Plan 510 MÁSTER EN INGENIERÍA INFORMÁTICA

Asignatura 53174 PROTOCOLOS CRIPTOGRÁFICOS

Grupo 1

Tipo de asignatura (básica, obligatoria u optativa)

Optativa

Créditos ECTS

3

Competencias que contribuye a desarrollar

Competencias Genéricas y Específicas: G1-G2-G3-G4-G5-G6-G7-G9-G10- E1-E2-E4-E5-E6-E7-E8-E9-E10-E16-E17:
G1.- Conocimiento del método científico. Conocer el método científico, en particular en el ámbito de las Matemáticas, formulando modelos e hipótesis de trabajo relevantes y planificando el análisis en relación con dichas hipótesis y la discusión de las conclusiones, de modo que se pueda avanzar en el conocimiento de las Matemáticas.
G2.- Competencia para aplicar los conocimientos adquiridos. Es la capacidad para aplicar los conocimientos técnicos adquiridos, de forma coherente y profesional, sobre todo en contextos novedosos o en constante renovación, que impliquen la realización de una actividad matemática.
G3.- Capacidad crítica, de análisis y síntesis, y capacidad de interpretación. Ser capaz de emitir juicios críticos sobre propuestas, hipótesis y validez científica de las conclusiones, así como sintetizar la presentación de propuestas y resultados, en el ámbito de las Matemáticas y de sus aplicaciones.
G4.- Competencias metodológicas. Es la capacidad para elegir la metodología más adecuada para el desarrollo de la investigación de un problema, adaptándola al contexto en el que se origina el problema.
G5.- Capacidad para valorar la originalidad y creatividad. Es la competencia para reconocer la originalidad en la concepción, formulación y resolución de problemas, sobre todo en el ámbito de la investigación matemática.
G6.- Capacidades de comunicación. Ser capaz de presentar, de forma oral y escrita, y tanto ante públicos especializados como no especializados, resultados avanzados de investigación en Matemáticas, teniendo en cuenta los antecedentes en la investigación, las hipótesis de trabajo, los desarrollos y las conclusiones.
G7.- Capacidad de trabajo en equipo. Capacidad para el desarrollo de una actividad matemática dentro de un equipo de investigación, bajo supervisión o de forma autónoma, pero al servicio de un proyecto investigador común, que puede ser multidisciplinar.
G9.- Desarrollar el interés por la formación permanente. Promover un interés permanente para ampliar conocimientos y el desarrollo de un perfil profesional específico, mediante el estudio, la reflexión y la investigación.
G10.- Capacidad de aprendizaje autónomo. Adquirir las destrezas necesarias para el aprendizaje autónomo en el ámbito de las Matemáticas, conociendo las fuentes de conocimiento para dicho aprendizaje y su utilización, y motivando el aprendizaje a lo largo de la vida en el ejercicio de la actividad matemática.
E1.- Adquisición de destrezas técnicas generales en el ámbito de una o varias disciplinas Matemáticas. Comprende esta competencia la capacidad de utilización de forma profesional del lenguaje y de las técnicas avanzadas propias de algunas de las especialidades de las Matemáticas, para favorecer la interpretación fluida de las fuentes especializadas de dichas disciplinas y la formulación adecuada de nuevos problemas en el ámbito de dicha especialidad.
E2.- Capacidad de comprensión de las bases teóricas y técnicas en las que se apoyan los conceptos y métodos de las materias propias de alguna de las especialidades de las Matemáticas. Comprende esta competencia la adquisición del corpus teórico que sustenta los conceptos y métodos de las materias propias de alguna de las especialidades de las Matemáticas, y la capacidad para un manejo experto y fluido de dichos conocimientos.
E4.- Capacidad y destrezas para la gestión de las fuentes de la investigación en Matemáticas. Comprende esta competencia la capacidad del estudiante para la búsqueda y gestión de documentación y bibliografía especializada, en el ámbito específico de la especialización en Matemáticas que le sea propia; el uso racional y crítico de ésta para determinar el estado del arte en un determinado problema, y el dominio de los recursos bibliográficos pertinentes.
E5.- Capacidad de aplicar y adaptar los modelos teóricos y las técnicas específicas tanto a problemas abiertos en su línea de especialización, como a problemas provenientes de otros ámbitos ya sean científicos o técnicos.
Competencia para adaptar los modelos teóricos propios de cada una de las disciplinas de las Matemáticas para el estudio de problemas abiertos relacionados o para el análisis de otros problemas provenientes de los ámbitos científicos y tecnológicos.

