GUÍA DOCENTE

DENOMINACIÓN DE LA ASIGNATURA

Denominación: **CÓDIGOS Y CRIPTOGRAFÍA**
Código: 101442
Plan de estudios: **GRADO DE INGENIERÍA INFORMÁTICA** Curso: 4
Denominación del módulo al que pertenece: OPTATIVO GENÉRICO
Materia: CÓDIGOS Y CRIPTOGRAFÍA
Carácter: OPTATIVA
Duración: PRIMER CUATRIMESTRE
Créditos ECTS: 6.0
Horas de trabajo presencial: 60
Porcentaje de presencialidad: 40.0%
Horas de trabajo no presencial: 90
Plataforma virtual: http://www.uco.es/moodle

DATOS DEL PROFESORADO

Nombre: ALBUJER BROTONS, ALMA LUISA (Coordinador)
Departamento: MATEMÁTICAS
Área: MATEMÁTICA APLICADA
Ubicación del despacho: Edificio C2 - Albert Einstein, 2a planta, Pasillo Sur. Campus de Rabanales
E-Mail: aalbujer@uco.es Teléfono: 680153136

REQUISITOS Y RECOMENDACIONES

Requisitos previos establecidos en el plan de estudios
Ninguno

Recomendaciones
Se recomienda que los alumnos tengan inquietud por conocer los distintos métodos de criptografía, interés por las matemáticas, cierta soltura con la programación y ganas de aprender a programar con MATLAB y adquirir soltura con dicho software.

COMPETENCIAS

CB4 Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado.

CB5 Que los estudiantes hayan desarrollado las habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía.

CEB1 Capacidad para la resolución de los problemas matemáticos que puedan plantearse en la ingeniería. Aptitud para aplicar los conocimientos sobre: álgebra lineal; cálculo diferencial e integral; métodos numéricos; algorítmica numérica; estadística y optimización.

GUÍA DOCENTE

OBJETIVOS

- Comprender el papel de las matemáticas en la transmisión segura y fiable de la información.
- Familiarizarse con algunos ejemplos notables de criptosistemas de clave simétrica. Saber cómo se usan, sus fortalezas y sus debilidades. Entender la diferencia entre criptografía de clave simétrica o privada y criptografía de clave asimétrica o pública.
- Diseño de protocolos criptográficos usando algoritmos conocidos.
- Conocer el funcionamiento del RSA y de algunos criptosistemas basados en logaritmos discretos.
- Conocer algunos algoritmos de cifrado digital de imágenes.
- Conocer algún algoritmo de tipo hash.

CONTENIDOS

1. Contenidos teóricos

En la parte teórica de la asignatura se estudiarán los conceptos teóricos que están en la base de la criptografía, y se tratarán los conceptos de criptografía de clave privada y de clave pública.

Se estudiarán desde un punto de vista teórico algunos de los principales métodos de criptografía de clave pública que más adelante se implementarán en las prácticas. Para ello deberemos estudiar algunos conceptos matemáticos necesarios para la buena comprensión y posterior implementación de los distintos códigos. Algunas de estas herramientas son:

- Una introducción a la lógica computacional
- Los cuerpos finitos como estructura algebraica
- Aritmética en un cuerpo finito, es decir, la aritmética modular
- Tests de primalidad

Esta base matemática será imprescindible para poder abordar los siguientes contenidos propios de los Códigos y la Criptografía

- Una introducción a la teoría de códigos
- Códigos lineales
- Teoría general de Codificación y Criptografía

2. Contenidos prácticos

Tras una introducción histórica, empezaremos a trabajar con algunos criptosistemas clásicos (cifrado afín, cifrado Hill, máquina enigma, etc.) pasando a estudiar algunos modernos (cifrado con mochilas, cifrado RSA, cifrado de imágenes, etc.). Para ello realizaremos las siguientes prácticas. El lenguaje de programación usado será MATLAB.

Práctica 1: Cifrado Afín. Cifrado César (caso particular del afín).
Práctica 2: Cifrado Hill y cifrado de permutación como caso particular del cifrado Hill.
Práctica 3: Práctica dedicada a la máquina enigma.
Práctica 4: Cifrado Asimétrico con Mochilas. Cifrado con Mochilas Trampa.
Práctica 5: Camino hacia la clave pública. Intercambio de claves de Diffie y Hellman.
Práctica 6: Cifrado RSA, cifrado ElGamal y autentificación de firma.
Práctica 7: Un poco de esteganografía con imágenes.
Práctica 8: Cifrando una imagen (Arnold).
Práctica 9: Implementación del MD5.

