



ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA

GUIA DOCENTE



CURSO 2019/2020

Máster en Ingeniería Informática (Plan 2018)

DATOS DE LA ASIGNATURA

Nombre:

Criptografía

Denominación en inglés:

Cryptography

Código:

1180422

Carácter:

Optativo

Horas:

Totales

Presenciales

No presenciales

Trabajo estimado:

75

30

45

Créditos:

Grupos reducidos

Grupos grandes

Aula estándar

Laboratorio

Prácticas de campo

Aula de informática

1.8

0.6

0

0

0.6

Departamentos:

Áreas de Conocimiento:

Ciencias Integradas

Matemática Aplicada

Curso:

Cuatrimestre:

1º - Primero

Segundo cuatrimestre

DATOS DE LOS PROFESORES

Nombre:

E-Mail:

Teléfono:

Despacho:

*Lozano Palacio, Antonio
José

antonio.lozano@dmate.uhu.es

959219921

Facultad de Ciencias
Experimentales, despacho
3.3.11

García Selfa, Irene

irene.garcia@dmate.uhu.es

959219930

Campus de El Carmen,
Facultad de Ciencias
Experimentales Módulo 3,
Planta 3, Despacho 10

*Profesor coordinador de la asignatura

[Consultar los horarios de la asignatura](#)

1. Descripción de contenidos**1.1. Breve descripción (en castellano):**

- Sistemas clásicos de cifrado: sistemas de la antigüedad. Cifradores del siglo XIX. Máquinas de cifrar del siglo XX.
- Aritmética modular: algoritmo de Euclides, teorema chino del resto, función de Euler. Factorización de números enteros.
- Sistemas de cifrado de clave pública: funciones de un solo sentido. Autenticación. Algunos algoritmos de clave pública.
- Sistemas de cifrado simétrico: sistemas simétricos. Cifrados de tipo Feistel. Algunos algoritmos de cifrado simétrico.
- Funciones resumen: definición de función resumen. Algunos algoritmos para la generación de resúmenes. Aplicaciones.
- Mecanismos y servicios de seguridad: autenticación y no repudio. Firma digital. Certificados X.509. SSSL, SET, TLS.
- Otras aplicaciones.

1.2. Breve descripción (en inglés):

- Classical ciphers: antique systems. 19th-century ciphers. 20th-century cipher machines.
- Modular arithmetic: Euclidean algorithm, chinese remainder theorem, Euler's totient function. Integer factorization.
- Public key cryptography systems: one-way functions. Authentication. Some public key algorithms.
- Symmetric cryptography systems. Feistel ciphers. Some symmetric key algorithms.
- Hash functions: definition. Some hashing algorithms. Applications.
- Mechanisms and security services: authentication and non-repudiation. Digital signature. X.509 certificates. SSL, SET, TLS.
- Other applications.

2. Situación de la asignatura**2.1. Contexto dentro de la titulación:**

La asignatura Criptografía se imparte en el segundo cuatrimestre del Máster en Ingeniería Informática. La necesidad de ocultar información a destinatarios no autorizados ha contribuido decisivamente al desarrollo de la Criptografía, cuyo objetivo principal es el desarrollo de algoritmos que permitan garantizar la confidencialidad e integridad del mensaje, así como la autenticación de remitente.

En los últimos años los ordenadores han pasado de ser instrumentos relativamente aislados, a formar parte de una intrincada red global de comunicaciones que conocemos como Internet. Las transacciones bancarias y el pago de impuestos a través de Internet, el uso del correo electrónico y el comercio electrónico son ejemplos de actividades cada vez más habituales que requieren el intercambio de una gran cantidad de información y de datos personales que no deberían caer en manos de terceras personas. Se hace por tanto imprescindible, para el ejercicio de la profesión de Ingeniería Informática, el poseer conocimientos sobre las técnicas criptográficas más comunes que permiten garantizar el intercambio seguro de información.

2.2. Recomendaciones:

Para cursar con éxito la asignatura Criptografía es imprescindible trabajar de manera continua para adquirir soltura en el manejo de las herramientas y poder asimilar los nuevos conceptos.

3. Objetivos (Expresados como resultados del aprendizaje):

Resultados de aprendizaje.

