Tu opinión importa!

La Universidad Europea te anima a participar en las encuestas de satisfacción para detectar puntos fuertes y áreas de mejora sobre el profesorado, la titulación y el proceso de enseñanza-aprendizaje.

Las encuestas estarán disponibles en el espacio de encuestas de tu campus virtual o a través de tu correo electrónico.

Tu valoración es necesaria para mejorar la calidad de la titulación.

Muchas gracias por tu participación.

PLAN DE TRABAJO DE LA ASIGNATURA

CÓMO COMUNICARTE CON TU DOCENTE

Cuando tengas una duda sobre los contenidos o actividades, no olvides escribirla en los foros de tu asignatura para que todos tus compañeros y compañeras puedan leerla.

¡Es posible que alguien tenga tu misma duda!

Si tienes alguna consulta exclusivamente dirigida al docente puedes enviarle un mensaje privado desde el Campus Virtual. Además, en caso de que necesites profundizar en algún tema, puedes acordar una tutoría.

Es conveniente que leas con regularidad los mensajes enviados por estudiantes y docentes, pues constituyen una vía más de aprendizaje.

CRONOGRAMA DE ACTIVIDADES

En este apartado se indica el cronograma de actividades formativas, así como las fechas de entrega de las actividades evaluables de la asignatura:

Semana	Contenidos	Actividades formativas/evaluables	Peso en la evaluación de la actividad evaluable
Semana 6	Bloques 1	Actividad individual	2%
Semana 9	Bloque 2	Actividad individual	8%
Semana 12	Bloque 3	Actividad individual	10%
Semana 13	Bloque 1, 2, 3 y 4.	Proyecto Grupal	20%
Semana 18	Bloque 1, 2, 3 y 4.	Prueba final	60%

Este cronograma podrá sufrir modificaciones que serán notificadas al estudiante en tiempo y forma.

DESCRIPCIÓN DE LAS ACTIVIDADES DE EVALUACIÓN

ctividades individuales y/o colaborativas

ACTIVIDAD: Actividades individuales y/o colaborativas

• ¿Qué son las actividades individuales y/o colaborativas?
  • Las actividades individuales y/o colaborativas consistirán en la resolución de problemas y ejercicios prácticos planteados al estudiante en clase presencial y/o a través del Campus Virtual, relacionados con los contenidos del curso. Deberán realizarse en el aula o fuera del horario oficial de clase presencial y/o virtual, según se indique en cada caso.
  • Las entregas de las actividades individuales se realizarán siempre a través del recurso online correspondiente que se habilitará en el Campus Virtual de la asignatura. El procedimiento de entrega de las actividades colaborativas será idéntico, salvo que el docente solicite su entrega en clase presencial y/o virtual al terminar la sesión de trabajo. Cada tarea tiene asociada un plazo límite de realización oficial, de forma que toda entrega que se encuentre fuera de plazo será calificada con cero puntos sobre diez.
• ¿Qué tenemos que hacer?
  • Realizar y entregar los ejercicios planteados en clase o en la tarea correspondiente del Campus Virtual, dentro de los plazos definidos.
  • De tratarse de una actividad colaborativa, trabajar activamente y de forma eficiente con tu equipo durante la realización de los ejercicios planteados, realizando preguntas que puedan ser de interés para tus compañeros.
• Tipo de actividad: Individual / Colaborativa
• Tipo de evaluación: Diagnóstica y formativa
  • El profesor recibirá los ejercicios de los estudiantes, los corregirá y calificará, señalando los errores cometidos.
• Peso: 20%
• ¿Cómo se evalúa?: Se evalúa según la rúbrica disponible en el Campus Virtual y que se muestra en la tabla inferior.

Proyecto grupal:

ACTIVIDAD: Proyecto grupal

- ¿Qué es la actividad de proyecto grupal?
  - En esta actividad se propondrán uno o varios proyectos o problemas que se desarrollarán a lo largo del curso.
  - Se realizará por grupos creados al comienzo del curso y que se mantendrán fijos a lo largo del semestre.
  - Se deberá realizar una presentación, por todos los miembros del grupo, del trabajo realizado en la fecha planificada para tal efecto.
- ¿Qué tenemos que hacer?
  - Para cada problema/proyecto se creará un recurso online en el Campus Virtual de la asignatura en el que estarán descritas las instrucciones para la realización de este. En dicho recurso, habrá que entregar, tanto en plazo como en forma, la resolución del problema/proyecto planteado. Solamente deberá entregarse una copia del informe por cada grupo de trabajo. Las entregas fuera de plazo serán penalizadas pudiendo tener una calificación de 0 puntos
- Tipo de actividad: Grupal / Colaborativa
- Tipo de evaluación: Formativa (profesor) / Autoevaluación
- Peso: 20%
- ¿Cómo se evalúa?: Se evalúa según la rúbrica disponible en el Campus Virtual y que se muestra en la tabla a continuación. El docente podrá solicitar un acta de las reuniones de trabajo mantenidas por cada grupo con el fin de evaluar de forma individual a sus miembros.