GUÍA DOCENTE

OBJETIVOS DE DESARROLLO SOSTENIBLE RELACIONADOS CON LOS CONTENIDOS

Sin relación

METODOLOGÍA

Aclaraciones generales sobre la metodología (opcional)

En las clases de teoría se desarrollarán los conceptos y contenidos teóricos necesarios para un correcto seguimiento de la asignatura y que permitirán, junto con las clases prácticas, adquirir las competencias de la asignatura. Estas clases no sólo se limitarán a lecciones magistrales por parte del profesor, sino que se promoverá la participación activa de los estudiantes.

En las clases de prácticas se irán programando los distintos métodos de cifrado y los estudiantes se irán ayudando unos a otros.

Adaptaciones metodológicas para alumnado a tiempo parcial y estudiantes con discapacidad y necesidades educativas especiales

En cuanto a los alumnos matriculados a tiempo parcial, se tendrán en cuenta las circunstancias y disponibilidad de cada uno de estos alumnos, tanto para el desarrollo de la asignatura, como para su evaluación. La adaptación a cada uno de los estudiantes matriculados a tiempo parcial se acordará con el profesor al inicio del cuatrimestre.

Así mismo, tanto la metodología como la evaluación se adaptará a aquellos alumnos con necesidades educativas especiales.

Actividades presenciales

Actividad	Grupo completo	Grupo mediano	Total
Actividades de evaluación	2	-	2
Laboratorio criptográfico	6	24	30
Lección magistral	24	-	24
Trabajos en grupo (cooperativo)	4	-	4
Total horas:	***36***	***24***	***60***

Actividades no presenciales

Actividad	Total
Ejercicios	20
Estudio	20
Programación de distintos métodos de cifrado	40
Trabajo de grupo	10
Total horas:	***90***

GUÍA DOCENTE

MATERIAL DE TRABAJO PARA EL ALUMNO

Casos y supuestos prácticos
Ejercicios y problemas
Presentaciones PowerPoint
Referencias Bibliográficas

Aclaraciones

Los materiales de trabajo se irán poniendo a disposición de los alumnos mediante la plataforma Moodle, y se les darán las instrucciones oportunas para que los alumnos usen los materiales de un modo correcto.

EVALUACIÓN

Competencias	Debate	Resolución de problemas	Supuesto práctico/discusión caso clínico/discusión trabajo científico
CB4	X	X	X
CB5	X	X	X
CEB1	X	X	X
Total (100%)	***20%***	***15%***	***65%***
Nota mínima (*)	***0***	***4***	***4***

(*)Nota mínima (sobre 10) necesaria para que el método de evaluación sea considerado en la calificación final de la asignatura. En todo caso, la calificación final para aprobar la asignatura debe ser igual o superior a 5,0.

Valora la asistencia en la calificación final:

No

Aclaraciones generales sobre los instrumentos de evaluación:

Periodo de validez de las calificaciones parciales: todas las convocatorias ordinarias del presente curso académico.

La teoría tendrá un peso del 35% en la calificación final, mientras que la práctica lo tendrá del 65%. En ambas partes se llevará a cabo una evaluación continua. En las clases teóricas se tendrán que hacer varias entregas a lo largo de la asignatura con cuestiones sobre los conceptos estudiados que serán debatidas en entrevistas individuales, y en las clases prácticas se irán implementando los distintos métodos estudiados.

Al final del cuatrimestre, las personas que no tengan superada esa evaluación continua tendrán que realizar un examen final tanto de la parte teórica como de la parte práctica.

Aclaraciones sobre la evaluación para el alumnado a tiempo parcial y necesidades educativas especiales:

En cuanto a los alumnos matriculados a tiempo parcial, se tendrán en cuenta las circunstancias y disponibilidad de cada uno de estos alumnos, tanto para el desarrollo de la asignatura, como para su evaluación. La adaptación a cada uno de los estudiantes matriculados a tiempo parcial se acordará con el profesor al inicio del cuatrimestre.

GUÍA DOCENTE

Así mismo, tanto la metodología como la evaluación se adaptará a aquellos alumnos con necesidades educativas especiales.

Aclaraciones sobre la evaluación de la primera convocatoria extraordinaria y convocatoria extraordinaria de finalización de estudios:

En el caso de las convocatorias extraordinarias reflejadas en el reglamento de de régimen académico, en concreto la primera convocatoria extraordinaria y la convocatoria extraordinaria de finalización de estudios, se regirán por los contenidos y criterios de la guía del curso anterior, y podrán acceder a ellas los estudiantes que cumplan los requisitos reflejados en el reglamento de régimen académico de la Universidad de Córdoba.

Criterios de calificación para la obtención de Matrícula de Honor:

Según el artículo 80.3 del RRA, la mención Matrícula de Honor podrá ser otorgada a alumnos que hayan obtenido al menos una calificación de 9, en los límites marcados en dicho artículo. En caso de empate se propondrá una actividad final para decidir.

