Guía docente
330120 - SSCI - Seguridad y Secreto en la Codificación de la Información

Última modificación: 04/05/2023

Unidad responsable: Escuela Politécnica Superior de Ingeniería de Manresa
Unidad que imparte: 749 - MAT - Departamento de Matemáticas.

Titulación: GRADO EN INGENIERÍA ELECTRÓNICA INDUSTRIAL Y AUTOMÁTICA (Plan 2009). (Asignatura optativa).
GRADO EN INGENIERÍA DE SISTEMAS TIC (Plan 2010). (Asignatura optativa).
GRADO EN INGENIERÍA ELECTRÓNICA INDUSTRIAL Y AUTOMÁTICA (Plan 2016). (Asignatura optativa).

Curso: 2023 **Créditos ECTS:** 6.0 **Idiomas:** Catalán, Inglés

PROFESORADO

Profesorado responsable: MONTSERRAT ALSINA AUBACH

Otros: ENRIC VENTURA CAPELL

CAPACIDADES PREVIAS

La asignatura es adecuada para complementar los estudios en cualquier grado industrial o de ITIC, pero está especialmente indicada en aquellos relacionados con sistemas electrónicos o digitales. No utiliza matemáticas avanzadas, sólo requiere unos conocimientos de aritmética y álgebra lineal, que se revisarán y ampliarán en el tema 2.
Es necesario disponer de un nivel de comprensión oral y escrita del inglés que no interfiera negativamente en la intercomunicación en el aula.
No se requieren conocimientos técnicos de sistemas de transmisión.

COMPETENCIAS DE LA TITULACIÓN A LAS QUE CONTRIBUYE LA ASIGNATURA

Específicas:
1. Capacidad para conocer, entender y utilizar la codificación de la información para garantizar la seguridad y el secreto en los procesos de transmisión.

Transversales:
2. TERCERA LENGUA: Conocer una tercera lengua, que será preferentemente inglés, con un nivel adecuado de forma oral y por escrito y en consonancia con las necesidades que tendrán las tituladas y los titulados en cada enseñanza.

METODOLOGÍAS DOCENTES

La asignatura consta de cuatro horas de clase presencial en el aula donde se combinan la teoría y los problemas con actividades más aplicadas (resolución de ejercicios, discusión de casos prácticos, ...), invitando a los estudiantes a una participación activa.

Se utilizará el inglés como lengua vehicular en el aula, integrándola en la metodología docente. Así: se impartirán clases magistrales, clases de problemas en inglés, se consultarán recursos de información recomendados en inglés, y se redactarán entregables (ejercicios, problemas, soporte escrito de presentaciones, etc) en inglés.

Existe la posibilidad, pero no la obligación, de programar algoritmos. En este caso, el alumnado podrá utilizar el lenguaje de programación que le sea más cómodo.

OBJETIVOS DE APRENDIZAJE DE LA ASIGNATURA

Al acabar la asignatura el alumnado debe ser capaz de:

- Comprender los principios actuales básicos de la transmisión de información y la necesidad de la codificación.

- Utilizar herramientas de aritmética modular

- Enumerar y describir los principales métodos criptográficos para proteger la información y conseguir confidencialidad, integridad, autenticidad y no repudio.

- Enumerar y describir los principales códigos detectores y correctos de errores.

- Elaborar programas que implementen algunos métodos para codificar y descodificar.

En cuanto a la competencia genérica en 3 ª lengua, al acabar la asignatura al alumnado se le habrán dado recursos para ser capaz de:

- Conocer terminología técnico-científica relativa al contenido de la asignatura en inglés.
- Leer y comprender textos en inglés y material audiovisual relacionados con el contenido de la asignatura.
- Resolver problemas y ejercicios en inglés.
- Producir textos técnicos y explicar en inglés contenidos relacionados con la asignatura.
- Utilizar el inglés en la intercomunicación en el aula, en actividades escritas y/u orales.

