

MÓDULO	APLICACIONES DE LAS MATEMÁTICAS	
MATERIA	MATEMÁTICAS APLICADAS A LA INFORMÁTICA	
SEMESTRE	PRIMERO	
CRÉDITOS	8	
ENSEÑANZA	PRESENCIAL	
DISTRIBUCIÓN DOCENTE POR UNIVERSIDADES	UNIVERSIDAD DE GRANADA (6 ECTS) UNIVERSIDAD DE ALMERÍA (2 ECTS)	
IDIOMA	ESPAÑOL/INGLÉS	
PROFESORES		
NOMBRE	DIRECCIÓN	
PASCUAL JARA MARTÍNEZ (3 ECTS)	Dpto. de Álgebra, Facultad de Ciencias, Universidad de Granada, 958243369, pjara@ugr.es	
FRANCISCO JAVIAER LOBILLO BORRERO (2 ECTS)	Dpto. de Álgebra, ETSI Informática y de Telecomunicación, Universidad de Granada, 958240826, jlobillo@ugr.es	
EVANGELINA SANTOS ALÁEZ (1 ECTS)	Dpto. de Álgebra, ETSI Informática y de Telecomunicación, Universidad de Granada, 958240823, esantos@ugr.es	
BLAS TORRECILLAS JOVER (2 ECTS)	Dpto. de Matemáticas, Facultad de Ciencias, Universidad de Almería, 950015029, btorrecci@ual.es	
TUTORÍAS		
El horario de tutorías está disponible en la página de profesorado del máster http://masteres.ugr.es/doctomat/pages/info_academica/profesorado , en el curso académico correspondiente.		
PRERREQUISITOS Y/O RECOMENDACIONES (si procede)		
Los de acceso al máster.		



COMPETENCIAS GENERALES Y ESPECÍFICAS

COMPETENCIAS GENERALES

- CG1. Saber aplicar los conocimientos adquiridos y desarrollar la capacidad en la resolución de problemas en entornos nuevos o pocos conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con el Álgebra, el Análisis Matemático, la Geometría y Topología o la Matemática Aplicada.
- CG2. Ser capaz de integrar conocimientos y enfrentarse a la complejidad de formar juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios.
- CG3. Ser capaz de comunicar sus conclusiones (y los conocimientos y razones últimas que los sustentan) a públicos especializados y no especializados de un modo claro y sin ambigüedades, utilizando en su caso, los medios tecnológicos y audiovisuales adecuados.
- CG4. Poseer las habilidades de aprendizaje que les permita continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.
- CG5. Utilizar con soltura herramientas de búsqueda de recursos bibliográficos.
- CG6. Usar el inglés, como lengua relevante en el ámbito científico.
- CG7. Saber trabajar en equipo y gestionar el tiempo de trabajo.

COMPETENCIAS ESPECÍFICAS

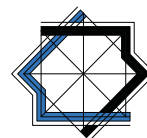
- CE1. Saber analizar y construir demostraciones, así como transmitir conocimientos matemáticos avanzados.
- CE2. Tener capacidad para elaborar y desarrollar razonamientos matemáticos avanzados.
- CE3. Asimilar la definición de un nuevo objeto matemático, en términos de otros ya conocidos y ser capaz de utilizar este objeto en diferentes contextos.
- CE4. Saber abstraer las propiedades estructurales (de objetos matemáticos, de la realidad observada y del mundo de las aplicaciones) distinguiéndolas de aquellas puramente ocasionales y poder comprobarlas o refutarlas.
- CE5. Resolver problemas matemáticos avanzados, planificando su resolución en función de las herramientas disponibles y de las restricciones de tiempo y recursos.
- CE6. Proponer, analizar, validar e interpretar modelos matemáticos complejos, utilizando las herramientas más adecuadas a los fines que se persigan.
- CE7. Saber elegir y utilizar aplicaciones informáticas, de cálculo numérico y simbólico, visualización gráfica, optimización u otras, para experimentar en matemáticas y resolver problemas complejos.

OBJETIVOS (EXPRESADOS COMO RESULTADOS ESPERABLES DE LA ENSEÑANZA)

- Conseguir que el alumno conozca los principales protocolos, algoritmos y técnicas utilizados en criptografía así como la capacidad de implementarlos y utilizarlos en entornos reales.
- Incidir en diferentes aplicaciones en el campo de la Informática de técnicas avanzadas de computación geométrica que el alumno debe adquirir.

