ESCUELA POLITÉCNICA SUPERIOR DE CÓRDOBA

GRADO DE INGENIERÍA INFORMÁTICA

CURSO 2024/25

CÓDIGOS Y CRIPTOGRAFÍA

Datos 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: moodle.uco.es/m2425

Profesor coordinador

Nombre: ALBUJER BROTONS, ALMA LUISA
Departamento: MATEMÁTICAS
Ubicación del despacho: Edificion C2, 2ª planta, Ala Sur, Despacho C22S080
E-Mail: alma.albujer@uco.es **Teléfono:** 957211058

Breve descripción de los contenidos

A lo largo de la asignatura se dará una visión histórica de la criptografía, se describirán las diferencias entre la criptografía de clave privada y la de clave pública y se estudiarán algunos métodos de cifrado concretos. Para ello, habrá que estudiar la base matemática necesaria para comprender los distintos métodos a desarrollar a lo largo de la asignatura.

Desde un punto de vista práctico, el alumnado programará los distintos métodos de cifrado estudiados.

Conocimientos previos necesarios

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.

Por otro lado, se recomienda que los alumnos revisen los contenidos estudiados en Álgebra Lineal sobre cálculo matricial, y en Matemática Discreta sobre cuerpos finitos y aritmética modular.

Programa de la asignatura

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.

También se estudiarán desde un punto de vista teórico algunos de los principales métodos de criptografía tanto de clave privada como de clave pública, que más adelante se implementarán en las prácticas. En concreto se considerarán los cifrados de clave privada afín, César, Hill, de permutación y asimétrico con mochilas y los cifrados de cave pública de mochila trampa y RSA. Además, se tratará la autentificación de firma y algunos métodos de esteganografía y criptografía digital. Por último, se estudiará la máquina Enigma y las funciones hash.

A lo largo del estudio de todos los conceptos anteriores, deberemos estudiar también algunos conceptos matemáticos necesarios para la buena comprensión y posterior implementación de los distintos códigos. Algunas de estas herramientas son:
- Los cuerpos finitos como estructura algebraica.
- Aritmética en un cuerpo finito, es decir, la aritmética modular.
- Propiedades de los números primos.

Esta base matemática será imprescindible para poder abordar los contenidos propios de la asignatura.

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 y cifrado César como caso particular del cifrado afín.
Práctica 2: Cifrado Hill y cifrado de permutación como caso particular del cifrado Hill.
Práctica 3: Cifrado asimétrico con mochilas. Cifrado con mochilas trampa.
Práctica 4: Camino hacia la clave pública. Intercambio de claves de Diffie y Hellman.
Práctica 5: Cifrado RSA y autentificación de firma.
Práctica 6: Un poco de esteganografía con imágenes.
Práctica 7: Cifrando una imagen (Arnold).
Práctica 8: Implementación del MD5.

Bibliografía

- M. W. Baldoni, C. Ciliberto y G. M. Paicentini Cattaneo, Elementary Number Theory, Cryptography and Codes. Universitext. Springer-Verlag, 2009.
- W. Easttom, Modern Cryptography, Applied Mathematics for Encryption and Information Security.

Springer Cham, 2021.
- N. Smart, Cryptography: An Introduction, 3rd Edition. McGraw-Hill College, 2004. https://www.cs.umd.edu/~waa/414-F11/IntroToCrypto.pdf.
- N. Koblitz, A course in Number Theory and Cryptography. Springer Science & Business Media, 2012. http://almuhammadi.com/sultan/crypto_books/Koblitz.2ndEd.pdf
- J. H. Silverman, J. Pipher y J. Hoffstein, An Introduction to Mathematical Cryptography. Undergraduate Texts in Mathematics. Springer New York, 2010.
- J. I. Hall, Notes on Coding Theory, 2010. https://users.math.msu.edu/users/halljo/classes/codenotes/Topstuff.pdf

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 y resultados de aprendizaje de la asignatura. Estas clases no sólo se limitarán a lecciones magistrales por parte del docente, 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 ellos, 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 adaptarán al alumnado con necesidades educativas especiales.

Actividades presenciales

Actividad	Grupo completo	Grupo mediano	Total
Actividades de comunicacion oral	4	-	4
Actividades de experimentacion práctica	6	24	30
Actividades de exposición de contenidos elaborados	26	-	26
Total horas:	***36***	***24***	***60***

Actividades no presenciales

Actividad	Total
Actividades de búsqueda de información	15
Actividades de procesamiento de la información	15
Actividades de resolución de ejercicios y problemas	60
Total horas:	***90***

Resultados del proceso de aprendizaje

Conocimientos, competencias y habilidades

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.

Métodos e instrumentos de evaluación

Competencias	Medios de ejecución práctica	Medios orales	Producciones elaboradas por el estudiantado
CB4		X	X
CB5	X	X	X
CEB1	X	X	X
Total (100%)	***15%***	***20%***	***65%***
Nota mínima (*)	***5***	***0***	***5***

(*)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.

Aclaraciones generales sobre los instrumentos de evaluación:
Periodo de validez de las calificaciones parciales: todas las convocatorias del presente curso académico.

El instrumento "medios de ejecución práctica" consiste en resolver una serie de ejercicios teóricos para asimilar la teoría estudiada. El instrumento "producciones elaboradas por el estudiantado" supone la realización de una serie de prácticas consistentes en la programación de los distintos métodos de criptografía estudiados. En ambas partes se llevará a cabo una evaluación continua.

Por último, el método "medios orales" supone el estudio de un nuevo método de criptografía, o de cualquier otro aspecto relacionado con la asignatura, la preparación de un trabajo sobre ello y la exposición de este al resto de los compañeros.

Al final del cuatrimestre, el alumnado que no tenga superada la evaluación continua tendrá que realizar un examen final.

Aclaraciones sobre la evaluación para el alumnado a tiempo parcial y necesidades educativas especiales:
En cuanto al alumnado matriculado a tiempo parcial, se tendrá en cuenta las circunstancias y disponibilidad de cada uno de los estudiantes en esta situación, tanto para el desarrollo de la asignatura como para su evaluación. La adaptación a cada uno de ellos se acordará con el profesor al inicio del cuatrimestre.

Así mismo, tanto la metodología como la evaluación se adaptarán al alumnado con necesidades educativas especiales.

Aclaraciones sobre la evaluación de la convocatoria extraordinaria y convocatoria extraordinaria de finalización de estudios:
Ambas convocatorias se regirán por los contenidos y criterios de evaluación de la presente guía. Podrán acceder a estas convocatorias 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 RRA, la mención Matrícula de Honor podrá ser otorgada a alumnos que hayan obtenido al menos una calificación de 9, en los límites marcados por dicho reglamento. En caso de empate se propondrá una actividad final para decidir.

Objetivos de desarrollo sostenible

Educación de calidad

Las estrategias metodológicas y el sistema de evaluación contempladas en esta Guía Docente responderán a los principios de igualdad y no discriminación y deberán ser adaptadas de acuerdo a las necesidades presentadas por estudiantes con discapacidad y necesidades educativas especiales en los casos que se requieran.
El estudiantado deberá ser informado de los riesgos y las medidas que les afectan, en especial las que puedan tener consecuencias graves o muy graves (artículo 6 de la Política de Seguridad, Salud y Bienestar; BOUCO 23-02-23).