

GUÍA DOCENTE CRIPTOGRAFIA

GRADO EN INGENIERÍA DE LA CIBERSEGURIDAD

CURSO 2026-27

Fecha de publicación: 07-07-2026



I.-Identificación de la Asignatura	
Tipo	OBLIGATORIA
Período de impartición	1 curso, 2Q semestre
Nº de créditos	6
Idioma en el que se imparte	Castellano

II.-Presentación
La criptología, ciencia y arte de la gestión segura de la información, estudia las técnicas que permiten transmitir, almacenar, manipular y distribuir datos con determinadas garantías de seguridad, incluso en entornos hostiles. Esta disciplina tiene dos vertientes estrechamente relacionadas. La primera, de carácter constructivo, se denomina criptografía y se ocupa del diseño de herramientas, mecanismos y protocolos criptográficos. La segunda, de carácter analítico, se denomina criptanálisis o criptoanálisis, y se centra en estudiar los esquemas criptográficos para identificar posibles vulnerabilidades. Ambas vertientes se retroalimentan y resultan imprescindibles para la evolución constante de las construcciones utilizadas en la práctica, anticipando con frecuencia la solución de problemas de seguridad antes de que su impacto práctico sea evidente. Esta asignatura ofrece una introducción a la criptografía desde una perspectiva moderna y formal. Su objetivo es que el estudiantado conozca las principales construcciones criptográficas, sea capaz de analizar si una implementación concreta se ajusta a la descripción formal de un diseño, y comprenda la terminología utilizada para definir y demostrar matemáticamente los distintos niveles de seguridad asociados a los mecanismos criptográficos más extendidos en la práctica.
II.B-Presentación en inglés
null

III.-Resultados de Aprendizaje



CG4. Capacidad para dirigir y liderar las actividades objeto de los proyectos del ámbito de la informática y la ciberseguridad comprendiendo los criterios de calidad que rigen dichas actividades investigadora y profesional.

CG7. Capacidad para evaluar y asegurar la confidencialidad, integridad y disponibilidad de los activos tecnológicos.

CG8. Capacidad para definir, evaluar y seleccionar contramedidas para la protección de los activos tecnológicos, entendiendo las peculiaridades de los distintos contextos en los que deben desplegarse.

CG11. Conocimiento para la realización de mediciones, cálculos, valoraciones, tasaciones, peritaciones, estudios, informes, planificación de tareas y otros trabajos análogos.

CG13. Capacidad para concebir, desarrollar, implantar y mantener sistemas, servicios y aplicaciones informáticas empleando los métodos de la ingeniería como instrumento para el aseguramiento de su calidad.

CG14. Conocimiento y comprensión de un área de estudio que parte de la base de la educación secundaria general y se suele encontrar a un nivel que, si bien se apoya en libros de texto avanzados, incluye también algunos aspectos que implican conocimientos procedentes de la vanguardia de su campo de estudio.

CG16. Capacidad de reunir e interpretar datos relevantes (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética.

CE19. Comprender los algoritmos criptográficos de clave pública y de clave privada más importantes y conocer sus aplicaciones en ciberseguridad.

CE24. Diseñar, desplegar, configurar y gestionar soluciones que protejan los datos almacenados y en tránsito (las comunicaciones).

CE25. Diseñar, desplegar, configurar y gestionar mecanismos adecuados para la gestión de identidades digitales (identificación, autenticación, autorización y auditoría o IAAA)

- Leyenda para las titulaciones no adaptadas al RD 822/21: **CB** - competencias básicas, **CG** - competencias generales, **CE** - competencias específicas, **CT** - competencias transversales.
- Leyenda para las titulaciones adaptadas al RD 822/21: **CON** - conocimientos, **COM** - competencias, **HAB** - habilidades.



IV.-Contenido

IV.A.-Temario de la asignatura

BLOQUE I.

TEMA 1. NOCIONES ELEMENTALES

- 1.1. Introducción a la criptografía.
- 1.2. Fundamentos de seguridad demostrable.

TEMA 2. CRIPTOGRAFÍA SIMÉTRICA

- 2.1. Criptografía clásica.
- 2.2. Cifrado simétrico.
- 2.3. Funciones Hash. MACs.

BLOQUE II

TEMA 3. CRIPTOGRAFÍA ASIMÉTRICA

- 3.1. Cifrado asimétrico
- 3.2. Intercambio de clave.
- 3.3. Firma digital.

TEMA 4. CRIPTOGRAFÍA AVANZADA

- 4.1. Esquemas de compromiso.
- 4.2. Compartición de secretos.