TEMARIO DE LA ASIGNATURA

1. Conceptos básicos de criptografía
2. Criptografía simétrica: DES, IDEA, AES, y cifrados de flujo.
3. Criptografía asimétrica: RSA, Diffie-Hellman y ElGamal.
4. Criptosistemas basados en curvas elípticas y en modelos no conmutativos
5. Códigos correctores de errores. Códigos cíclicos.
6. Criptosistema de McEliece.
7. Algoritmos básicos en anillos de polinomios.
8. Algoritmo de la división y bases de Groebner.
9. Cálculo de invariantes en álgebra conmutativa y no conmutativa.
10. Aplicaciones a la geometría en el plano y el espacio.



11. Aplicaciones a otros campos de la Matemática: interpolación, ecuaciones diferenciales, programación, optimización, ...
12. Aplicaciones a otras ciencias, la industria y la empresa.

Sesiones prácticas de Ordenador con programas de protección de seguridad de sistemas informáticos, y de las comunicaciones, y programas de cálculo simbólico.

BIBLIOGRAFÍA

1. Brassard, Guiles: "Modern Cryptography, a tutorial", Springer-Verlag, 1988.
2. Dawson; Golic: "Cryptography: policy and algorithms", 1996.
3. Koblitz, Neal: "A course in number theory and cryptography", Springer-Verlag, 1979.
4. Manuel Lucena López: "http://wwwdi.ujaen.es/~mlucena/lcripto.html" "Criptografía y Seguridad en Computadores", Universidad de Jaén.
5. D.R. Stinson: "Cryptography: Theory & Practice", CRC 1995.
6. J.-C. Faugère, L. Perret. "Efficient Computation of Gröbner Bases and Applications in Cryptography. Springer.
7. Davenport, J. H.; Siret, Y.; Tournier, E. Computer algebra. Systems and algorithms for algebraic computation. With a preface by Daniel Lazard. Translated from the French by A. Davenport and J. H. Davenport. With a foreword by Anthony C. Hearn. Academic Press, Inc. [Harcourt Brace Jovanovich, Publishers], London, 1988. xx+267 pp.
8. Keith O. Geddes, Stephen R. Czapor, George Labahn, Algorithms for Computer Algebra. Kluwer Academic Publishers, Boston, MA, 1992. xxii+585 pp.
9. Geometric modeling and algebraic geometry. Edited by Bert Jüttler and Ragni Piene. Springer-Verlag, Berlin, 2008. viii+231 pp.
10. Cox, David; Little, John; O'Shea, Donal Ideals, varieties, and algorithms. An introduction to computational algebraic geometry and commutative algebra. Third edition. Undergraduate Texts in Mathematics. Springer, New York, 2007. xvi+551 pp.
11. Martin Kreuzer, Lorenzo Robbiano, Computational commutative algebra. 2. Springer-Verlag, Berlin, 2005. x+586 pp.
12. Algebraic statistics for computational biology. Edited by Lior Pachter and Bernd Sturmfels. Cambridge University Press, New York, 2005. xii+420 pp.
13. W. C. Huffman, V. Pless. Fundamentals of Error-Correcting Codes, Cambridge University Press, 2010.
14. R. J. McEliece. A public-key cryptosystem based on algebraic coding theory. JPL DSN Progress Report, pages 114-116, 1978.
15. Differential equations with symbolic computation. Edited by Dongming Wang and Zhiming Zheng. Trends in Mathematics. Birkhuser Verlag, Basel, 2005. viii+374 pp.
16. D. Hankelson, A. Menezes, S. Vanstone. Guide to Elliptic Curve Cryptography, Springer, 2004.

ENLACES RECOMENDADOS

1. StackExchange: <https://math.stackexchange.com>
2. Mathoverflow: <https://mathoverflow.net>

METODOLOGÍA DOCENTE

Las actividades formativas se desarrollarán desde una metodología participativa y aplicada que se centra en el trabajo del estudiante (presencial y no presencial, individual y grupal).

Cada crédito ECTS se corresponde con 25 horas de trabajo del alumno y para esta materia un 30% se desarrollará en el aula y por tele-docencia incluyendo también en este porcentaje las tutorías, seminarios, exposiciones y exámenes. El





70% restante se ocupará con actividades no presenciales centradas en la tutoría online y en el estudio y trabajo del alumno.

Con objeto de conseguir las competencias esperadas se realizarán:

- *Actividades presenciales:* Sesiones teóricas y prácticas incentivando la participación de los estudiantes en seminarios de investigación y exposiciones (los estudiantes dispondrán en todo momento del material y las referencias necesarias para ello).
- *Actividades no presenciales:* Estudio, trabajo individual, tutorías online, trabajo en grupo y autoevaluaciones que facilitarán el estudio de los contenidos, el análisis y la resolución de problemas.