BIBLIOGRAFIA

1. Bibliografía básica

- J. I. Hall. Notes on Coding Theory. http://www.mth.msu.edu/~jhall/classes/classes.html.
- R. Hill. A first course in coding theory. Oxford University Press, 1986.
- J. Hoffstein, J. Pipher, J.H. Silverman. An introduction to mathematical cryptography. Springer (2008).
- N. Koblitz. A course in Number Theory and Criptography, 2nd ed.. Springer-Verlag (1994).
- D. R. Kohel. Cryptography. http://echidna.maths.usyd.edu.au/~kohel/tch/Crypto/.
- J. Menezes, P. C. van Oorschot, S. A. Vanstone. Handbook of applied cryptography. CRC Press (1997). (Versiónelectrónica: http://www.cacr.math.uwaterloo.ca/hac/).
- R. A. Podestá. Introducción a la teoría de códigos autocorrectores. http://www.famaf.unc.edu.ar/series/pdf/pdfCMat/CMat35-3.pdf.
- N. Smart, Cryprography, an introduction. http://www.cs.bris.ac.uk/~nigel/Crypto_Book/.
- D. R. Stinson. Cryptography theory and practice. Chapman & Hall/CRC (2006).
- Elementary Number Theory, Cryptography and Codes (Baldoni, Ciliberto, Cattaneo 2009). Springer

2. Bibliografía complementaria

Ninguna.

CRITERIOS DE COORDINACIÓN

Actividades conjuntas: conferencias, seminarios, visitas...
Fecha de entrega de trabajos

Las estrategias metodológicas y el sistema de evaluación contempladas en esta Guía Docente serán adaptadas de acuerdo a las necesidades presentadas por estudiantes con discapacidad y necesidades educativas especiales en los casos que se requieran.

PLAN DE CONTINGENCIA: ESCENARIO A

El escenario A, se corresponde con una menor actividad académica presencial en el aula como consecuencia de medidas sanitarias de distanciamiento interpersonal que limite el aforo permitido en las aulas.

GUÍA DOCENTE

METODOLOGÍA

Aclaraciones generales sobre la metodología en el escenario A

Se adoptará un sistema multimodal o híbrido de enseñanza que combine, en todo lo posible, las clases presenciales en aula y las clases presenciales por videoconferencia (sesiones síncronas) que se impartirán en el horario aprobado por el Centro. La distribución temporal de las actividades que se llevarán a cabo de forma presencial en aula y presencial por videoconferencia estará determinado por el Centro en función del aforo permitido en los espacios docentes y las medidas sanitarias de distanciamiento interpersonal que estén vigentes en cada momento.

En las clases de teoría se desarrollarán los conceptos y contenidos teóricos necesarios para un correcto seguimiento de la asignatura y que permitirán, junto con las clases prácticas, adquirir las competencias de la asignatura. Estas clases no sólo se limitarán a lecciones magistrales por parte del profesor, sino que se promoverá la participación activa de los estudiantes.

Las explicaciones se desarrollarán en pizarra y/o con el apoyo de presentaciones, aunque para el alumnado que no se encuentre presencialmente en el aula se retransmitirá la clase con una sesión de videoconferencia síncrona mediante alguna de las herramientas con soporte oficial por parte de la Universidad de Córdoba.

En las clases de prácticas se irán programando los distintos métodos de cifrado y los estudiantes se irán ayudando unos a otros. En caso de que la totalidad (o parte) del alumnado no se encuentre presencialmente en el aula los alumnos participarán mediante sesiones de videoconferencia síncronas.

EVALUACIÓN

Competencias	Debate	Resolución de problemas	Supuesto práctico/discusión caso clínico/discusión trabajo científico
CB4	X	X	X
CB5	X	X	X
CEB1	X	X	X
Total (100%)	***20%***	***15%***	***65%***
Nota mínima (*)	***0***	***4***	***4***

(*)Nota mínima (sobre 10) necesaria para que el método de evaluación sea considerado en la calificación final de la asignatura. En todo caso, la calificación final para aprobar la asignatura debe ser igual o superior a 5,0.

Valora la asistencia en la calificación final (Escenario A):

No

GUÍA DOCENTE

Aclaraciones generales sobre los instrumentos de evaluación (Escenario A):

Periodo de validez de las calificaciones parciales: todas las convocatorias ordinarias del presente curso académico. En el caso de las convocatorias extraordinarias reflejadas en el reglamento de régimen académico, se regirán por los contenidos y criterios de la guía del curso anterior, y podrán acceder a ellas los estudiantes que cumplan los requisitos reflejados en el reglamento de régimen académico de la Universidad de Córdoba.