IV.B.-Actividades formativas

Tipo	Descripción
Otras actividades	Seminarios y charlas abiertos a la asistencia de alumnos que quieran profundizar en distintos temas relacionados con la materia impartida.



V.-Tiempo de trabajo del alumnado (30h grado y 25h máster)

Clases teóricas	25
Clases de resolución de ejercicios, problemas, casos, etc.	20
Prácticas en laboratorios experimentales, tecnológicos, clínicos, campo, etc.	10
Realización de pruebas	5
Tutorías académicas	14
Actividades relacionadas: jornadas, seminarios, etc.	4
Preparación de clases teóricas	36
Preparación de prácticas/ejercicios/casos	36
Preparación de pruebas	30
Total de horas de trabajo del alumnado	180

VI.-Metodología y plan de trabajo

Tipo	Periodo	Contenido
Tutorías académicas	Semana 1 a Semana 15	Se plantearán diversas reuniones en grupos reducidos para resolución de dudas e intercambio de ideas. Podrán ser realizadas presencialmente o a través de la herramienta de comunicación Teams.
Prácticas	Semana 1 a Semana 15	Clases de ejercicios (sin ordenador), repartidas en 5 sesiones específicas (10 horas) y otras no anunciadas en las que, en función del ritmo de la clase, se expondrán y resolverán problemas en común con el fin de facilitar la asimilación de los contenidos impartidos.
Pruebas	Semana 8 a Semana 8	Primer Parcial de la asignatura (P1)
Pruebas	Semana 13 a Semana 13	Segundo Parcial de la asignatura (P2)
Clases Teóricas	Semana 1 a Semana 15	Clases magistrales, en las que se presentarán los contenidos del temario de la asignatura con numerosos ejemplos. Se fomentará en todo momento la participación de los alumnos.



VII.-Método de evaluación

El modelo de evaluación general es la evaluación continua, tal como establece el Reglamento de evaluación de los resultados de aprendizaje de la Universidad Rey Juan Carlos.

Deberán utilizarse todos los sistemas de evaluación establecidos para la asignatura en la memoria de la titulación, excepto aquellos que tuviesen una ponderación mínima del 0%, que podrán utilizarse en los cursos académicos en los que el profesorado lo considere oportuno. Cada uno de los sistemas de evaluación podrá ser aplicado mediante una o más actividades de evaluación, coherentes con ese sistema. Ninguna de las actividades de evaluación podrá superar individualmente el 60% de la calificación global de la asignatura.

La suma de las actividades de evaluación no revaluables no podrá superar el 40% de la calificación global de la asignatura y, en general, no deberían tener nota mínima (salvo en el caso de actividades de carácter práctico en las que, estrictamente, no pudieran reproducirse en la convocatoria extraordinaria las condiciones de evaluación de la convocatoria ordinaria).

El alumnado que no consiga superar la asignatura en la convocatoria ordinaria, o no se hayan presentado, podrán presentarse a la convocatoria extraordinaria únicamente a las actividades de evaluación revaluables no superadas.

El uso de herramientas basadas en inteligencia artificial está prohibido en cualquier ejercicio y prueba de evaluación de la asignatura salvo que el profesor lo indique de forma explícita en el enunciado o en el material de esta. En caso de que esté permitido, se darán indicaciones precisas de qué usos están permitidos y cuáles no.

La distribución y características de las actividades de evaluación son las que se describen a continuación.

VII.A.- Descripción de las actividades de evaluación y su ponderación

Sistema de evaluación	Revaluable en convocatoria extraordinaria	Ponderación	Actividad de evaluación	Nota mínima	Contenidos	Fecha
SE1 - Prueba escrita de respuesta abierta o tipo test.	Sí. Las pruebas seguirán el mismo formato que en la convocatoria ordinaria.	80%	Parcial 1 (P1): 40%	$P1 + T1 \geq 2$ puntos sobre 5.	Bloque I	Semana 8
			Parcial 2 (P2): 40%	$P2 + T2 \geq 2$ puntos sobre 5.	Bloque II	Fecha oficial del examen de la convocatoria ordinaria.
SE2 - Resolución de problemas y casos prácticos.	Sí. Se revalorará mediante la prueba extraordinaria del bloque correspondiente.	20%	Test 1 (T1): 10%	$P1 + T1 \geq 2$ puntos sobre 5.	Bloque I	Semana 8
			Test 2 (T2): 10%	$P2 + T2 \geq 2$ puntos sobre 5.	Bloque II	Semana 15

Cálculo de la nota final

La asignatura se evaluará mediante evaluación continua. Durante el curso se realizarán cuatro pruebas, dos asociadas al bloque I y dos asociadas al bloque II:

