GUÍA DE ESTUDIO

MAI

MATEMÁTICAS APLICADAS A LA INFORMÁTICA

Curso académico 2016/17

MÁSTER EN MATEMÁTICAS

ugr | Universidad de Granada

1. Introducción

Esta asignatura engloba dos grandes bloques dedicados a sendas aplicaciones matemáticas a la informática: la criptografía y los algoritmos de computación en anillos de polinomios. Ambos bloques pueden ser estudiados de manera independiente por lo que la temporización del trabajo puede hacerse siguiendo dos líneas de tiempo paralelas. El bloque de criptografía (temas 1 a 6) será impartido por los profesores Blas Torrecillas y Javier Lobillo; el bloque de algoritmos en anillos de polinomios lo impartirán Pascual Jara, Dragos Stefan y Evangelina Santos.

2. Requisitos técnicos

Se requieren los requisitos mínimos para cualquier tipo de formación on-line:

Acceso a Internet y navegador:

- Firefox, Internet Explorer, Safari, etc.

Software de ofimática, visualización de documentos, imágenes y video de uso extendido:

- Openoffice, Microsoft Word, etc.
- Lectores de PDF.
- Pluggins de navegador para reproducción de flash.

Se recomienda además un conocimiento básico de latex necesario para la realización de trabajos.

3. Descripción de la asignatura

1. Datos generales

La asignatura se encuadra en el Módulo II b(2) del Máster en Matemáticas. Se imparte en el segundo semestre y consta de 8 créditos ECTS. Es impartida como enseñanza semipresencial a través de la plataforma Moodle del CEVUG de la Universidad de Granada. En la asignatura se utilizarán los idiomas español e inglés.

2. Profesorado

PASCUAL JARA MARTÍNEZ
Departamento de Álgebra
Facultad de Ciencias. UGR
Teléfono: 958243369
correo electrónico: pjara@ugr.es

FRANCISCO JAVIER LOBILLO BORRERO
Departamento de Álgebra
ETSIIT. UGR
Teléfono: 958240826
correo electrónico: jlobillo@ugr.es

EVANGELINA SANTOS ALÁEZ

Departamento de Álgebra
ETSIIT. UGR
Teléfono: 958240823
correo electrónico: esantos@ugr.es

BLAS TORRECILLAS JOVER
Departamento de Álgebra y Análisis Matemático
Facultad de Ciencias. UAL
Teléfono: 950015029
correo electrónico: btorreci@ual.es

DRAGOS STEFAN
Department of Mathematics
Faculty of Sciences. University of Bucarest (Romania)
e-mail: dstefan@al.math.unibuc.ro

3. Temario

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.

4. Competencias

1. Competencias generales o transversales

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 (omultidisciplinares) relacionados con el Álgebra, el Análisis Matemático, la Geometría y Topología o la Matemática Aplicada.

CG2. Ser capaz de integrar de 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. Poder comunicarse en inglés, como lengua relevante en el ámbito científico.

CG7. Saber trabajar en equipo y gestionar el tiempo de trabajo.

2. 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. Conocer los problemas centrales, la relación entre ellos y las técnicas más adecuadas en los distintos campos de estudio, así como las demostraciones rigurosas de los resultados relevantes.

CE4. Asimilar la definición de un nuevo objeto matemático, en términos de otros ya conocidos y ser capaz de utilizar este objeto en diferentes contextos.

CE5. 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.

CE6. Resolver problemas matemáticos avanzados, planificando su resolución en función de las herramientas disponibles y de las restricciones de tiempo y recursos.

CE7. Proponer, analizar, validar e interpretar modelos matemáticos complejos, utilizando las herramientas más adecuadas a los fines que se persigan. CE7. Saber elegir, utilizar aplicaciones informáticas, de cálculo numérico y simbólico, visualización gráfica, optimización u otras para experimentar en matemáticas y resolver problemas.

CE8. Desarrollar programas informáticas que resuelvan problemas

matemáticos utilizando para cada caso el entorno computacional adecuado.

5. Objetivos

- 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.

6. Bibliografía

1. Brassard, Guiles: "Moderm 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" "Criptografia 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 Davenport and J. H.
8. Davenport. With a foreword by Anthony C. Hearn. Academic Press, Inc. [Harcourt Brace Jovanovich, Publishers], London, 1988. xx+267 pp.
9. Keith O. Geddes, Stephen R. Czapor, George Labahn, Algorithms for Computer Algebra. Kluwer Academic Publishers, Boston, MA, 1992. xxii+585 pp.
10. Geometric modeling and algebraic geometry. Edited by Bert Juettler and Ragni Piene. Springer-Verlag, Berlin, 2008. viii+231 pp
11. 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.
12. Martin Kreuzer, Lorenzo Robbiano, Computational commutative algebra. 2. Springer-Verlag, Berlin, 2005. x+586 pp.
13. Algebraic statistics for computational biology. Edited by Lior Pachter and Bernd Sturmfels. Cambridge University Press, New York, 2005. xii+420 pp.
14. Differential equations with symbolic computation. Edited by Dongming Wang and Zhiming Zheng. Trends in Mathematics. Birkhuser Verlag, Basel, 2005. viii+374 pp.

7. Recursos on-line

Para cada uno de los bloques que componen la asignatura los profesores subirán diferentes tipos de materiales:

- textos básicos de estudio
- presentaciones de las clases presenciales
- relaciones de problemas
- sesiones de trabajo con programas de cálculo simbólico
- ...

y se añadirán

- enlaces a páginas recomendadas
- programas para descargar
- otros recursos disponibles de la plataforma Moodle

8. Evaluación

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 serán:

a. Participación en las actividades presenciales y online.
b. 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).
c. Otros procedimientos para evaluar la participación del estudiante en las diferentes actividades planificadas.
d. Examen final.

La calificación global responderá a la puntuación ponderada de los diferentes aspectos y actividades que integran el sistema de evaluación, de manera general se indica la siguiente ponderación:

1. Trabajos individuales y grupales: hasta 30%
2. Prácticas y/o problemas: hasta 30%
3. Actividades en seminarios : hasta 10%
4. Otras actividades: hasta 10%
5. Examen final: hasta 40%