Guía docente
270131 - C - Criptografía

Última modificación: 11/07/2025

Unidad responsable: Facultad de Informática de Barcelona
Unidad que imparte: 749 - MAT - Departamento de Matemáticas.

Titulación: GRADO EN INGENIERÍA INFORMÁTICA (Plan 2010). (Asignatura optativa).

Curso: 2025 **Créditos ECTS:** 6.0 **Idiomas:** Castellano

PROFESORADO

Profesorado responsable: FERNANDO MARTÍNEZ SÁEZ

Otros: Primer quadrimestre:
FERNANDO MARTÍNEZ SÁEZ - 11, 12

COMPETENCIAS DE LA TITULACIÓN A LAS QUE CONTRIBUYE LA ASIGNATURA

Específicas:
CEC4.2. Demostrar comprensión, aplicar y gestionar la garantía y la seguridad de los sistemas informáticos.
CT1.2A. Demostrar conocimiento y comprensión de los conceptos fundamentales de la programación y de la estructura básica de un computador. CEFB5. Conocimiento de la estructura, funcionamiento e interconexión de los sistemas informáticos, así como los fundamentos de su programación.
CT1.2C. Interpretar, seleccionar y valorar conceptos, teorías, usos y desarrollos tecnológicos relacionados con la informática y su aplicación a partir de los fundamentos matemáticos, estadísticos y físicos necesarios. CEFB1: Capacidad para la resolución de los problemas matemáticos que puedan plantarse en la ingeniería. Aptitud para aplicar los conocimientos sobre: algebra, cálculo diferencial e integral i métodos numéricos; estadística y optimización.
CTI2.3. Demostrar comprensión, aplicar y gestionar la garantía y la seguridad de los sistemas informáticos (CEIC6).
CTI3.1. Concebir sistemas, aplicaciones y servicios basados en tecnologías de red, incluyendo Internet, web, comercio electrónico, multimedia, servicios interactivos y computación ubicua.

Genéricas:
G3. TERCERA LENGUA: Conocer el idioma inglés con un nivel adecuado de forma oral y por escrito, y con consonancia con las necesidades que tendrán los graduados y graduadas en ingeniería informática. Capacidad de trabajar en un grupo multidisciplinar y en un entorno multilingüe, y de comunicar, tanto por escrito como de forma oral, conocimientos, procedimientos, resultados e ideas relacionadas con la profesión de ingeniero técnico en informática.
G9. RAZONAMIENTO: Capacidad de razonamiento crítico, lógico y matemático. Capacidad para resolver problemas dentro de su área de estudio. Capacidad de abstracción: capacidad de crear y utilizar modelos que reflejen situaciones reales. Capacidad de diseñar y realizar experimentos sencillos, y analizar e interpretar sus resultados. Capacidad de análisis, síntesis y evaluación.

METODOLOGÍAS DOCENTES

Clases teóricas en las que se expondrán los contenidos de la materia y clases prácticas en las que se familiarizarán con los aspectos prácticos de la materia

OBJETIVOS DE APRENDIZAJE DE LA ASIGNATURA

1.Discernir entre criptosistemas que podrían ser seguros de aquellos que no son más que palabrería.
2.Diferenciar entre criptografía de clave secreta y clave pública.
3.Estudiar las ideas básicas en las que se basa la criptografía de clave secreta.
4.Estudiar las ideas básicas en las que se basa la criptografía de clave pública
5.Entender el concepto firma digital y su importancia en las comunicaciones

HORAS TOTALES DE DEDICACIÓN DEL ESTUDIANTADO

Tipo	Horas	Porcentaje
Horas actividades dirigidas	6,0	3.85
Horas grupo grande	30,0	19.23
Horas aprendizaje autónomo	90,0	57.69
Horas grupo pequeño	30,0	19.23

Dedicación total: 156 h

CONTENIDOS

Conceptos básicos

Descripción:
Criptología, Criptografía y Criptoanálisis.
Criptología clásica y criptología moderna.
Técnicas básicas: cifrado-descifrado y firma.
Criptología de clave privada y de clave pública.
Bases matemáticas de la criptología.