HORAS TOTALES DE DEDICACIÓN DEL ESTUDIANTADO

Tipo	Horas	Porcentaje
Horas grupo pequeño	30,0	20.00
Horas grupo grande	30,0	20.00
Horas aprendizaje autónomo	90,0	60.00

Dedicación total: 150 h

CONTENIDOS

Título del contenido 1: INTRODUCCIÓN A LA TEORÍA DE LA INFORMACIÓN

Descripción:
Problema del ruido y la privacidad en los canales de transmisión de la información. Ejemplos y vocabulario básico.

Dedicación: 20h
Grupo grande/Teoría: 4h
Grupo mediano/Prácticas: 4h
Aprendizaje autónomo: 12h

Título del contenido 2: HERRAMIENTAS DE ARITMÉTICA MODULAR

Descripción:
Definiciones y conceptos básicos. Resultados fundamentales de utilidad en la teoría de códigos y la criptografía.

Dedicación: 20h
Grupo grande/Teoría: 4h
Grupo mediano/Prácticas: 4h
Aprendizaje autónomo: 12h

Título del contenido 3: TEORÍA DE CÓDIGOS

Descripción:
Introducción a la teoría de códigos detectores y correctores. Códigos de bloque y códigos aritméticos. Códigos lineales y códigos perfectos. Códigos de Hamming. Otros códigos y aplicaciones.

Dedicación: 60h
Grupo grande/Teoría: 12h
Grupo mediano/Prácticas: 12h
Aprendizaje autónomo: 36h

Título del contenido 4: CRIPTOGRAFÍA

Descripción:
Principios básicos de la criptografía y el criptoanálisis. Criptosistemas de clave privada. Criptosistemas de clave pública.

Dedicación: 50h
Grupo grande/Teoría: 10h
Grupo mediano/Prácticas: 10h
Aprendizaje autónomo: 30h

ACTIVIDADES

TÍTULO DE LA ACTIVIDAD 1: PRUEBA DE EVALUACIÓN CONTINUA (CONTENIDOS 1-2)

Descripción:
Prueba individual con una parte de los conceptos teóricos de la asignatura, resolución de ejercicios y problemas relacionados con los objetivos del aprendizaje.

Objetivos específicos:
Al finalizar la actividad, el alumnado debe ser capaz de:
Conocer, comprender y utilizar los principios básicos de la teoría de la información y la aritmética modular.

Material:
Enunciados, tablas y calculadora.

Entregable:
La prueba resuelta se entrega al profesor.
Su calificación se denota A1 i representa un 20% de la calificación final de la asignatura.

Dedicación: 6h
Grupo grande/Teoría: 1h 30m
Aprendizaje autónomo: 4h 30m

TÍTULO DE LA ACTIVIDAD 2: PRUEBA DE EVALUACIÓN CONTINUA (CONTENIDO 3)

Descripción:
Prueba individual con una parte de los conceptos teóricos de la asignatura, resolución de ejercicios y problemas relacionados con los objetivos del aprendizaje.

Objetivos específicos:
Al finalizar la actividad, el alumnado debe ser capaz de:
Conocer y comprender el funcionamiento de los códigos detectores y correctores de errores.

Material:
Enunciados, tablas y calculadora.

Entregable:
La prueba resuelta se entrega al profesor.
Su calificación se denota A2 i representa un 20% de la calificación final de la asignatura.

Dedicación: 6h
Grupo grande/Teoría: 1h 30m
Aprendizaje autónomo: 4h 30m

TÍTULO DE LA ACTIVIDAD 3: PRUEBA DE EVALUACIÓN CONTINUA (CONTENIDO 4)

Descripción:
Prueba individual con una parte de los conceptos teóricos de la asignatura, resolución de ejercicios y problemas relacionados con los objetivos del aprendizaje.

Objetivos específicos:
Al finalizar la actividad, la estudiante o estudiante debe ser capaz de:
Conocer y comprender el funcionamiento de los criptosistemas para cifrar y descifrar.

Material:
Enunciados, tablas y calculadora.

Entregable:
La prueba resuelta se entrega al profesor.
Su calificación se denota A3 i representa un 20% de la calificación final de la asignatura.