Las actividades en el aula se realizarán en sesiones de 2'5 horas.

EVALUACIÓN (INSTRUMENTOS DE EVALUACIÓN, CRITERIOS DE EVALUACIÓN Y PORCENTAJE SOBRE LA CALIFICACIÓN FINAL, ETC.)

La asistencia y participación en las clases es indispensable para superar el curso. Para los alumnos que deseen profundizar más en la materia se propondrá material y trabajos adicionales. A los estudiantes que no pueden asistir a todas las clases se les ayudará a superar el curso mediante trabajos dirigidos y material para enseñanza programada para ser desarrollada a través de Internet.

Los Procedimientos para la evaluación:

- Participación en las actividades presenciales y online.
- Análisis de contenido de los trabajos individuales y grupales realizados en las clases prácticas, en los seminarios actividades de autoevaluación y tutorías (presenciales y online).
- Otros procedimientos para evaluar la participación del estudiante en las diferentes actividades planificadas.
- Examen final.

La calificación global responderá a la puntuación ponderada de los diferentes aspectos y actividades que integran el sistema de evaluación, por lo tanto éstas pueden variar en función de las necesidades específicas de las asignaturas que componen cada materia; de manera general se indica la siguiente ponderación:

- Trabajos individuales y grupales: hasta 30%.
- Prácticas y/o problemas: hasta 30%.
- Actividades en seminarios : hasta 10%.
- Otras actividades: hasta 10%.
- Examen final: hasta 40%.

EVALUACIÓN ÚNICA FINAL

Atendiendo a la normativa vigente sobre evaluación y calificación de los estudiantes de las Universidades participantes en el máster, el estudiante que no pueda cumplir con el método de evaluación continua por motivos laborales, estado de salud, discapacidad o cualquier otra causa debidamente justificada que les impida seguir el régimen de evaluación continua, podrá acogerse a una evaluación única final. Para acogerse a la evaluación única final, el estudiante, en las dos primeras semanas de impartición de la asignatura, lo solicitará a la Coordinación del Máster, quien dará traslado al profesorado correspondiente, alegando y acreditando las razones que le asisten para no poder seguir el sistema de evaluación continua. Por ello en las convocatorias oficiales se desarrollará un examen que se dividirá en los siguientes apartados:

- Prueba escrita, del mismo temario teórico que el resto de sus compañeros.
- Prueba escrita del temario práctico.

CONVOCATORIA EXTRAORDINARIA

Tal y como establece la normativa al respecto, los estudiantes que no hayan superado la asignatura en la convocatoria ordinaria dispondrán de una convocatoria extraordinaria. A ella podrán concurrir todos los



estudiantes, con independencia de haber seguido o no un proceso de evaluación continua. De esta forma, el estudiante que no haya realizado la evaluación continua tendrá la posibilidad de obtener el 100% de la calificación mediante la realización de una prueba y/o trabajo.

EVALUACIÓN POR INCIDENCIAS

En la evaluación por incidencias se tendrá en cuenta la normativa de evaluación de las distintas universidades participantes. De esta forma, los estudiantes que no puedan concurrir a pruebas de evaluación que tengan asignadas una fecha de realización por la Comisión Académica del Master, podrán solicitar al Coordinador del Máster la evaluación por incidencias en los siguientes supuestos debidamente acreditados: ante la coincidencia de fecha y hora por motivos de asistencia a las sesiones de órganos colegiados de gobierno o de representación universitaria; por coincidencia con actividades oficiales de los deportistas de alto nivel y de alto rendimiento o por participación en actividades de carácter oficial representando a la Universidad de origen; por coincidencia de fecha y hora de dos o más procedimientos de evaluación de asignaturas de distintos cursos y/o titulaciones; en supuestos de enfermedad debidamente justificada a través de certificado médico oficial; por fallecimiento de un familiar hasta segundo grado de consanguinidad o afinidad acaecido en los diez días previos a la fecha programada para la realización de la prueba; por inicio de una estancia de movilidad saliente en una universidad de destino cuyo calendario académico requiera la incorporación del estudiante en fechas que coincidan con las fechas de realización de la prueba de evaluación.

INFORMACIÓN ADICIONAL

Aunque se hará uso de la teledocencia para todas las actividades programadas en el aula, salvo situaciones justificadas, los estudiantes deben seguir de forma presencial las sesiones que tengan lugar en su universidad.

Ver también web del máster.