- **Test 1 (T1):** prueba de teoría y cuestiones cortas sobre el bloque I. Representa el 10% de la nota final. Se realizará en torno a la semana 8 del curso. La calificación T1 será un valor entre 0 y 1.
- **Test 2 (T2):** prueba de teoría y cuestiones cortas sobre el bloque II. Representa el 10% de la nota final. Se realizará en la última semana con clases. La calificación T2 será un valor entre 0 y 1.
- **Parcial 1 (P1):** prueba escrita con ejercicios y problemas teórico-prácticos sobre el bloque I. Representa el 40% de la nota final. Se realizará en torno a la semana 8 del curso. La calificación P1 será un valor entre 0 y 4.
- **Parcial 2 (P2):** prueba escrita con ejercicios y problemas teórico-prácticos sobre el bloque II. Representa el 40% de la nota final. Se realizará en el periodo de exámenes de la convocatoria ordinaria. La calificación P2 será un valor entre 0 y 4.

Las pruebas T1 y T2 se realizarán online a través del Aula Virtual, bien en el aula y horario de clase o bien en remoto, en función de la disponibilidad. Tendrán una duración aproximada de 45 minutos. Las pruebas P1 y P2 serán presenciales y tendrán una duración aproximada de 90 minutos. Todas las actividades de evaluación son revaluables en la convocatoria extraordinaria.

Para aprobar la asignatura en la convocatoria ordinaria será necesario cumplir simultáneamente las siguientes condiciones:

- **Bloque I:** $P1 + T1$ deberá ser al menos 2 puntos sobre 5. Si no se alcanza esta nota mínima, el bloque I deberá reevaluarse en la convocatoria extraordinaria.
- **Bloque II:** $P2 + T2$ deberá ser al menos 2 puntos sobre 5. Si no se alcanza esta nota mínima, el bloque II deberá reevaluarse en la convocatoria extraordinaria.
- **Nota final:** $P1 + P2 + T1 + T2$ deberá ser al menos 5 puntos sobre 10.

Si se cumplen las tres condiciones anteriores, la asignatura se considerará aprobada.

Convocatoria extraordinaria

En la convocatoria extraordinaria solo podrán reevaluarse las actividades que no hayan alcanzado la nota mínima establecida en la convocatoria ordinaria. Si un estudiante hubiese superado la nota mínima en todos los bloques y, aun así, su calificación global no fuese suficiente para aprobar la asignatura, podrá reevaluarse excepcionalmente de una o de las dos pruebas extraordinarias correspondientes a los bloques en los que hubiese obtenido una calificación inferior a 5 puntos sobre 5. Los estudiantes que no hayan aprobado en la convocatoria ordinaria podrán realizar una o dos de las siguientes pruebas durante el periodo de exámenes de la convocatoria extraordinaria:

- **Prueba extraordinaria 1 (F1):** teoría, ejercicios y problemas sobre el bloque I. Representa el 50% de la nota final y revalúa los



contenidos del bloque I. Será obligatoria si $P1 + T1 < 2$ y optativa en los casos en que proceda según lo indicado anteriormente. La calificación F1 será un valor entre 0 y 5 y sustituirá a la nota asociada al bloque I, es decir, a $P1 + T1$. Si no se realiza, se mantendrá la calificación obtenida en la convocatoria ordinaria.

•**Prueba extraordinaria 2 (F2):** teoría, ejercicios y problemas sobre el bloque II. Representa el 50% de la nota final y revalúa los contenidos del bloque II. Será obligatoria si $P2 + T2 < 2$ y optativa en los casos en que proceda según lo indicado anteriormente. La calificación F2 será un valor entre 0 y 5 y sustituirá a la nota asociada al bloque II, es decir, a $P2 + T2$. Si no se realiza, se mantendrá la calificación obtenida en la convocatoria ordinaria.

Las pruebas extraordinarias se realizarán de manera presencial. Cada prueba tendrá una duración aproximada de 90 minutos. Para aprobar la asignatura en la convocatoria extraordinaria será necesario cumplir simultáneamente las siguientes condiciones:

- Bloque I:** la calificación asociada al bloque I deberá ser al menos 2 puntos sobre 5.
 - Bloque II:** la calificación asociada al bloque II deberá ser al menos 2 puntos sobre 5.
 - Nota final:** la suma de las calificaciones asociadas al bloque I y al bloque II deberá ser al menos 5 puntos sobre 10.
- Si se cumplen las tres condiciones anteriores, la asignatura se considerará aprobada.

