ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA

GUIA DOCENTE

CURSO 2023-24

MÁSTER UNIVERSITARIO EN INGENIERÍA INFORMÁTICA

DATOS DE LA ASIGNATURA

Nombre:
CRIPTOGRAFÍA
Denominación en Inglés:
Criptography

Código:	**Tipo Docencia:**	**Carácter:**
1230422	Semipresencial	Optativa

Horas:

	Totales	**Presenciales**	**No Presenciales**
Trabajo Estimado	75	15	60

Créditos:

Grupos Grandes	**Grupos Reducidos**			
	Aula estándar	**Laboratorio**	**Prácticas de campo**	**Aula de informática**
1.8	0.6	0	0	0.6

Departamentos:	**Áreas de Conocimiento:**
CIENCIAS INTEGRADAS	MATEMATICA APLICADA
Curso:	**Cuatrimestre**
2º - Segundo	Primer cuatrimestre

DATOS DEL PROFESORADO (*Profesorado coordinador de la asignatura)

Nombre:	E-mail:	Teléfono:
* Antonio Jose Lozano Palacio	antonio.lozano@dmat.uhu.es	959 219 921
Irene Garcia Selfa	irene.garcia@dmat.uhu.es	959 219 930

Datos adicionales del profesorado (Tutorías, Horarios, Despachos, etc...)

Nombre	Despacho
Antonio José Lozano Palacio	Facultad de Ciencias Experimentales, despacho 3.3.11.
Irene García Selfa	Facultad de Ciencias Experimentales, despacho 3.3.10.
Horarios de tutorías: ver espacio Moodle de la asignatura. Alternativamente pueden encontrarse en http://www.uhu.es/etsi/informacion-academica/informacion-comun-todos-los-titulos/horarios-2/	

DATOS ESPECÍFICOS 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. Autentificación. 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: autentificación 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. Autentication. Some public key algorithms.
- Symmetric cryptography systems. Feistel ciphers. Some symmetric key algorithms.
- Hash functions: definition. Some hashing algorithms. Applications.
- Mechanisms and security services: autentication 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 primer cuatrimestre del segundo curso 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 autentificación del 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 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 (resultado del aprendizaje, y/o habilidades o destrezas y conocimientos):

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 y aprenderá el funcionamiento de los protocolos criptográficos más utilizados en la actualidad, asi como a implementar algoritmos de cifrado y autentificación, y también el funcionamiento de una infraestructura de clave pública.

Conocimientos/Contenidos: conoce los mecanismos necesarios para poder generar una interacción hombre-máquina adecuada, las tecnologías de identificación de usuarios, así como los periféricos necesarios para las mismas (C14).

Habilidades o destrezas: Maneja los conceptos de seguridad desde un punto de vista hardware y un punto de vista software (HD12).

4. Competencias a adquirir por los estudiantes

4.1 Competencias específicas:

-

4.2 Competencias básicas, generales o transversales:

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.

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

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 mulitidisciplinares, siendo capaces de integrar estos conocimientos.

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.

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.

CT5: Utilizar de manera avanzada las tecnologías de la información y la comunicación, desarrollando, al nivel requerido, las Competencias Informáticas e Informacionales (CI2).

CT3: Desarrollar una actitud y una aptitud de búsqueda permanente de la excelencia en el quehacer académico y en el ejercicio profesional futuro.

5. Actividades Formativas y Metodologías Docentes

5.1 Actividades formativas:

- Sesiones de teoría/problemas/casos prácticos sobre los contenidos del programa

- 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

- 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 (foros, wikis, chats)

- Trabajo individual/autónomo del estudiante

- Actividades no presenciales con evaluación por pares

- Desarrollo cooperativo de trabajos utilizando herramientas de discusión asíncrona (foros, wikis, ...)