Dedicación: 6h
Grupo grande/Teoría: 1h 30m
Aprendizaje autónomo: 4h 30m

TÍTULO DE LA ACTIVIDAD 4: TRABAJO DE INVESTIGACIÓN (CONTENIDO 1, 2, 3 Y 4)

Descripción:
Individualmente o por parejas, fuera del aula, habrá que realizar un pequeño trabajo de investigación sobre un contenido relacionado con la asignatura. Se entregará una memoria escrita y se hará una presentación oral del trabajo.

Objetivos específicos:
Búsqueda de la información, comunicación oral, tercera lengua.

Material:
Bibliografia i internet.

Entregable:
Comunicación oral en clase con soporte multimedia.
Su calificación se denota A4 i representa un 40% de la calificación final de la asignatura.

Dedicación: 20h
Grupo grande/Teoría: 4h
Aprendizaje autónomo: 16h

TÍTULO DE LA ACTIVIDAD 5: PRUEBA FINAL (CONTENIDO 1, 2, 3 Y 4)

Descripción:
Prueba individual que muestre el logro global de los conceptos de la asignatura.

Objetivos específicos:
Evaluar el logro general de los objetivos de los contenidos 1, 2 3 y 4.

Material:

Entregable:
La prueba o trabajo se entrega al profesor.
Su calificación se denota A5 i representa un 60% de la calificación final de la asignatura.

Dedicación: 15h
Grupo grande/Teoría: 3h
Aprendizaje autónomo: 12h

TÍTULO DE LA ACTIVIDAD 6: PRUEBA DE REEVALUACIÓN (CONTENIDO 1, 2, 3 Y 4)

Descripción:
Prueba individual que muestre el logro global de los conceptos de la asignatura.
Sólo la pueden realizar los alumnos que hayan obtenido la calificación de 'suspenso' en el periodo ordinario de evaluación. No la pueden realizar aquel alumnos que tengan un 'no presentado' o ¿¿hayan aprobado la asignatura en el periodo ordinario de evaluación.

Objetivos específicos:
Reevaluar el logro general de los objetivos de los contenidos 1, 2, 3 y 4.

Entregable:
La prueba o trabajo se entrega al profesor.
Su calificación se denota A6 y se tiene en cuenta en el proceso de reevaluación.

SISTEMA DE CALIFICACIÓN

Actividad 1: A1 = 20% de la nota de la asignatura
Actividad 2: A2 = 20% de la nota de la asignatura
Actividad 3: A3 = 20% de la nota de la asignatura
Actividad 4: A4 = 40% de la nota de la asignatura
Actividad 5: A5 = 60% de la nota de la asignatura
Si un alumno no realiza alguna de las actividades, su calificación en esta actividad será 0.

El alumnado tiene opción a mejorar la calificación de las actividades (Actividad 1, 2 y 3) realizando la actividad 5 opcional.

La nota final será: NF = Max (0.2 A1 + 0.2 A2 + 0.2 A3, 0.6A5) + 0.4 A4

La evaluación del nivel alcanzado de la competencia genérica en tercera lengua efecturará siguiendo el criterio de los tres niveles que indican las parrillas de medida, A (bien logrado), B (alcanzado), C (no alcanzado), en consonancia con los criterios de evaluación que se aprueben en la EPSEM.

Proceso de reevaluación:

El alumnado que haya obtenido la calificación de 'suspenso' en el periodo ordinario de evaluación puede acceder al proceso de reevaluación, realizando la actividad 6. No pueden acceder aquellos alumnos que tengan un 'no presentado' o ¿¿hayan aprobado asignatura en el periodo ordinario de evaluación.

La nota final reevaluada de la asignatura no puede superar el 5 y se calcula:

NFR = mínimo {5, 0.4 A4 + 0.6 A6}

BIBLIOGRAFÍA

Básica:
- Brunat, J. M.; Ventura, Enric. Informació i codis [en línea]. Barcelona: Edicions UPC, 2001 [Consulta: 17/11/2020]. Disponible a: http://hdl.handle.net/2099.3/36184. ISBN 8483015285.
- Herrera, Jordi; Domingo, Josep. Criptografia per als serveis telemàtics i el comerç electrònic. Barcelona: EDIUOC, 1999. ISBN 8484290379.
- Rosen, Kenneth H. Discrete mathematics and its applications [en línea]. Global ed. Boston: McGraw Hill, 2013 [Consulta: 06/09/2023]. Disponible a: https://www-ingebook-com.recursos.biblioteca.upc.edu/ib/NPcd/IB_BooksVis?cod_primaria=1000187&codigo_libro=11905. ISBN 9780071315012.