Prueba integradora de conocimiento:

ACTIVIDAD: Prueba integradora de conocimiento

• ¿Qué es la actividad de prueba de evaluación?
  • La prueba de conocimiento intermedia es una prueba de conocimiento que engloba los problemas y contenidos vistos durante toda la asignatura.
  • Se realizará en la fecha establecidas a tal efecto.
• ¿Qué tenemos que hacer?
  • Realizar y resolver, de manera clara y argumentada, los ejercicios y cuestiones planteados durante la actividad.
• Tipo de actividad: Individual
• Tipo de evaluación: Sumativa.
• Peso: 60%
• ¿Cómo se evalúa?: Se evalúa según las puntuaciones establecidas en cada ejercicio propuesto y teniendo en cuenta los criterios establecidos en la siguiente rúbrica.

RÚBRICAS DE LAS ACTIVIDADES EVALUABLES

Actividades individuales y/o colaborativas

No realizado/ inadecuado	Poco adecuado	Adecuado	Muy adecuado

Justificación de la metodología seleccionada	No entrega la actividad o entrega una actividad que no atiende a las pautas marcadas.	Apenas hay justificación ni reflexión sobre la metodología seleccionada.	Justifica la metodología y los pasos realizados, aunque no es adecuada en algunos puntos.	Justifica valiéndose de referencias y utiliza una metodología adecuada.
Resolución precisa y clara	No entrega la actividad o entrega una actividad que no atiende a las pautas marcadas.	Falta de pasos de resolución necesarios o estos son inexistentes.	Se realizan los pasos de resolución necesarios, pero existen pequeñas inconsistencias o errores.	Resolución precisa con justificación y claridad de todos los pasos del desarrollo.
Resultado final correcto	No proporciona resultado alguno.	El resultado final no se aproxima al resultado esperado.	El resultado final, aunque no es el resultado esperado, se aproxima.	Resultado final correcto.

Proyecto grupal:

	No realizado/ inadecuado	**Poco adecuado**	**Adecuado**	**Muy adecuado**
Resolución precisa y clara	No entrega la actividad o entrega una actividad que no atiende a las pautas marcadas.	Falta de pasos de resolución necesarios o estos son inexistentes.	Se realizan los pasos de resolución necesarios, pero existen pequeñas inconsistencias	Resolución precisa con justificación y claridad de todos los pasos del desarrollo.
Resultado final correcto	No entrega la actividad o entrega una actividad que no atiende a las pautas marcadas.	El resultado final no se aproxima al resultado esperado.	El resultado final, aunque no es el resultado esperado, se aproxima o es correcto parcialmente.	Resultado final correcto.

Responsabilidad y Planificación	No realiza las entregas en los plazos acordados			Realiza las entregas en los plazos acordados
Habilidades de comunicación (Lenguaje simbólico)	El lenguaje utilizado es incorrecto	Tiene bastantes errores en el uso del lenguaje simbólico	Existen algunos errores menores en el uso del lenguaje simbólico	El uso del lenguaje simbólico es correcto en toda la actividad
Habilidades de comunicación (presentación de resultados)	El contenido carece de claridad y enfoque. La presentación es confusa.	Parte del contenido carece de claridad. La presentación no es adecuada.	Existen momentos o aspectos puntuales poco claros, pero en general la presentación es adecuada.	Todo el contenido está claro y bien enfocado. La presentación es concisa, visualmente atractiva.

Pruebas de conocimiento:

	No realizado/ inadecuado	**Poco adecuado**	**Adecuado**	**Muy adecuado**
Justificación de la metodología seleccionada	No entrega la actividad o entrega una actividad que no atiende a las pautas marcadas.	Apenas hay justificación ni reflexión sobre la metodología seleccionada.	Justifica la metodología y los pasos realizados, aunque no es adecuada en algunos puntos.	Justifica valiéndose de referencias y utiliza una metodología adecuada.
Resolución precisa y clara	No entrega la actividad o entrega una actividad que no atiende a las pautas marcadas.	Falta de pasos de resolución necesarios o estos son inexistentes.	Se realizan los pasos de resolución necesarios, pero existen pequeñas inconsistencias o errores.	Resolución precisa con justificación y claridad de todos los pasos del desarrollo.

Resultado final correcto	No proporciona resultado alguno.	El resultado final no se aproxima al resultado esperado.	El resultado final, aunque no es el resultado esperado, se aproxima.	Resultado final correcto.

REGLAMENTO PLAGIO

Atendiendo al Reglamento disciplinario de los estudiantes de la Universidad Europea:

- El plagio, en todo o en parte, de obras intelectuales de cualquier tipo se considera falta muy grave.
- Las faltas muy graves relativas a plagios y al uso de medios fraudulentos para superar las pruebas de evaluación, tendrán como consecuencia la pérdida de la convocatoria correspondiente, así como el reflejo de la falta y su motivo, en el expediente académico.

REGLAMENTO USO DE IA

El estudiante debe ser el autor o autora de sus trabajos/actividades.

El uso de herramientas de Inteligencia Artificial (IA) debe ser autorizado por el docente en cada trabajo/actividad, indicando de qué manera está permitido su uso. El docente informará previamente en qué situaciones se podrá usar herramientas de IA para mejorar la ortografía, gramática y edición en general. El estudiante es responsable de precisar la información dada por la herramienta y declarar debidamente el uso de cualquier herramienta de IA, en función de las directrices que marque el docente. La decisión final sobre la autoría del trabajo y la idoneidad del uso reportado de una herramienta de IA recae en el docente y en los responsables de la titulación.