5.2 Metodologías Docentes:

- Clase magistral participativa

- Desarrollo de prácticas en laboratorios especializados o en 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

- Visualización y escuchas de sesiones grabadas de seminarios ad hoc con entrevistas a expertos en algunos temas claves de la materia o vídeos seleccionados que incentiven algunas competencias

- Tutorías en línea. Utilización de foros y otros medios de comunicación e interacción con el profesorado

- Trabajos colaborativos. Llevar a cabo una actividad basada en un objetivo común en el que el estudiante debe colaborar activamente para realizarla

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 distintintos 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.

De acuerdo a la distribución de 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, hasta un máximo de tres, 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.

La distribución prevista del número de horas dedicada a cada actividad formativa y metodología docente puede encontrarse en la memoria de verificación del título, en el enlace http://www.uhu.es/etsi/descargas/memoriasGrados/Nuevo_Master_IInformatica_Sede.pdf

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 Zn. 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. Aplicacioness.

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. Servicios de 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., Schneie, 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.

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.
- Apuntes proporcionados por los profesores a través de la plataforma Moodle.

8. Sistemas y criterios de evaluación

8.1 Sistemas de evaluación:

- Examen de teoría/problemas

- Defensa de prácticas

- Examen de prácticas

- Defensa de trabajos e informes escritos

- Pruebas de evaluación mediante plataformas de enseñanza virtual

- Participación en las actividades propuestas

8.2 Criterios de evaluación relativos a cada convocatoria:

8.2.1 Convocatoria I:

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, con objeto de evaluar la evolución de los conocimientos adquiridos durante el curso, se realizarán a lo largo del mismo un máximo de tres pruebas cortas de evaluación -mediante la plataforma Moodle- que versarán sobre aspectos teórico prácticos del temario. Se realizará también 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 en la calificación global del alumno 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 cortas de evaluación mediante plataforma de enseñanza virtual: (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 calif. global= 0.35*calif. examen de teoría-problemas+0.3*calif. prácticas+0.25*calif. pruebas de evaluación+0.1*participación.

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.

En todas las convocatorias, 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.

En todas las convocatorias 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.

8.2.2 Convocatoria II:

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 calif. global= 0.35*calif. examen de teoría-problemas+0.3*calif.prácticas+0.35*calif. cuestionario

8.2.3 Convocatoria III:

Se desarrollará de acuerdo a lo indicado en la convocatoria II.

8.2.4 Convocatoria extraordinaria:

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.

8.3 Evaluación única final:

8.3.1 Convocatoria I:

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 8.2.2. 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.

8.3.2 Convocatoria II:

Se realizará de acuerdo a lo descrito en la convocatoria I.

8.3.3 Convocatoria III:

Se realizará de acuerdo a lo descrito en la convocatoria I.

8.3.4 Convocatoria Extraordinaria:

Se realizará de acuerdo a lo descrito en la convocatoria I.

9. Organización docente semanal orientativa:							
Fecha	Grupos Grandes	G. Reducidos				Pruebas y/o act. evaluables	Contenido desarrollado
		Aul. Est.	Lab.	P. Camp	Aul. Inf.		
02-10-2023	2	0	0	0	0		Temas 1 y 2.
09-10-2023	1	0	0	0	1		Tema 3, Práctica 1.
16-10-2023	1	0	0	0	1		Tema 3.
23-10-2023	1	1	0	0	0	Actividad evaluable 1	Tema 4.Práctica 2.
30-10-2023	2	0	0	0	0		Tema 4 y 5.
06-11-2023	1	1	0	0	0	Actividad evaluable 2	Temas 5 y 6.
13-11-2023	1	0	0	0	1		Temas 7 y 8. Práctica 3.
20-11-2023	0	1	0	0	0	Actividad evaluable 3	
27-11-2023	0	0	0	0	0		
04-12-2023	0	0	0	0	0		
11-12-2023	0	0	0	0	0		
18-12-2023	0	0	0	0	0		
08-01-2024	0	0	0	0	0		
15-01-2024	0	0	0	0	0		
22-01-2024	0	0	0	0	0		
TOTAL	**9**	**3**	**0**	**0**	**3**		