Con esta asignatura el alumno tendrá conocimiento de la historia, la terminología y las bases de la Criptografía. Asimismo dominará las técnicas criptográficas más comunes que permiten garantizar el intercambio seguro de información, aprenderá el funcionamiento de los protocolos criptográficos más utilizados en la actualidad, así como a implementar algoritmos de cifrado y autenticación, y también el funcionamiento de una infraestructura de clave pública.

Competencias específicas:

- Conocimiento de los métodos matemáticos básicos en los que se fundamentan los principales algoritmos criptográficos.
- Capacidad para seleccionar los criptosistemas más adecuados en cada situación e implementarlos de manera segura.

4. Competencias a adquirir por los estudiantes**4.1. Competencias específicas:**

4.2. Competencias básicas, generales o transversales:

- **CB6:** 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
- **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
- **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
- **CG4:** Capacidad para el modelado matemático, cálculo y simulación en centros tecnológicos y de ingeniería de empresa, particularmente en tareas de investigación, desarrollo e innovación en todos los ámbitos relacionados con la Ingeniería en Informática.
- **CG8:** Capacidad para la aplicación de los conocimientos adquiridos y de resolver problemas en entornos nuevos o poco conocidos dentro de contextos más amplios y multidisciplinarios, siendo capaces de integrar estos conocimientos
- **CT1:** Gestionar adecuadamente la información adquirida expresando conocimientos avanzados y demostrando, en un contexto de investigación científica y tecnológica o altamente especializado, una comprensión detallada y fundamentada de los aspectos teóricos y prácticos y de la metodología de trabajo en el campo de estudio.
- **CT3:** Desarrollar una actitud y una aptitud de búsqueda permanente de la excelencia en el quehacer académico y en el ejercicio profesional futuro.
- **CT5:** Utilizar de manera avanzada las tecnologías de la información y la comunicación, desarrollando, al nivel requerido, las Competencias Informáticas e Informacionales ('C12).

5. Actividades Formativas y Metodologías Docentes

5.1. Actividades formativas:

- Sesiones de Teoría sobre los contenidos del Programa.
- Sesiones de Resolución de Problemas.
- Sesiones Prácticas en Laboratorios Especializados o en Aulas de Informática.
- Actividades Académicamente Dirigidas por el Profesorado: seminarios, conferencias, desarrollo de trabajos, debates, tutorías colectivas, actividades de evaluación y autoevaluación.

5.2. Metodologías docentes:

- Clase Magistral Participativa.
- Desarrollo de Prácticas en Laboratorios Especializados o Aulas de Informática en grupos reducidos.
- Resolución de Problemas y Ejercicios Prácticos.
- Tutorías Individuales o Colectivas. Interacción directa profesorado-estudiantes.
- Planteamiento, Realización, Tutorización y Presentación de Trabajos.
- Evaluaciones y Exámenes.

5.3. Desarrollo y justificación:

Tanto las sesiones académicas de teoría y problemas como las clases prácticas, que se desarrollen de manera presencial en el aula, se dedicarán principalmente a la puesta en común y la resolución de aquellas cuestiones y dudas que puedan plantear los alumnos sobre los distintos conceptos teóricos y prácticos de la asignatura. Se intentará que estas cuestiones se resuelvan de manera participativa por el alumnado, bajo la supervisión del profesor, valorando positivamente la participación activa de los alumnos en estas sesiones. Asimismo se profundizará en aquellos conceptos que, por su complejidad, puedan suponer una mayor dificultad para su aprendizaje autónomo y se resolverán problemas y ejercicios prácticos destinados a mejorar la asimilación de los conceptos teóricos. En las sesiones prácticas se hará uso de programas específicos y lenguajes de programación, conocidos por los alumnos. Se propondrá a los mismos la resolución de ejercicios, relacionados con el contenido de las prácticas, para su posterior evaluación. En las sesiones académicas teórico-prácticas y clases prácticas se trabajarán las competencias CB6, CB7, CG4, CT1, CT3 y CT5.

El carácter semipresencial del Máster hace que el trabajo individual del alumno constituya una parte importante de su aprendizaje. Por este motivo, se plantearán además distintas actividades formativas de carácter no presencial y se aplicarán diversas metodologías docentes, también no presenciales: lectura de los contenidos de los temas, entrega de ejercicios/prácticas/trabajos evaluables, actividades de autoevaluación, tutorías colectivas a través de plataformas de enseñanza virtual, trabajo individual/autónomo del estudiante, actividades no presenciales con evaluación por pares, desarrollo cooperativo de trabajos mediante herramientas de discusión asíncrona y visualización de videos que incentiven algunas de las competencias. Mediante estas actividades formativas se trabajarán las competencias CB10, CG8, CT1, CT3 y CT5.

