Guía docente de la asignatura

Matemáticas Aplicadas a la Informática (M37/56/2/18)

Fecha de aprobación por la Comisión Académica: 12/07/2022

Máster	Máster Universitario en Matemáticas
MÓDULO	Módulo Iib(2). Aplicaciones de las Matemáticas
RAMA	Ciencias
CENTRO RESPONSABLE DEL TÍTULO	Escuela Internacional de Posgrado

Semestre	Primero	**Créditos**	8	**Tipo**	Optativa	**Tipo de enseñanza**	

PRERREQUISITOS Y/O RECOMENDACIONES

Las de acceso al título.

BREVE DESCRIPCIÓN DE CONTENIDOS (Según memoria de verificación del Máster)

- Criptografía simétrica y asimétrica.
- Certificación digital.
- Protocolos.
- Técnicas geométricas aplicadas a la Informática.
- Geometría Computacional

COMPETENCIAS

COMPETENCIAS BÁSICAS

- CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación.
- CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de

resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio.
- CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular 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.
- CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades.
- CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

COMPETENCIAS GENERALES

- CG01 - Utilizar con soltura herramientas de búsqueda de recursos bibliográficos.
- CG02 - Usar el inglés, como lengua relevante en el ámbito científico.
- CG03 - Saber trabajar en equipo y gestionar el tiempo de trabajo.

COMPETENCIAS ESPECÍFICAS

- CE04 - 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.
- CE07 - Saber elegir y utilizar aplicaciones informáticas, de cálculo numérico y simbólico, visualización gráfica, optimización u otras, para experimentar en matemáticas y resolver problemas complejos.
- CE08 - Desarrollar programas informáticos que resuelvan problemas matemáticos avanzados, utilizando para cada caso el entorno computacional adecuado.

RESULTADOS DE APRENDIZAJE (Objetivos)

- Conseguir que el estudiante 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.

PROGRAMA DE CONTENIDOS TEÓRICOS Y PRÁCTICOS

TEÓRICO

- Conceptos básicos de criptografía.
- Criptografía simétrica: DES, IDEA, AES, y cifrados de flujo.
- Criptografía asimétrica: RSA, Diffie-Hellman y ElGamal.
- Criptosistemas basados en curvas elípticas y en modelos no conmutativos
- Códigos correctores de errores. Códigos cíclicos.
- Criptosistema de McEliece.
- Algoritmos básicos en anillos de polinomios.

- Algoritmo de la división y bases de Groebner.
- Cálculo de invariantes en álgebra conmutativa y no conmutativa.
- Aplicaciones a la geometría en el plano y el espacio.
- Aplicaciones a otros campos de la Matemática: interpolación, ecuaciones diferenciales, programación, optimización, ...
- Aplicaciones a otras ciencias, la industria y la empresa.

PRÁCTICO

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

BIBLIOGRAFÍA

BIBLIOGRAFÍA FUNDAMENTAL

- Brassard, Guiles: "Modern Cryptography, a tutorial", Springer-Verlag, 1988.
- Dawson; Golic: "Cryptography: policy and algorithms", 1996.
- Koblitz, Neal: "A course in number theory and cryptography", Springer-Verlag, 1979.
- Manuel Lucena López: "http://wwwdi.ujaen.es/~mlucena/lcripto.html" "Criptografía y Seguridad en Computadores", Universidad de Jaén.
- D.R. Stinson: "Cryptography: Theory & Practice", CRC 1995.
- J.-C Faugère, L. Perret. “Efficient Computation of Gröbner Bases and Applications in Cryptography. Springer.
- 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.
- Keith O. Geddes, Stephen R. Czapor, George Labahn, Algorithms for Computer Algebra. Kluwer Academic Publishers, Boston, MA, 1992. xxii+585 pp.
- Geometric modeling and algebraic geometry. Edited by Bert Juettler and Ragni Piene. Springer-Verlag, Berlin, 2008. viii+231 pp.
- 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.
- Martin Kreuzer, Lorenzo Robbiano, Computational commutative algebra. 2. Springer-Verlag, Berlin, 2005. xx+586 pp.
- Algebraic statistics for computational biology. Edited by Lior Pachter and Bernd Sturmfels. Cambridge University Press, New York, 2005. xii+420 pp.
- W. C. Huffman, V. Pless. Fundamentals of Error-Correcting Codes, Cambridge University Press, 2010.
- R. J. McEliece. A public-key cryptosystem based on algebraic coding theory. JPL DSN Progress Report, pages 114-116, 1978.
- Differential equations with symbolic computation. Edited by Dongming Wang and Zhiming Zheng. Trends in Mathematics. Birkhuser Verlag, Basel, 2005. viii+374 pp.
- D. Hankelson, A. Menezes, S. Vanstone.Guide to Elliptic Curve Criptography, Springer, 2004.

BIBLIOGRAFÍA COMPLEMENTARIA

ENLACES RECOMENDADOS

- StackExchange: https://math.stackexchange.com
- Mathoverflow: https://mathoverflow.net
- Sagemath online: https://sagecell.sagemath.org/

METODOLOGÍA DOCENTE

- MD01 Lección magistral/expositiva
- MD02 Sesiones de discusión y debate
- MD03 Resolución de problemas y estudio de casos prácticos
- MD05 Seminarios
- MD06 Ejercicios de simulación
- MD07 Análisis de fuentes y documentos
- MD08 Realización de trabajos en grupo
- MD09 Realización de trabajos individuales

EVALUACIÓN (instrumentos de evaluación, criterios de evaluación y porcentaje sobre la calificación final)

EVALUACIÓN ORDINARIA

El régimen de asistencia incluye que cada estudiante asista presencialmente a las sesiones de clase impartidas en su universidad de matrícula y online a las impartidas en otras universidades. Los estudiantes que no puedan seguir el régimen de asistencia indicado no tendrán acceso a la evaluación continua y deberán solicitar Evaluación Final Única.

Para la evaluación ordinaria se podrán solicitar a los estudiantes entregas de tareas relativas a cada bloque, que consistirán en resolución de ejercicios, desarrollo de trabajos (individuales o en grupo) o exposiciones. Para su evaluación se tendrán en cuenta la precisión y corrección de los razonamientos. En el cómputo final se ponderarán las calificaciones de estas actividades proporcionalmente al número de sesiones dedicadas a cada bloque.

Estas actividades constituirán el 100% de la nota final.

EVALUACIÓN EXTRAORDINARIA

En la convocatoria extraordinaria se evaluará de la misma forma que la ordinaria, mediante la entrega y defensa de las actividades propuestas, alterando la fecha de entrega.

EVALUACIÓN ÚNICA FINAL

Esta modalidad de evaluación estará formada por todas aquellas pruebas que los profesores estimen oportunas, de forma que se pueda acreditar que el estudiante ha adquirido la totalidad de las competencias generales y específicas descritas en el apartado correspondiente de esta Guía Docente.