

Facultad de Ciencias

GUÍA DOCENTE DE LA ASIGNATURA

346 - Criptología

Máster Universitario en Matemáticas y Computación
Optativa. Curso 1

Curso Académico 2023-2024

1. DATOS IDENTIFICATIVOS

| | | | |
|--------------------------|---|----------------------|-------------------|
| Título/s | Máster Universitario en Matemáticas y Computación | Tipología v Curso | Optativa. Curso 1 |
| Centro | Facultad de Ciencias | | |
| Módulo / materia | ÁLGEBRA Y GEOMETRÍA | | |
| Código y denominación | 346 - Criptología | | |
| Créditos ECTS | 3 | Cuatrimestre | Cuatrimestral (1) |
| Web | | | |
| Idioma de impartición | Español | English friendly | No |
| | | Forma de impartición | Presencial |

| | |
|----------------------|--|
| Departamento | DPTO. MATEMATICA APLICADA Y CIENCIAS DE LA COMPUTACION |
| Profesor responsable | JAIME GUTIERREZ GUTIERREZ |
| E-mail | jaime.gutierrez@unican.es |
| Número despacho | E.T.S. de Ingenieros Industriales y de Telecomunicación. Planta: - 4. DESPACHO (S4041) |
| Otros profesores | |

2. CONOCIMIENTOS PREVIOS

Algebra lineal
Teoría de grupos, anillos y cuerpos
Conocimientos de programación

3. COMPETENCIAS GENÉRICAS Y ESPECÍFICAS DEL PLAN DE ESTUDIOS TRABAJADAS

| |
|--|
| Competencias Genéricas |
| Conocimiento actualizado de las áreas más activas en ámbitos relacionados con Matemáticas, Computación o la interacción de ambas |
| Competencias Específicas |
| Conocer resultados avanzados y conocer y comprender problemas abiertos de Matemáticas y/o Computación para su iniciación a la investigación. |
| Conocer cómo modelizar matemáticamente situaciones prácticas provenientes de problemas de Ciencia, Ingeniería o Ciencias Sociales |
| Aplicar, analizar, diseñar y/o implementar algoritmos eficientes orientados a situaciones que admiten una modelización matemática. |
| Competencias Básicas |
| Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación |
| 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 |
| 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 |
| Competencias Transversales |
| Que perfeccionen su competencia digital y, en general, sus habilidades para buscar, obtener, seleccionar, tratar, analizar y comunicar informaciones diversas, así como para transformarlas en conocimiento y ofrecerlo a la consideración de los demás. |
| Que cultiven su capacidad de aprendizaje autónomo, además de las competencias interpersonales relacionadas con el trabajo en equipo, la colaboración grupal en contextos social y culturalmente diversos, la capacidad crítica y autocrítica, y la auto-regulación emocional. |
| Exposición y presentación pública del trabajo mediante una comunicación efectiva. |

3.1 RESULTADOS DE APRENDIZAJE

-El alumno ha adquirido la suficiente información y destreza para desarrollar las competencias.

4. OBJETIVOS

Entender los principios básicos de las técnicas criptográficas: el cifrado-descifrado tanto simétrico como asimétrico, técnicas de criptoanálisis, las funciones hash criptográficas, firma digital, etc. Analizar (complejidad y programación) los algoritmos más importantes de estas técnicas. Conocer y comprender los estándares más aceptados.

5. MODALIDADES ORGANIZATIVAS Y MÉTODOS DOCENTES

| ACTIVIDADES | HORAS DE LA ASIGNATURA |
|---|------------------------|
| ACTIVIDADES PRESENCIALES | |
| HORAS DE CLASE (A) | |
| - Teoría (TE) | 20 |
| - Prácticas en Aula (PA) | |
| - Prácticas de Laboratorio Experimental(PLE) | |
| - Prácticas de Laboratorio en Ordenador (PLO) | 10 |
| - Prácticas Clínicas (CL) | |
| Subtotal horas de clase | 30 |
| ACTIVIDADES DE SEGUIMIENTO (B) | |
| - Tutorías (TU) | 8 |
| - Evaluación (EV) | 7 |
| Subtotal actividades de seguimiento | 15 |
| Total actividades presenciales (A+B) | 45 |
| ACTIVIDADES NO PRESENCIALES | |
| Trabajo en grupo (TG) | |
| Trabajo autónomo (TA) | 30 |
| Tutorías No Presenciales (TU-NP) | |
| Evaluación No Presencial (EV-NP) | |
| Total actividades no presenciales | 30 |
| HORAS TOTALES | 75 |