De este modo, se propondrá a los alumnos la realización de un trabajo, relacionado con los contenidos de la asignatura, que podrán exponer, para su posterior debate y que se evaluará mediante un esquema de evaluación por pares. Se realizarán sesiones de resolución de problemas dedicadas a la resolución de ejercicios, por parte de los alumnos, que deberán entregar para su valoración. En función del desarrollo del curso, estas sesiones podrían realizarse telemáticamente, mediante la plataforma Moodle. Si la disponibilidad del material lo permite, se pondrá también a disposición de los alumnos material adicional (videos, artículos, entrevistas, etc.) que ayuden a alcanzar los objetivos de la asignatura. Mediante estas actividades se trabajarán las competencias CB9, CB10, CG4, CG8, CT1, CT3 y CT5.

Finalmente, se habilitarán foros en el espacio de la asignatura, en la plataforma Moodle, para tratar cuestiones relacionadas con los fundamentos teóricos y/o prácticos de la asignatura y la puesta en común de cuestiones y dudas que puedan surgir al margen de las tratadas en las clases magistrales, y se fomentará el trabajo colaborativo entre los alumnos. Mediante estas actividades se trabajarán las competencias CB9, CB10, CT1, CT3 y CT5.

6. Temario desarrollado:

Tema 1: INTRODUCCIÓN.

- 1.1. Seguridad.
- 1.2. Criptografía.
- 1.3. Criptoanálisis.

Tema 2: SISTEMAS CLÁSICOS.

- 2.1. Sistemas de la antigüedad.
- 2.2. Cifradores del siglo XIX.
- 2.3. Máquinas de cifrar del siglo XX.

Tema 3. ARITMÉTICA MODULAR.

- 3.1. Algoritmo de Euclides.
- 3.2. Ecuaciones diofánticas.
- 3.3. Teorema chino del resto.
- 3.4. Inversos en $\mathbb{Z}_n$. Función de Euler.
- 3.5. Factorización de números enteros.

Tema 4. SISTEMAS DE CLAVE PÚBLICA.

- 4.1. Cifrado de clave pública.
- 4.2. Funciones de un sólo sentido.
- 4.3. Autentificación.
- 4.4. Algunos algoritmos de clave pública: RSA, Diffie Hellman, El Gamal, Rabin, etc.

Tema 5. SISTEMAS DE CIFRADO SIMÉTRICO.

- 5.1. Sistemas simétricos.
- 5.2. Cifrado Feistel.
- 5.3. Algoritmos DES, TDES.
- 5.4. Algoritmo Rijndael.
- 5.5. Modos de operación.

Tema 6. FUNCIONES RESUMEN.

- 6.1. Definición de función resumen.
- 6.2. Algoritmos para la generación de resúmenes: MD5, SHA-1, etc.
- 6.3. Aplicaciones.

Tema 7. MECANISMOS Y SERVICIOS DE SEGURIDAD.

- 7.1. Autentificación y no repudio.
- 7.2. Firma digital.
- 7.3. Certificados X.509.
- 7.4. PEM.
- 7.5. S/MIME.
- 7.6. SSL, SET, TLS.

TEMA 8. OTRAS APLICACIONES.

- 8.1. Tarjetas inteligentes.
- 8.2. Telecomunicaciones.

7. Bibliografía

7.1. Bibliografía básica:

- De Miguel García, R., CRIPTOGRAFÍA CLÁSICA Y MODERNA, Septem Ediciones, 2009.
- Delfs, H., Helmut, K., INTRODUCTION TO CRYPTOGRAPHY: PRINCIPLES AND APPLICATIONS, Ed. Springer, 2007.
- Ferguson, N., Schneier, B. PRACTICAL CRYPTOGRAPHY. Ed. Wiley. 2003.
- Hoffstein, J., AN INTRODUCTION TO MATHEMATICAL CRYPTOGRAPHY, Ed. Springer, 2008.
- Katz, J., INTRODUCTION TO MODERN CRYPTOGRAPHY, Chapman & Hall/CRC, 2008.
- Menezes, A. J., Van Oorschot, P.C., Vanstone, S. A. HANDBOOK OF APPLIED CRYPTOGRAPHY. CRC Press. 1996. (<http://cacr.uwaterloo.ca/hac/>).
- St. Denis, T., Johnson, S., CRYPTOGRAPHY FOR DEVELOPERS, Rockland, MA: Syngress Publishing, Inc, 2007.
- Stallings, W. CRYPTOGRAPHY AND NETWORK SECURITY: PRINCIPLES AND PRACTICE, 3rd edition. Prentice Hall. 2002.
- Stinson, D. CRYPTOGRAPHY: THEORY AND PRACTICE. Chapman & Hall/CRC. 2002.
- Apuntes proporcionados por los profesores a través de la plataforma Moodle.