Técnicas modernas de clave secreta

Descripción:
Cifrado en bloque y cifrado en flujo.
Data Encryption Standard: Descripción, Historia, Estandarización, Criptoanálisis.
Advanced Encryption Standard: Descripción, Estandarización.
Modos de operación para sistemas de cifrado en bloque.

Criptosistemas de clave pública

Descripción:
Operaciones aritméticas multi-precisión. Algoritmo de Euclides.- Congruencias, grupo multiplicativo, aritmética modular, exponenciación modular, teorema chino.
Cálculo de raíces cuadradas.
Números primos, criterios de primalidad probabilísticos, generación aleatoria de números primos.
Factorización de números enteros, estado actual del problema y perspectivas.
El problema del logaritmo discreto: variantes sobre cuerpos finitos y curvas elípticas.
Criptosistema RSA (Rivest, Shamir, Adleman).
Criptosistema de ElGamal.
Sistema de Diffie-Hellman para la distribución de claves.

Firmas digitales

Descripción:
Funciones hash criptográficas. Secure Hash Standard.
Firmas digitales: RSA, DSA y ECDSA
PKI: certificados digitales X509, CRL y OCSP.

Protocolos criptográficos y estándares

Descripción:
Transformaciones de cifrado y descifrado.Técnicas mixtas clave privada-clave pública.
Esquemas y protocolos de indentificación.
SSL.
Micropagos.
Secretos compartidos.
Votaciones electrónicas.
Watermarks.
SMIME.
PKCS...

El futuro próximo?

Descripción:
Criptografía basada en retículos. Criptografía sobre curvas hiperelípticas. Criptografía cuàntica.

ACTIVIDADES

Conceptos básicos

Objetivos específicos:
1, 2

Competencias relacionadas:
G3. TERCERA LENGUA: Conocer el idioma inglés con un nivel adecuado de forma oral y por escrito, y con consonancia con las necesidades que tendrán los graduados y graduadas en ingeniería informática. Capacidad de trabajar en un grupo multidisciplinar y en un entorno multilingüe, y de comunicar, tanto por escrito como de forma oral, conocimientos, procedimientos, resultados e ideas relacionadas con la profesión de ingeniero técnico en informática.
G9. RAZONAMIENTO: Capacidad de razonamiento crítico, lógico y matemático. Capacidad para resolver problemas dentro de su área de estudio. Capacidad de abstracción: capacidad de crear y utilizar modelos que reflejen situaciones reales. Capacidad de diseñar y realizar experimentos sencillos, y analizar e interpretar sus resultados. Capacidad de análisis, síntesis y evaluación.

Dedicación: 6h
Aprendizaje autónomo: 2h
Grupo grande/Teoría: 2h
Grupo pequeño/Laboratorio: 2h

Criptografía de clave secreta

Objetivos específicos:
1, 2, 3

Competencias relacionadas:
G3. TERCERA LENGUA: Conocer el idioma inglés con un nivel adecuado de forma oral y por escrito, y con consonancia con las necesidades que tendrán los graduados y graduadas en ingeniería informática. Capacidad de trabajar en un grupo multidisciplinar y en un entorno multilingüe, y de comunicar, tanto por escrito como de forma oral, conocimientos, procedimientos, resultados e ideas relacionadas con la profesión de ingeniero técnico en informática.
G9. RAZONAMIENTO: Capacidad de razonamiento crítico, lógico y matemático. Capacidad para resolver problemas dentro de su área de estudio. Capacidad de abstracción: capacidad de crear y utilizar modelos que reflejen situaciones reales. Capacidad de diseñar y realizar experimentos sencillos, y analizar e interpretar sus resultados. Capacidad de análisis, síntesis y evaluación.

