

# MATEMÁTICAS APLICADAS A LA INFORMÁTICA

<b>MÓDULO</b>	II b (2). APLICACIONES DE LA MATEMÁTICAS	
<b>MATERIA</b>	MATEMÁTICA APLICADAS A LA INFORMÁTICA	
<b>SEMESTRE</b>	SEGUNDO	
<b>CRÉDITOS</b>	8	
<b>COORDINA</b>	UNIVERSIDAD DE GRANADA	
<b>ENSEÑANZA</b>	SEMIPRESENCIAL	
<b>UNIVERSIDADES EN LAS QUE SE IMPARTE</b>	UNIVERSIDAD DE GRANADA	
<b>IDIOMA</b>	INGLÉS (4 ECTS), ESPAÑOL (4 ECTS)	
<b>PROFESORES</b>		
	<b>NOMBRE</b>	<b>DIRECCIÓN</b>
	PASCUAL JARA MARTÍNEZ	Departamento de Álgebra Facultad de Ciencias. UGR T.: 958243369 CE: pjara@ugr.es
	FRANCISCO JAVIER LOBILLO BORRERO	Departamento de Álgebra Facultad de Ciencias. UGR T.: 958240826 CE: jlobillo@ugr.es
	EVANGELINA SANTOS ALÁEZ	Departamento de Álgebra Facultad de Ciencias. UGR T.: 958240823 CE: esantos@ugr.es
	BLAS TORRECILLAS JOVER	Departamento de Álgebra y Análisis Matemático Facultad de Ciencias. UAL T.: 950015029 CE: btorreci@ual.es
	DRAGOS STEFAN	Department of Mathematics Faculty of Sciences. University of Bucarest (Romania) e-mail: dstefan@al.math.unibuc.ro
<b>PRERREQUISITOS Y/O RECOMENDACIONES (si procede)</b>		
Los de acceso al máster		
<b>COMPETENCIAS GENERALES Y ESPECÍFICAS</b>		

## 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. Firma Digital. Certificados digitales.
6. Protocolos: Secreto compartido. Protocolos de conocimiento cero. Implementación de protocolos de seguridad
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 Practicas 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://www.di.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. Differential equations with symbolic computation. Edited by Dongming Wang and Zhiming Zheng. Trends in Mathematics. Birkhuser Verlag, Basel, 2005. viii+374 pp.

### ENLACES RECOMENDADOS

<http://150.214.18.236/login/index.php>

### METODOLOGÍA DOCENTE

La enseñanza de esta materia será semipresencial y el uso intensivo de las fuentes de Internet es determinante para mejorar e intensificar la calidad docente. Los profesores y estudiantes dispondrán de claves de acceso a la plataforma virtual que les permitirán descargar materiales, atender tutorías, realizar autoevaluaciones y otras actividades propias de este tipo de enseñanza.

Como referencia general cada ECTS se corresponde con 25 horas de trabajo del alumno y para esta materia un 20% (40 horas) se han establecido como actividades presenciales (sesiones teóricas, prácticas de prácticas de ordenador) otras 24 horas incluyen exposiciones, tutorías colectivas y exámenes, un 12%.

Las 25 horas por crédito serán estructuradas como sigue:

- 8 horas de actividades presenciales, en aula y laboratorio, y de trabajos en grupo, seminarios y exámenes.
- 17 horas de actividades no presenciales, centradas en la tutoría online y en el estudio y trabajo del alumno.

Las actividades se programarán con el objeto de conseguir las competencias esperadas de la siguiente forma:

- Actividades presenciales: Sesiones teóricas y prácticas incentivando la participación de los estudiantes en seminarios 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 y la creación de guías teóricas y trabajo práctico.

### PROGRAMA DE ACTIVIDADES

12 Sesiones Segundo semestre	Temas del temario	Actividades presenciales (NOTA: Modificar según la metodología docente propuesta para la asignatura)						Actividades no presenciales (NOTA: Modificar según la metodología docente propuesta para la asignatura)			
		Sesiones teóricas (horas)	Sesiones prácticas + Prácticas Ordenador (horas)	Exposiciones y seminarios (horas)	Tutorías colectivas (horas)	Exámenes (horas)	Etc.	Sesiones Online (horas)	Estudio y trabajo individual del alumno (horas)	Trabajo en grupo (horas)	Auto evaluación
Sesiones 1-2	1-2	2	1+2		2			5	15	5	0
Sesiones 3-4	3-4	2	1+2		1			5	15	5	2
Sesiones 5-6	5-6	2	1+2		2			5	15	5	2
Sesiones 7-8	7-8	2	1+2		2			5	15	5	2
Sesiones 9-10	9-10	2	1+2		2			5	15	5	2
Sesiones 11-12	11-12	2	1+2		1			5	15	5	2
Total horas		12	18		10			30	90	30	10

### 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%

### INFORMACIÓN ADICIONAL

En la web del máster