VII.B.- Evaluación del alumnado con dispensa académica de asistencia a clase

La concesión de Dispensa Académica de Asistencia a Clase (DAAC) no implica que se quede automáticamente eximido de participar en las actividades de evaluación continua ni en las actividades formativas presenciales de asistencia obligatoria establecidas en la guía docente. Una vez concedida la dispensa, el alumnado deberá contactar con el docente, que podría proponerle las adaptaciones que considere convenientes, siempre que garanticen la adquisición y adecuada evaluación de los resultados de aprendizaje previstos. El alumnado deberá mantener a lo largo de curso una comunicación fluida con el docente para que este le proporcione información sobre las fechas en que se realizarán esas actividades formativas y de evaluación, en caso de que su programación no estuviese ya fijada y a disposición del alumnado en el momento de la concesión de la dispensa.

Asignatura con posibilidad de dispensa: Sí

VII.C.- Revisión y reclamación de las actividades de evaluación

Se realizará conforme al Reglamento de evaluación de los resultados de aprendizaje de la Universidad Rey Juan Carlos.

VII.D.- Alumnado con discapacidad o necesidades educativas especiales

Con el fin de garantizar la igualdad de oportunidades, la no discriminación, la accesibilidad universal y la mayor garantía de éxito académico, las adaptaciones curriculares para alumnado con discapacidad o con necesidades educativas especiales serán pautadas por la Unidad de Atención a Personas con Discapacidad, de acuerdo con la normativa que regula el servicio de Atención a Estudiantes con Discapacidad, aprobada por Consejo de Gobierno de la Universidad Rey Juan Carlos.

Para que esas adaptaciones puedan realizarse, será requisito la emisión de un informe de adaptaciones curriculares por parte de dicha Unidad, por lo que el alumnado con discapacidad o necesidades educativas especiales deberán contactar con este servicio para analizar conjuntamente las distintas opciones.

VII.E.- Conducta académica, integridad y honestidad académica

La Universidad Rey Juan Carlos está plenamente comprometida con los más altos estándares de integridad y honestidad académica, por lo que estudiar en la URJC supone asumir y suscribir los valores de integridad y la honestidad académica recogidos en el Código Ético de la Universidad.

Para acompañar este proceso, la Universidad dispone de la Normativa de Convivencia de la Universidad Rey Juan Carlos y de diferentes herramientas (antiplagio, supervisión) que ofrecen una garantía colectiva para el completo desarrollo de estos valores esenciales.

Las herramientas basadas en inteligencia artificial pueden mejorar la experiencia de aprendizaje, pero debe utilizarse de forma ética, legal, honesta y transparente. Por este motivo, deben seguirse las recomendaciones de uso adecuado indicadas por los docentes de la asignatura.



VIII.-Recursos y materiales didácticos

Bibliografía básica

1. **Cryptography: an Introduction**, Nigel Smart. Disponible gratuitamente on-line: <https://www.cs.umd.edu/~waa/414-F11/IntroToCrypto.pdf>
2. **Criptografía Esencial. Principios básicos para el diseño de esquemas y protocolos seguros**. M.I. González Vasco, A. Pérez del Pozo, Ed. RAMA; 2021.
3. **Introduction to Modern Cryptography**, Jonathan Katz, Yehuda Lindell. Chapman and Hall/CRC, Cryptography and Network Security Series, 2014.

Bibliografía complementaria

1. **A Classical Introduction to Cryptography**, Serge Vaudenay, Springer. 2006
2. **Cryptography Made Simple**, Nigel P. Smart. Information Security and Cryptography Series, Springer International Publishing, 2016.

IX.-Profesorado

Nombre y apellidos	ÁNGEL LUIS PÉREZ DEL POZO
Correo electrónico	angel.perez@urjc.es
Departamento	Matemática Aplicada, Ciencia e Ingeniería de los Materiales y Tecnología Electrónica
Campus de impartición	Móstoles
Categoría	Titular de Universidad
Titulación académica	Doctor
Responsable de asignatura	No
Horario de tutorías	Para consultar las tutorías póngase en contacto con el/la profesor/a a través de correo electrónico
Nº de Quinquenios	3
Nº de Sexenios	2
Nº de Sexenios de transferencia	0
Nº de evaluaciones positivas Docencia	3
Nombre y apellidos	MISAELE ENRIQUE MARRIAGA CASTILLO
Correo electrónico	misael.marriaga@urjc.es
Departamento	Matemática Aplicada, Ciencia e Ingeniería de los Materiales y Tecnología Electrónica
Campus de impartición	Móstoles



Categoría	Titular de Universidad
Titulación académica	Doctor
Responsable de asignatura	Si
Horario de tutorías	Para consultar las tutorías póngase en contacto con el/la profesor/a a través de correo electrónico
Nº de Quinquenios	2
Nº de Sexenios	1
Nº de Sexenios de transferencia	0
Nº de evaluaciones positivas Docencia	2