Dedicación: 22h
Aprendizaje autónomo: 12h
Grupo grande/Teoría: 6h
Grupo pequeño/Laboratorio: 4h

Prueba de criptografía de clave secreta

Objetivos específicos:
1, 2, 3

Competencias relacionadas:
G3. TERCERA LENGUA: Conocer el idioma inglés con un nivel adecuado de forma oral y por escrito, y con consonancia con las necesidades que tendrán los graduados y graduadas en ingeniería informática. Capacidad de trabajar en un grupo multidisciplinar y en un entorno multilingüe, y de comunicar, tanto por escrito como de forma oral, conocimientos, procedimientos, resultados e ideas relacionadas con la profesión de ingeniero técnico en informática.
G9. RAZONAMIENTO: Capacidad de razonamiento crítico, lógico y matemático. Capacidad para resolver problemas dentro de su área de estudio. Capacidad de abstracción: capacidad de crear y utilizar modelos que reflejen situaciones reales. Capacidad de diseñar y realizar experimentos sencillos, y analizar e interpretar sus resultados. Capacidad de análisis, síntesis y evaluación.

Dedicación: 1h
Actividades dirigidas: 1h

Criptografía de clave pública

Objetivos específicos:
1, 2, 4

Competencias relacionadas:
G3. TERCERA LENGUA: Conocer el idioma inglés con un nivel adecuado de forma oral y por escrito, y con consonancia con las necesidades que tendrán los graduados y graduadas en ingeniería informática. Capacidad de trabajar en un grupo multidisciplinar y en un entorno multilingüe, y de comunicar, tanto por escrito como de forma oral, conocimientos, procedimientos, resultados e ideas relacionadas con la profesión de ingeniero técnico en informática.
G9. RAZONAMIENTO: Capacidad de razonamiento crítico, lógico y matemático. Capacidad para resolver problemas dentro de su área de estudio. Capacidad de abstracción: capacidad de crear y utilizar modelos que reflejen situaciones reales. Capacidad de diseñar y realizar experimentos sencillos, y analizar e interpretar sus resultados. Capacidad de análisis, síntesis y evaluación.

Dedicación: 50h
Aprendizaje autónomo: 30h
Grupo grande/Teoría: 12h
Grupo pequeño/Laboratorio: 8h

Firma digital

Objetivos específicos:
5

Competencias relacionadas:
G3. TERCERA LENGUA: Conocer el idioma inglés con un nivel adecuado de forma oral y por escrito, y con consonancia con las necesidades que tendrán los graduados y graduadas en ingeniería informática. Capacidad de trabajar en un grupo multidisciplinar y en un entorno multilingüe, y de comunicar, tanto por escrito como de forma oral, conocimientos, procedimientos, resultados e ideas relacionadas con la profesión de ingeniero técnico en informática.
G9. RAZONAMIENTO: Capacidad de razonamiento crítico, lógico y matemático. Capacidad para resolver problemas dentro de su área de estudio. Capacidad de abstracción: capacidad de crear y utilizar modelos que reflejen situaciones reales. Capacidad de diseñar y realizar experimentos sencillos, y analizar e interpretar sus resultados. Capacidad de análisis, síntesis y evaluación.

Dedicación: 8h
Aprendizaje autónomo: 4h
Grupo grande/Teoría: 4h

Protocolos y estándares criptográficos

Objetivos específicos:
1

Competencias relacionadas:
G3. TERCERA LENGUA: Conocer el idioma inglés con un nivel adecuado de forma oral y por escrito, y con consonancia con las necesidades que tendrán los graduados y graduadas en ingeniería informática. Capacidad de trabajar en un grupo multidisciplinar y en un entorno multilingüe, y de comunicar, tanto por escrito como de forma oral, conocimientos, procedimientos, resultados e ideas relacionadas con la profesión de ingeniero técnico en informática.
G9. RAZONAMIENTO: Capacidad de razonamiento crítico, lógico y matemático. Capacidad para resolver problemas dentro de su área de estudio. Capacidad de abstracción: capacidad de crear y utilizar modelos que reflejen situaciones reales. Capacidad de diseñar y realizar experimentos sencillos, y analizar e interpretar sus resultados. Capacidad de análisis, síntesis y evaluación.