E6.- Capacidad de analizar problemas, detectando el posible uso de modelos matemáticos para contribuir a su comprensión y resolución. Comprende esta competencia la capacidad analítica frente a nuevas situaciones para identificar la aplicación de modelos matemáticos, existentes o de nuevo diseño, que contribuyan a la comprensión y solución de los problemas planteados.
E7.- Capacidad de defender trabajos de investigación avanzados en el ámbito de sus líneas de especialización así como de mantener debates científicos sobre los mismos, ya sean estos propios o adquiridos. Capacidad estrechamente vinculada a la competencia de una buena comunicación científica, en el ámbito propio de la especialización adquirida, tanto para defender las tesis propias como para debatir con juicio crítico con terceros, en una relación entre pares.
E8.- Capacidad de discernir entre las diferentes orientaciones de las técnicas específicas que concurren en la comprensión y resolución de un problema, comprendiendo la oportunidad y el uso de cada una de ellas individualmente así como la cooperación entre ellas de cara a la resolución global del problema.
E9.- Capacidad de comprender nuevos avances y perspectivas científicas en el ámbito de la investigación en las líneas de su especialización. Competencia para comprender la formulación de nuevos avances, en el ámbito de la investigación propio de cada disciplina de las Matemáticas, y las perspectivas que plantean.
E10.- Capacidad de detectar líneas de trabajo e investigación emergentes en al ámbito de las Matemáticas o de sus aplicaciones, identificando la relación, origen e influencia con el estado de conocimiento propio de cada una de las especializaciones de las Matemáticas. Competencia para reconocer líneas de investigación emergentes en el ámbito de las Matemáticas o de sus aplicaciones, identificando las interrelaciones existentes con cada una de las especialidades.
E16.- Adquirir una visión global y comprensiva de la Investigación en Matemáticas. Comprende esta competencia la adquisición de una visión global de la investigación en Matemáticas, que valore la complementariedad de los enfoques matemáticos propios de cada disciplina para avanzar en el conocimiento, así como el estado actual de las líneas de investigación más activas en cada una de las áreas de conocimiento de las Matemáticas.
E17.- Adquirir recursos y destrezas para la comunicación de resultados de investigación en Matemáticas de forma clara, ante audiencias especializadas y no especializadas.

Objetivos/Resultados de aprendizaje

Estudio científico y técnico en profundidad, y utilización práctica, de los protocolos criptográficos de mayor uso en criptografía en los sectores de firma digital, comercio electrónico o elecciones y votaciones electrónicas, así como los protocolos técnicos de acuerdo y transporte de llaves, de autentificación o de compartición de secretos. A la vez revisar las técnicas matemáticas necesarias de aritmética entera y modular, cálculo polinómico y computación simbólica, en las que se fundamenta la criptografía contemporánea y la transmisión, con seguridad, de la información electrónica.

Contenidos

Revisión de aritmética modular. Conceptos y métodos de la criptografía. Esquemas criptográficos de clave pública. Protocolos de acuerdo y transporte de claves. Protocolos de autentificación. Protocolos de firma digital. Protocolos de votaciones electrónicas. Protocolos de comercio electrónico. Sistemas para compartir secretos.

Principios Metodológicos/Métodos Docentes

Clases expositivas, clases de problemas, clases interactivas, prácticas y tutorías.

Criterios y sistemas de evaluación

Trabajo individualizado escrito hasta el 50%. Trabajo individualizado expuesto hasta el 50%. Examen final hasta el 100%.

Recursos de aprendizaje y apoyo tutorial

El profesor aportará textos concretos explicados de una parte significativa de la asignatura. También aportará secuencialmente textos, enlaces electrónicos y artículos de investigación que sean de referencia para los contenidos del curso.

Calendario y horario

El que ha programado la Escuela para el primer semestre académico y que figura en la web www.cie.uva.es, en el horario que ha programado la coordinación del máster.

Tabla de Dedicación del Estudiante a la Asignatura/Plan de Trabajo

La habitual en cursos de interacción Informática-Matemáticas con seguimiento personalizado, con pruebas y entregas a lo largo del curso.

Responsable de la docencia (recomendable que se incluya información de contacto y breve CV en el que aparezcan sus lineas de investigación y alguna publicación relevante)

Consultar la página web del Profesor Antonio Campillo López http://www.singacom.uva.es/oldsite/campillo/index_es.html

Idioma en que se imparte

Español. Individualizadamente tamién en francés o en inglés