6. ORGANIZACIÓN DOCENTE

| CONTENIDOS | | TE | PA | PLE | PLO | CL | TU | EV | TG | TA | TU-NP | EV-NP | Semana |
|---|--|-------|------|------|-------|------|------|------|------|-------|-------|-------|--------|
| 1 | <p>TEMA 1. Sistemas criptográficos simétricos(DES, AES, cifrado en flujo, hash y blockchain y asimétricos (RSA, mochila, curvas elípticas,).</p> <p>TEMA 2. Protocolos criptográficos(funciones hash criptográficas, firma digital, intercambio de claves, blockchain....).</p> <p>TEMA 3. Criptoanálisis(retículas, sistemas de ecuaciones polinomiales, ...).</p> <p>TEMA 4. Complejidad y programación de los algoritmos más importantes en criptología.</p> <p>TEMA 5. A collusion-resistant identity-based scheme for symmetric key generation</p> | 20,00 | 0,00 | 0,00 | 10,00 | 0,00 | 8,00 | 7,00 | 0,00 | 30,00 | 0,00 | 0,00 | 1-7 |
| TOTAL DE HORAS | | 20,00 | 0,00 | 0,00 | 10,00 | 0,00 | 8,00 | 7,00 | 0,00 | 30,00 | 0,00 | 0,00 | |
| Esta organización tiene carácter orientativo. | | | | | | | | | | | | | |

| | |
|-------|--|
| TE | Horas de teoría |
| PA | Horas de prácticas en aula |
| PLE | Horas de prácticas de laboratorio experimental |
| PLO | Horas de prácticas de laboratorio en ordenador |
| CL | Horas de prácticas clínicas |
| TU | Horas de tutoría |
| EV | Horas de evaluación |
| TG | Horas de trabajo en grupo |
| TA | Horas de trabajo autónomo |
| TU-NP | Tutorías No Presenciales |
| EV-NP | Evaluación No Presencial |

7. MÉTODOS DE LA EVALUACIÓN

| Descripción | Tipología | Eval. Final | Recuper. | % |
|--|--|-------------|----------|---------------|
| Evaluación continua | Otros | No | No | 20,00 |
| Calif. mínima | 0,00 | | | |
| Duración | | | | |
| Fecha realización | A lo largo del curso | | | |
| Condiciones recuperación | | | | |
| Observaciones | Consistirán en entrega de ejercicios y programas a lo largo del curso. Los ejercicios que deben resolver en este tipo de pruebas surgen durante el desarrollo de las clases presenciales y, deben ser resueltas en el citado contexto. Por tanto, son pruebas que por su estructura no admiten recuperación. | | | |
| Trabajo de la asignatura | Trabajo | No | Sí | 80,00 |
| Calif. mínima | 0,00 | | | |
| Duración | | | | |
| Fecha realización | Hasta fecha anunciada al principio de curso, cercana al final del curso | | | |
| Condiciones recuperación | | | | |
| Observaciones | Se podrá recuperar volviéndolo a presentar, en la convocatoria extraordinaria. | | | |
| TOTAL | | | | 100,00 |
| Observaciones | | | | |
| Criterios de evaluación para estudiantes a tiempo parcial | | | | |
| Los alumnos matriculados a tiempo parcial deberán realizar un examen final en laboratorio. | | | | |

8. BIBLIOGRAFÍA Y MATERIALES DIDÁCTICOS

| BÁSICA |
|---|
| -Stinson, Douglas R. Cryptography, theory and practice. CRC Press Series on Discrete Mathematics and its Applications, 1996 . |
| -Jaime Gutierrez y Juan Tena. Protocolos Criptograficos y seguridad en redes. Servicio de publicaciones Universidad de Cantabria, 2003. |
| -D. Micciancio and S. Goldwasser. Complexity of Lattices Problems, The Kluwer International Series in Engineering and Computer Science, vol. 671, 2002. |
| Complementaria |
| -B. Schneider. Applied Cryptography. J. Wiley, 1994. |
| - Diversos artículos e informes científicos. |
| - T. Cormen, C. Leiserson, R. Rivest, C. Stein: "Introduction to Algorithms". MIT press. |

9. SOFTWARE

| PROGRAMA / APLICACIÓN | CENTRO | PLANTA | SALA | HORARIO |
|--------------------------------------|--------------|--------|------|---------|
| Sage | Industriales | | | |
| Diverso software criptográfico libre | | | | |

10. COMPETENCIAS LINGÜÍSTICAS

- | | |
|---|---|
| <input checked="" type="checkbox"/> Comprensión escrita | <input type="checkbox"/> Comprensión oral |
| <input checked="" type="checkbox"/> Expresión escrita | <input type="checkbox"/> Expresión oral |
| <input type="checkbox"/> Asignatura íntegramente desarrollada en inglés | |

Observaciones