Dedicación: 19h
Aprendizaje autónomo: 16h
Grupo grande/Teoría: 3h

Prueba de criptografía de clave pública

Objetivos específicos:
1, 2, 4, 5

Competencias relacionadas:
G3. TERCERA LENGUA: Conocer el idioma inglés con un nivel adecuado de forma oral y por escrito, y con consonancia con las necesidades que tendrán los graduados y graduadas en ingeniería informática. Capacidad de trabajar en un grupo multidisciplinar y en un entorno multilingüe, y de comunicar, tanto por escrito como de forma oral, conocimientos, procedimientos, resultados e ideas relacionadas con la profesión de ingeniero técnico en informática.
G9. RAZONAMIENTO: Capacidad de razonamiento crítico, lógico y matemático. Capacidad para resolver problemas dentro de su área de estudio. Capacidad de abstracción: capacidad de crear y utilizar modelos que reflejen situaciones reales. Capacidad de diseñar y realizar experimentos sencillos, y analizar e interpretar sus resultados. Capacidad de análisis, síntesis y evaluación.

Dedicación: 1h
Actividades dirigidas: 1h

Criptografía del futuro

Objetivos específicos:
1, 2

Competencias relacionadas:
G3. TERCERA LENGUA: Conocer el idioma inglés con un nivel adecuado de forma oral y por escrito, y con consonancia con las necesidades que tendrán los graduados y graduadas en ingeniería informática. Capacidad de trabajar en un grupo multidisciplinar y en un entorno multilingüe, y de comunicar, tanto por escrito como de forma oral, conocimientos, procedimientos, resultados e ideas relacionadas con la profesión de ingeniero técnico en informática.
G9. RAZONAMIENTO: Capacidad de razonamiento crítico, lógico y matemático. Capacidad para resolver problemas dentro de su área de estudio. Capacidad de abstracción: capacidad de crear y utilizar modelos que reflejen situaciones reales. Capacidad de diseñar y realizar experimentos sencillos, y analizar e interpretar sus resultados. Capacidad de análisis, síntesis y evaluación.

Dedicación: 5h
Aprendizaje autónomo: 4h
Grupo grande/Teoría: 1h

DNI electrónico

Objetivos específicos:
2, 5

Competencias relacionadas:
G3. TERCERA LENGUA: Conocer el idioma inglés con un nivel adecuado de forma oral y por escrito, y con consonancia con las necesidades que tendrán los graduados y graduadas en ingeniería informática. Capacidad de trabajar en un grupo multidisciplinar y en un entorno multilingüe, y de comunicar, tanto por escrito como de forma oral, conocimientos, procedimientos, resultados e ideas relacionadas con la profesión de ingeniero técnico en informática.
G9. RAZONAMIENTO: Capacidad de razonamiento crítico, lógico y matemático. Capacidad para resolver problemas dentro de su área de estudio. Capacidad de abstracción: capacidad de crear y utilizar modelos que reflejen situaciones reales. Capacidad de diseñar y realizar experimentos sencillos, y analizar e interpretar sus resultados. Capacidad de análisis, síntesis y evaluación.

Dedicación: 2h
Aprendizaje autónomo: 1h
Grupo pequeño/Laboratorio: 1h

Correo seguro

Objetivos específicos:
1, 2, 3, 4, 5

Competencias relacionadas:
G3. TERCERA LENGUA: Conocer el idioma inglés con un nivel adecuado de forma oral y por escrito, y con consonancia con las necesidades que tendrán los graduados y graduadas en ingeniería informática. Capacidad de trabajar en un grupo multidisciplinar y en un entorno multilingüe, y de comunicar, tanto por escrito como de forma oral, conocimientos, procedimientos, resultados e ideas relacionadas con la profesión de ingeniero técnico en informática.
G9. RAZONAMIENTO: Capacidad de razonamiento crítico, lógico y matemático. Capacidad para resolver problemas dentro de su área de estudio. Capacidad de abstracción: capacidad de crear y utilizar modelos que reflejen situaciones reales. Capacidad de diseñar y realizar experimentos sencillos, y analizar e interpretar sus resultados. Capacidad de análisis, síntesis y evaluación.