7.2. Bibliografía complementaria:

- Schneier, B. APPLIED CRYPTOGRAPHY: PROTOCOLS, ALGORITHMS AND SOURCE CODE IN C, 2nd edition, JohnWiley & Sons, 1996.
- Welschenbach, M., Kramer D. CRYPTOGRAPHY IN C AND C++. Apress; Bk&CD-Rom edition, 2001.

8. Sistemas y criterios de evaluación.

8.1. Sistemas de evaluación:

- Examen de teoría/problemas
- Defensa de Prácticas
- Defensa de Trabajos e Informes Escritos
- Seguimiento Individual del Estudiante

8.2. Criterios de evaluación y calificación:

Sistema de evaluación continua: aquellos alumnos que no soliciten su evaluación en acto único serán evaluados, en las distintas convocatorias, como se indica a continuación.

- **Convocatoria I.** Seguirá, por defecto, un esquema de evaluación continua: durante el curso se propondrá a los alumnos la realización de, entre dos y cuatro prácticas, consistentes en la implementación de algoritmos criptográficos, similares a los explicados en las clases de teoría, en un lenguaje de programación que sea conocido por ellos. Asimismo, se realizarán pruebas de evaluación, mediante la plataforma Moodle, que versarán sobre aspectos teórico-prácticos del temario, un examen de teoría-problemas, en la fecha establecida por la E.T.S.I. y se valorará la participación activa en las distintas actividades, foros, clases presenciales, etc. La ponderación de cada una de estas pruebas y las competencias evaluadas con cada una de ellas, son las que se muestran a continuación:
- Calificación obtenida en el examen de teoría-problemas (35%). (CG4, CG8, CB7, CB9, CT1, CT3).
- Defensa de las prácticas propuestas (30%). (CG8, CB6, CB7, CB9, CB10, CT1, CT5).
- Pruebas de evaluación realizadas a través de la plataforma Moodle: (25%). (CG4, CG8, CB7).
- Participación activa en las distintas actividades, foros, clases presenciales, etc. (10%). (CB7, CB9, CT1, CT3, CT5).

De este modo, la calificación global se calculará como $\text{calif. global} = 0.35 \cdot \text{calif. examen de teoría-problemas} + 0.3 \cdot \text{calif. prácticas} + 0.25 \cdot \text{calif. pruebas de evaluación} + 0.1 \cdot \text{participación}$.

- **Convocatorias II y III.** Los alumnos deberán realizar un examen de teoría-problemas en la fecha fijada por la E.T.S.I. y entregar, antes del comienzo del examen y en soporte informático adecuado, las prácticas que se hubieran propuesto durante el curso. Asimismo, las actividades evaluables correspondientes a las *pruebas de evaluación realizadas a través de Moodle* y la *participación activa en las actividades* se sustituirán por una prueba tipo test sobre cuestiones teórico-prácticas relacionadas con los contenidos de la asignatura. La ponderación de cada una de estas pruebas y las competencias evaluadas con cada una de ellas, son las que se muestran a continuación:
- Calificación obtenida en el examen de teoría-problemas (35%). (CG4, CG8, CB7, CB9, CT1, CT3).
- Defensa de las prácticas propuestas (30%). (CG8, CB6, CB7, CB9, CB10, CT1, CT5).
- Cuestionario teórico-práctico: (35%). (CG4, CG8, CB7, CT1, CT3, CT5).

De este modo, la calificación global se calculará como $\text{calif. global} = 0.35 \cdot \text{calif. examen de teoría-problemas} + 0.3 \cdot \text{calif. prácticas} + 0.35 \cdot \text{calif. cuestionario}$.