Complementaria:
- Adámek, J. Foundations of coding: theory and applications of error-correcting codes, with an introduction to cryptography and information theory. Chichester: John Wiley & Sons, 1991. ISBN 0471621870.
- Hill, Raymond. A first course in coding theory. Oxford: Clarendon Press, 2009. ISBN 0198538030.
- Justesen, Jørn; Høholdt, Tom. A course in error-correcting codes. Zürich: European Mathematical Society, 2004. ISBN 3037190019.
- Lin, Shu. Error control coding fundamentals and applications. 2nd ed. Englewood Cliffs: Pearson Prentice-Hall, 2004. ISBN 0130179736.
- McEliece, Robert J. The theory of information and coding. Cambridge: Cambridge University Press, 2004. ISBN 0521831857.
- MacWilliams, Florence Jessie; Sloane, N. J. A. The theory of error correcting codes. Amsterdam: North-Holland, 2006. ISBN 0444851933.
- Pless, Vera. Introduction to the theory of error-correcting codes. 3rd ed. New York: John Wiley & Sons, 1998. ISBN 0471190470.
- Roman, Steven. Coding and information theory. New York: Springer-Verlag, 1992. ISBN 0387978127.
- Pretzel, Oliver. Error correcting codes and finite fields. Oxford: Clarendon Press, 1992. ISBN 0198596782.
- Xambó Descamps, Sebastián. Block error-correcting codes: a computational primer. Berlin: Springer, 2003. ISBN 3540003959.
- Stinson, D. R. Cryptography: theory and practice. 3rd ed. Boca Raton: CRC Press, 2006. ISBN 1584885084.
- Gonzalez, J.; Rio, A. Introducció a la matemàtica dels sistemes criptogràfics. Barcelona: SCM, 2000.
- Juher, David. Introducció a la criptografia. 2a ed. Girona: Servei de Publicacions de la Universitat de Girona, 2001. ISBN 8484580229.
- Juher, David. L'art de la comunicació secreta: el llenguatge de la criptografia. Barcelona: Llibres de l'Índex, 2004. ISBN 8495317710.

- Rifà Coma, Josep; Huguet Rotger, Llorenç. Comunicación digital: teoría matemática de la información, codificación algebraica, criptología. Barcelona: Masson, 1991. ISBN 8431105763.
- López García, Cándido; Fernández Veiga, Manuel. Teoría de la información y codificación [en línea]. Vigo: Universidad de Vigo, 2002 [Consulta: 03/12/2021]. Disponible a: http://www.investigo.biblioteca.uvigo.es/xmlui/bitstream/handle/11093/188/mybook.pdf?sequence=1. ISBN 8484082202.
- Munuera Gómez, Juan; Tena Ayuso, Juan. Codificación de la información. Valladolid: Universidad, Secretariado de Publicaciones e Intercambio Científico, 1997. ISBN 8477627649.
- Caballero Gil, Pino. Introducción a la criptografía. 2ª ed. Madrid: Ra-Ma, 2002. ISBN 8478975209.
- Córdoba, A. "Felipe II, el diablo y las matemáticas". Saber leer [en línea]. enero 2003, no. 161, p. 10-11 [Consulta: 17/11/2020]. Disponible a: http://matematicas.uam.es/~antonio.cordoba/miscelanea/ensayos/Felipe%20II.pdf.- Pastor, J.; Sarasa, M. A.; Salazar, J. L. Criptografia digital: fundamentos y aplicaciones. 2ª ed. Zaragoza: Publicaciones Universitarias Universidad de Zaragoza, 2001. ISBN 8477335583.
- Sgarro, Andrea. Códigos secretos. Madrid: Pirámide, 1990. ISBN 8436805259.
- Singh, Simon. Los códigos secretos: el arte y la ciencia de la criptografia, desde el antiguo Egipto a la era de internet. Barcelona: Círculo de Lectores, 2000. ISBN 8422685604.