Dedicación: 3h
Aprendizaje autónomo: 1h
Grupo pequeño/Laboratorio: 2h

Funciones hash

Objetivos específicos:
5

Competencias relacionadas:
G3. TERCERA LENGUA: Conocer el idioma inglés con un nivel adecuado de forma oral y por escrito, y con consonancia con las necesidades que tendrán los graduados y graduadas en ingeniería informática. Capacidad de trabajar en un grupo multidisciplinar y en un entorno multilingüe, y de comunicar, tanto por escrito como de forma oral, conocimientos, procedimientos, resultados e ideas relacionadas con la profesión de ingeniero técnico en informática.
G9. RAZONAMIENTO: Capacidad de razonamiento crítico, lógico y matemático. Capacidad para resolver problemas dentro de su área de estudio. Capacidad de abstracción: capacidad de crear y utilizar modelos que reflejen situaciones reales. Capacidad de diseñar y realizar experimentos sencillos, y analizar e interpretar sus resultados. Capacidad de análisis, síntesis y evaluación.

Dedicación: 3h
Aprendizaje autónomo: 2h
Grupo pequeño/Laboratorio: 1h

AES

Objetivos específicos:
1, 2, 3

Competencias relacionadas:
G3. TERCERA LENGUA: Conocer el idioma inglés con un nivel adecuado de forma oral y por escrito, y con consonancia con las necesidades que tendrán los graduados y graduadas en ingeniería informática. Capacidad de trabajar en un grupo multidisciplinar y en un entorno multilingüe, y de comunicar, tanto por escrito como de forma oral, conocimientos, procedimientos, resultados e ideas relacionadas con la profesión de ingeniero técnico en informática.
G9. RAZONAMIENTO: Capacidad de razonamiento crítico, lógico y matemático. Capacidad para resolver problemas dentro de su área de estudio. Capacidad de abstracción: capacidad de crear y utilizar modelos que reflejen situaciones reales. Capacidad de diseñar y realizar experimentos sencillos, y analizar e interpretar sus resultados. Capacidad de análisis, síntesis y evaluación.

Dedicación: 11h
Aprendizaje autónomo: 6h
Grupo pequeño/Laboratorio: 5h

Distribución de claves y firma digital

Objetivos específicos:
2, 3, 4, 5

Competencias relacionadas:
G3. TERCERA LENGUA: Conocer el idioma inglés con un nivel adecuado de forma oral y por escrito, y con consonancia con las necesidades que tendrán los graduados y graduadas en ingeniería informática. Capacidad de trabajar en un grupo multidisciplinar y en un entorno multilingüe, y de comunicar, tanto por escrito como de forma oral, conocimientos, procedimientos, resultados e ideas relacionadas con la profesión de ingeniero técnico en informática.
G9. RAZONAMIENTO: Capacidad de razonamiento crítico, lógico y matemático. Capacidad para resolver problemas dentro de su área de estudio. Capacidad de abstracción: capacidad de crear y utilizar modelos que reflejen situaciones reales. Capacidad de diseñar y realizar experimentos sencillos, y analizar e interpretar sus resultados. Capacidad de análisis, síntesis y evaluación.

Dedicación: 10h
Aprendizaje autónomo: 6h
Grupo pequeño/Laboratorio: 4h

Sistema criptográfico

Objetivos específicos:
2, 3, 4, 5

Competencias relacionadas:
G3. TERCERA LENGUA: Conocer el idioma inglés con un nivel adecuado de forma oral y por escrito, y con consonancia con las necesidades que tendrán los graduados y graduadas en ingeniería informática. Capacidad de trabajar en un grupo multidisciplinar y en un entorno multilingüe, y de comunicar, tanto por escrito como de forma oral, conocimientos, procedimientos, resultados e ideas relacionadas con la profesión de ingeniero técnico en informática.
G9. RAZONAMIENTO: Capacidad de razonamiento crítico, lógico y matemático. Capacidad para resolver problemas dentro de su área de estudio. Capacidad de abstracción: capacidad de crear y utilizar modelos que reflejen situaciones reales. Capacidad de diseñar y realizar experimentos sencillos, y analizar e interpretar sus resultados. Capacidad de análisis, síntesis y evaluación.