La teoría tendrá un peso del 35% en la calificación final, mientras que la práctica lo tendrá del 65%. En ambas partes se llevará a cabo exclusivamente una evaluación continua. Para la evaluación de la parte teórica, se tendrán que hacer varias entregas a lo largo de la asignatura con cuestiones sobre los conceptos estudiados que serán debatidas en entrevistas individuales. En las clases prácticas se irán implementando los distintos métodos estudiados.

Al final del cuatrimestre, las personas que no tengan superada esa evaluación continua tendrán que realizar un examen final tanto de la parte teórica como de la parte práctica a fin de recuperarlas.

Aclaraciones sobre la evaluación para el alumnado a tiempo parcial y necesidades educativas especiales (Escenario A):

En cuanto a los alumnos matriculados a tiempo parcial, se tendrán en cuenta las circunstancias y disponibilidad de cada uno de estos alumnos, tanto para el desarrollo de la asignatura, como para su evaluación. La adaptación a cada uno de los estudiantes matriculados a tiempo parcial se acordará con el profesor al inicio del cuatrimestre.

Así mismo, tanto la metodología como la evaluación se adaptará a aquellos alumnos con necesidades educativas especiales.

PLAN DE CONTINGENCIA: ESCENARIO B

El escenario B, contempla la suspensión de la actividad presencial en el aula como consecuencia de medidas sanitarias.

METODOLOGÍA

Aclaraciones generales sobre la metodología en el escenario B

La actividad docente presencial se llevará a cabo por videoconferencia (sesiones síncronas) en el horario aprobado por el Centro. Se propondrán actividades alternativas para los grupos reducidos que garanticen la adquisición de las competencias de esa asignatura.

En las clases de teoría se desarrollarán los conceptos y contenidos teóricos necesarios para un correcto seguimiento de la asignatura y que permitirán, junto con las clases prácticas, adquirir las competencias de la asignatura. Las explicaciones se desarrollarán con sesiones de videoconferencia síncronan mediante alguna de las plataformas que cuente con soporte oficial por parte de la UCO.

En las clases de prácticas se irán programando los distintos métodos de cifrado con la ayuda del profesor mediante sesiones de videoconferencia síncronas. Se fomentará que los estudiantes se ayuden unos a otros.

GUÍA DOCENTE

EVALUACIÓN

Competencias	Debate	Resolución de problemas	Supuesto práctico/discusión caso clínico/discusión trabajo científico
CB4	X	X	X
CB5	X	X	X
CEB1	X	X	X
Total (100%)	***20%***	***15%***	***65%***
Nota mínima (*)	***0***	***4***	***4***

(*)Nota mínima (sobre 10) necesaria para que el método de evaluación sea considerado en la calificación final de la asignatura. En todo caso, la calificación final para aprobar la asignatura debe ser igual o superior a 5,0.

Herramientas Moodle	Debate	Resolución de problemas	Supuesto práctico/discusión caso clínico/discusión trabajo científico
Tarea		X	X
Videoconferencia	X		X

Valora la asistencia en la calificación final (Escenario B):

No

Aclaraciones generales sobre los instrumentos de evaluación (Escenario B):

Periodo de validez de las calificaciones parciales: todas las convocatorias ordinarias del presente curso académico.

En el caso de las convocatorias extraordinarias reflejadas en el reglamento de régimen académico, se regirán por los contenidos y criterios de la guía del curso anterior, y podrán acceder a ellas los estudiantes que cumplan los requisitos reflejados en el reglamento de régimen académico de la Universidad de Córdoba.

La teoría tendrá un peso del 35% en la calificación final, mientras que la práctica lo tendrá del 65%. En ambas partes se llevará a cabo exclusivamente una evaluación continua. Para la evaluación de la parte teórica, se tendrán que hacer varias entregas a lo largo de la asignatura con cuestiones sobre los conceptos estudiados que serán debatidas en entrevistas individuales. En las clases prácticas se irán implementando los distintos métodos estudiados.

Al final del cuatrimestre, las personas que no tengan superada esa evaluación continua tendrán que realizar un examen final tanto de la parte teórica como de la parte práctica a fin de recuperarlas.

GUÍA DOCENTE

Aclaraciones sobre la evaluación para el alumnado a tiempo parcial y necesidades educativas especiales (Escenario B):

En cuanto a los alumnos matriculados a tiempo parcial, se tendrán en cuenta las circunstancias y disponibilidad de cada uno de estos alumnos, tanto para el desarrollo de la asignatura, como para su evaluación. La adaptación a cada uno de los estudiantes matriculados a tiempo parcial se acordará con el profesor al inicio del cuatrimestre.

Así mismo, tanto la metodología como la evaluación se adaptará a aquellos alumnos con necesidades educativas especiales.