Sistema de evaluación única final. En cada convocatoria, aquellos alumnos que soliciten su evaluación en acto único, de acuerdo a las normas establecidas en la normativa de evaluación de la Universidad de Huelva, deberán realizar un examen de teoría-problemas en la fecha fijada por la E.T.S.I. y entregar, antes del comienzo del examen y en soporte informático adecuado, las prácticas que se hubieran propuesto durante el curso. Las actividades evaluables correspondientes a las *pruebas de evaluación realizadas a través de Moodle* y la *participación activa en las actividades* se sustituirán por una prueba tipo test sobre cuestiones teórico-prácticas relacionadas con los contenidos de la asignatura. La ponderación de cada una de estas pruebas y las competencias evaluadas con cada una de ellas serán las ya indicadas en el punto dedicado a las convocatorias II y III. Con objeto de que, aquellos alumnos que así lo deseen, puedan solicitar su evaluación en acto único se habilitará una encuesta en Moodle que estará activa las dos primeras semanas del cuatrimestre. Transcurrido este plazo aquellos alumnos que, por alguna de las causas excepcionales y sobrevenidas descritas en la normativa de evaluación, deseen acogerse a la modalidad de evaluación única, tendrán que entregar una solicitud firmada a los profesores de la asignatura.

Siempre que el alumno no se manifieste en sentido contrario, la superación (calificación igual o superior a 5 puntos) de alguna de las partes (teoría-problemas / prácticas / evaluación a través de Moodle-participación en actividades / cuestionario) en la convocatoria I, será efectiva también en la convocatoria II y con la misma calificación. No se guardarán, para la convocatoria III, partes aprobadas en las convocatorias I y/o II. Tampoco se guardarán de un curso académico a otro.

- **Convocatoria extraordinaria para la finalización del título.** Se realizará en las mismas condiciones que las convocatorias II y III si bien, en este caso, el alumno deberá entregar las prácticas propuestas en el curso inmediatamente anterior a la fecha de realización del examen extraordinario.

Para la obtención de la calificación "Matrícula de Honor" será condición necesaria, que no suficiente, la obtención de una calificación global ponderada igual o superior a 9.5 puntos. Para su concesión se atenderá, en primer lugar, a la nota global ponderada obtenida por los alumnos candidatos y, en caso de empate entre dos o más alumnos, se concederá dicha calificación a los alumnos que hayan obtenido mayor calificación en (por este orden) el examen de teoría-problemas, ejercicios de prácticas de la asignatura, trabajos realizados durante el curso, pruebas de evaluación a través de Moodle y participación activa en las distintas actividades.

Se valorará positiva o negativamente, según proceda, el dominio de los conceptos teóricos, la interpretación de los resultados, la brevedad y claridad en la exposición, la habilidad en la aplicación de los diversos métodos prácticos y la precisión en los cálculos.

9. Organización docente semanal orientativa:

Semanas	Grupos Grandes	Grupos Reducidos	Aula Estándar	Grupos Reducidos	Aula de Informática	Grupos Reducidos	Laboratorio	Grupos Reducidos	prácticas de campo	Pruebas y/o actividades evaluables	Contenido desarrollado
#1	1	0	0	0	0	0	0	0	0	El 50 de las horas que se indican en el cronograma son no presenciales.	Tema 1.
#2	1	0	0	0	0	0	0	0	0		Tema 2.
#3	1	0	0	0	0	0	0	0	0		Tema 3.
#4	1	0	0	0	0	0	0	0	0		Tema 3.
#5	1	0	2	0	0	0	0	0	0		Tema 3, Práctica 1.
#6	2	0	0	0	0	0	0	0	0		Tema 3.
#7	1	2	0	0	0	0	0	0	0	Actividad evaluable 1.	Tema 4.
#8	1	0	0	0	0	0	0	0	0		Tema 4.
#9	2	0	2	0	0	0	0	0	0		Tema 4. Práctica 2.
#10	1	0	0	0	0	0	0	0	0		Tema 5.
#11	1	0	0	0	0	0	0	0	0		Tema 5.
#12	1	2	2	0	0	0	0	0	0	Actividad evaluable 2.	Tema 6.Práctica 3.
#13	1	0	0	0	0	0	0	0	0		Tema 6.
#14	1	0	0	0	0	0	0	0	0		Tema 7.
#15	2	2	0	0	0	0	0	0	0	Actividad evaluable 3.	Tema 8.
	18	6	6	0	0	0	0	0	0		