ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA

GUIA DOCENTE

CURSO 2016/2017

Máster Oficial en Ingeniería Informática

DATOS DE LA ASIGNATURA			
Nombre:			
Criptografía			
Denominación en inglés:			
Criptography			
Código:		**Carácter:**	
1140219		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:**
2º - Segundo	Primer cuatrimestre

DATOS DE LOS PROFESORES			
Nombre:	**E-Mail:**	**Teléfono:**	**Despacho:**
*Lozano Palacio, Antonio José	antonio.lozano@dmat.uhu.es	959219921	Facultad de Ciencias Experimentales, despacho 3.3.11

*Profesor coordinador de la asignatura

Consultar los horarios de la asignatura

DATOS ESPECÍFICOS DE LA ASIGNATURA

1. Descripción de contenidos

1.1. Breve descripción (en castellano):

Bloque I. Generalidades.

Tema 1: INTRODUCCIÓN.
Tema 2: SISTEMAS CLÁSICOS.
Tema 3: ARITMÉTICA MODULAR.

Bloque II.Criptosistemas asimétricos

Tema 5: SISTEMAS DE CLAVE PÚBLICA.

Bloque III. Criptosistemas simétricos.

Tema 4: SISTEMAS DE CIFRADO SIMÉTRICO.

Bloque IV. Aplicaciones.

Tema 6: FUNCIONES RESUMEN. FIRMA DIGITAL.
Tema 7: MECANISMOS Y SERVICIOS DE SEGURIDAD.
Tema 8: OTRAS APLICACIONES.

1.2. Breve descripción (en inglés):

Introduction, classical ciphers, modular arithmetic. Public key cryptography systems. Symmetric cryptography systems. Hash functions, digital signature, mechanisms and security services. 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 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 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 hoy 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 en 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):

- Conocimiento de la historia, la terminología y las bases de la criptografía.
- Adquirir por parte del alumno conocimientos sobre criptosistemas clásicos y sistemas de cifrado simétricos y asimétricos, así como aplicaciones de la criptografía.
- Dominio de las técnicas criptográficas más comunes que permiten garantizar el intercambio seguro de información.
- Seleccionar los criptosistemas más adecuados para cada situación e implementarlos de manera segura
- Saber implementar algoritmos de cifrado y autentificación, así como el funcionamiento de una infraestructura de clave pública.
- Conocimiento del funcionamiento de diferentes protocolos criptográficos que se utilizan en la actualidad.

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
- **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 mulitidisciplinares, siendo capaces de integrar estos conocimientos

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. Metologías 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.
- Conferencias y Seminarios.
- Evaluaciones y Exámenes.

5.3. Desarrollo y justificación:

Las sesiones académicas de teoría, de 1 hora de duración, se irán desarrollando en el aula, alternando explicaciones teóricas y resolución de problemas cuando se considere oportuno. En ellas se expondrán los conceptos y procedimientos propios de la asignatura, ilustrados con ejemplos y aplicaciones.
En las sesiones prácticas, impartidas en el aula de informática, se hará uso de programas específicos y lenguajes de programación, conocidos por los alumnos, para mostrar los aspectos prácticos más relevantes de la asignatura. Se propondrá a los alumnos la resolución de ejercicios, relacionados con el contenido de las prácticas, para su posterior evaluación.
Asimismo, los alumnos podrán realizar exposiciones de los trabajos realizados durante el curso, para su posterior debate. Se usarán los recursos disponibles como pizarra, proyector de transparencias o proyector de vídeo. Se realizarán también sesiones de resolución de problemas dedicadas a la resolución de ejercicios, por parte de los alumnos, que deberán entregar para su valoración.

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.
4.2. Autentificación.
4.3. 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.
9.1. Tarjetas inteligentes.
9.2. 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., 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.
- Lucena López. M. J. CRIPTOGRAFÍA Y SEGURIDAD EN COMPUTADORES. http://sertel.upc.edu/tdatos/Libros/Lucena.pdf
- Menezes, A. J., Van Oorschot, P.C., Vanstone, S. A. HANDBOOK OF APPLIED CRYPTOGRAPHY. CRC Press. 1996. http://cacr.uwaterloo.ca/hac/
- Schneier, B. *APPLIED CRYPTOGRAPHY: PROTOCOLS, ALGORITHMS AND SOURCE CODE IN C*, 2nd edition, John Wiley & Sons, 1996.
- 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.
- Welschenbach, M., Kramer D. *CRYPTOGRAPHY IN C AND C++*. Apress; Bk&CD-Rom edition, 2001.

7.2. Bibliografía complementaria:

Apluntes proporcionados por el profesor de la asignatura a través de la plataforma de enseñanza virtual.

8. Sistemas y criterios de evaluación.

8.1. Sistemas de evaluación:

- Examen de teoría/problemas
- Defensa de Prácticas
- Defensa de Trabajos e Informes Escritos

8.2. Criterios de evaluación y calificación:

La calificación de la asignatura se calculará como la media ponderada de las calificaciones obtenidas en el examen de teoría-problemas (40%), ejercicios de prácticas de la asignatura (30%) y trabajos y actividades evaluables realizadas durante el curso (30%). De este modo, la calificación global se calculará como
calif. global: 0.4*calif. examen de teoría+0.3*calif. prácticas+0.3*calif. actividades.

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		Temas 1, 2
#2	1	0	0	0	0		Temas 2, 3
#3	1	0	0	0	0		Tema 3
#4	2.5	0	0	0	0		Tema 3
#5	2.5	0	0	0	0		Tema 4
#6	1	1	0	0	0		Tema 4
#7	1	1	0	0	0	Act. evaluable 1	Tema 5
#8	1	0	1.5	0	0		Tema 5, Práctica 1
#9	1	1	0	0	0		Tema 5
#10	1	0	1.5	0	0		Tema 5, Tema 6, Práctica 2
#11	1	1	0	0	0	Act. evaluable 2	Tema 6
#12	1	0	1.5	0	0		Tema 6, Práctica 3
#13	1	1	0	0	0		Tema 7
#14	1	0	1.5	0	0		Tema 7, Práctica 4
#15	1	1	0	0	0	Act. evaluable 3	Tema 8
	18	6	6	0	0		