Dedicación: 1h
Grupo pequeño/Laboratorio: 1h

Openssl/TLS

Objetivos específicos:
3, 4, 5

Competencias relacionadas:
G3. TERCERA LENGUA: Conocer el idioma inglés con un nivel adecuado de forma oral y por escrito, y con consonancia con las necesidades que tendrán los graduados y graduadas en ingeniería informática. Capacidad de trabajar en un grupo multidisciplinar y en un entorno multilingüe, y de comunicar, tanto por escrito como de forma oral, conocimientos, procedimientos, resultados e ideas relacionadas con la profesión de ingeniero técnico en informática.
G9. RAZONAMIENTO: Capacidad de razonamiento crítico, lógico y matemático. Capacidad para resolver problemas dentro de su área de estudio. Capacidad de abstracción: capacidad de crear y utilizar modelos que reflejen situaciones reales. Capacidad de diseñar y realizar experimentos sencillos, y analizar e interpretar sus resultados. Capacidad de análisis, síntesis y evaluación.

Dedicación: 8h
Aprendizaje autónomo: 6h
Grupo pequeño/Laboratorio: 2h

SISTEMA DE CALIFICACIÓN

Se harán dos pruebas en las que el contenido total correspondiente a criptografía de clave secreta tenga un peso del 20% de la nota final y el contenido total correspondiente a criptografía de clave pública tenga un peso del 40% de la nota final. Estas dos pruebas se podrán substituir por un examen final.

El otro 40% de la nota corresponderá al laboratorio.

BIBLIOGRAFÍA

Básica:
- Paar, C.; Pelzl, J. Understanding cryptography: a textbook for students and practitioners. Springer, 2010. ISBN 9783642041006.
- Hoffstein, J.; Pipher, J. C.; Silverman, J. H. An Introduction to mathematical cryptography. 2nd ed. Springer, 2014. ISBN 9781493917105.
- Menezes, A.J.; Van Oorschot, P.C.; Vanstone, S.A. Handbook of applied cryptography. CRC Press, 1997. ISBN 0849385237.
- van Oorschot, Paul C. Computer Security and the Internet : tools and jewels. Cham: Springer, 2020. ISBN 9783030336486.
- Mollin, R.A. RSA and public-key cryptography. Chapman & Hall/CRC, 2003. ISBN 1584883383.
- Stallings, W. Cryptography and network security: principles and practice. 8th edition Global Edition. Boston: Pearson, 2023. ISBN 9781292437484.

Complementaria:
- Anderson, R.J. Security engineering : a guide to building dependable distributed systems. 3rd ed. Indianapolis, Indiana: John Wiley & Sons, Inc., 2020. ISBN 9781119642831.
- Stinson, D.R.; Paterson, M.B. Cryptography: theory and practice. 4th ed. Chapman & Hall/CRC, 2018. ISBN 9781138197015.
- Salomaa, A. Public-key cryptography. Springer-Verlag, 1996. ISBN 9783642082542.
- Koblitz, N. A course in number theory and cryptography. 2nd e. Springer-Verlag, 1994. ISBN 0387942939.
- Blake, I. F; Seroussi, G.; Smart, N. Elliptic curves in cryptography. Cambridge University Press, 1999. ISBN 0521653746.
- Delfs, H.; Knebl, H. Introduction to cryptography: principles and applications. 2nd ed. Springer, 2007. ISBN 3540492437.
- Schneier, B. Applied cryptography: protocols, algorithms, and source code in C. 2nd ed. John Wiley & Sons, 1996. ISBN 0471117099.
- Yan, S.Y. Computational number theory and modern cryptography. Hoboken: John Wiley & Sons, 2013. ISBN 9781118188613.
- Daemen, J.; Rijmen, V. The design of Rijndael: AES the advanced encryption standard. Springer, 2001. ISBN 3540425802.
- Hankerson, D.; Menezes, A.; Vanstone, S. Guide to elliptic curve cryptography. Springer, 2004. ISBN 038795273X.
- Pastor Franco, J.; Sarasa López, M.Á.; Salazar Riaño, J.L. Criptografía digital : fundamentos y aplicaciones. 2a ed. Zaragoza: Prensas Universitarias de Zaragoza, 2001. ISBN 9788477335580.