Universidad Carlos III de Madrid

COSEC · Dpto. Informática

Guía de las asignaturas

Criptografía y Seguridad Informática
Seguridad en las Tecnologías de la Información

Grado en Ingeniería Informática

Doble Grado en Informática y Administración de Empresas

COSEC LAB - Curso 2019/2020

Descripción general

- Carácter obligatorio — Créditos ECTS: 6
- Curso: 2 ° — Cuatrimestre: 2 °
- Profesor coordinador:
  - Ana Isabel González-Tablas Ferreres, aigonzal@inf.uc3m.es, Desp. 2.2.B31
  - Docencia impartida por profesores del Grupo de Seguridad en las T.I. (COSEC LAB) del Dpto. de Informática

Colmenarejo	Leganés mañana	Leganés tarde	Leganés bilingüe
Lorena González lgmanzan@inf.uc3m.es	Ana I. González-Tablas aigonzal@inf.uc3m.es	Pablo Martín pmgonzal@inf.uc3m.es	José Luis de Miguel jomiguel@inf.uc3m.es
José de Fuentes jfuentes@inf.uc3m.es	José Soler josolerc@inf.uc3m.es		Sergio Pastrana spastrana@inf.uc3m.es
	Sergio Pastrana spastrana@inf.uc3m.es		

Objetivos

1. Reconocer la importancia actual de la seguridad de la información y de las tecnologías que permiten su tratamiento, los puntos débiles de éstas y las amenazas que sufren
2. Conocer los principios, métodos y medios de los sistemas de seguridad

- Para lograr estos objetivos el alumno debe adquirir una serie de conocimientos, capacidades y actitudes *(consúltese la ficha de la asignatura)*

Programa

1. Fundamentos matemáticos
2. Cifrado de datos
   1. Introducción a los criptosistemas
   2. Métodos criptográficos clásicos y criptoanálisis
   3. Criptosistemas simétricos. Cifrados en bloque y en flujo
   4. Criptosistemas asimétricos
   5. Generación y distribución de claves
3. Autenticación de datos
   1. Funciones resumen. MAC
   2. Firma digital
   3. Infraestructuras de clave pública
4. Autenticación de usuarios

PARTIAL EXAM

FINAL EXAM

Prácticas

1. Fundamentos matemáticos
2. Cifrado de datos
    1. Introducción a los criptosistemas
    2. Métodos criptográficos clásicos y criptoanálisis
    3. Criptosistemas simétricos. Cifrados en bloque y en flujo
    4. Criptosistemas asimétricos
    5. Generación y distribución de claves
3. Autenticación de datos
    1. Funciones resumen. MAC
    2. Firma digital
    3. Infraestructuras de clave pública
4. Autenticación de usuarios

LAB 1 ; test

LAB 2 ; test

LAB 3 ; test

Metodología: Actividades

Teoría y Problemas

1. Clases magistrales
   1. Exposición del profesor basada en notas de clase publicadas en Pág. Web Magistral A.G. y textos de referencia
2. Problemas
   1. Resolución de ejercicios con enunciados previamente publicados (Pág. Web Magistral A.G.)
   2. Las soluciones se publican después (Pág. Web Magistral A.G.)
3. Sesiones de teoría
   1. Habitualmente en aula teoría
   2. Algunas en AULA INFORMÁTICA
   3. Combinación de teoría y problemas
4. Foros de teoría y problemas
   1. Atención de dudas (Pág. Web Magistral A.G)
5. Evaluación
   1. 1 examen de E.C. + 1 examen final

Prácticas

1. Trabajo práctico del alumno
   1. Publicación de enunciados en Pág. Web del Magistral A.G.
2. Sesiones de prácticas
   1. En AULA INFORMÁTICA
   2. Atención de dudas
3. Foros de las prácticas
   1. Atención de dudas (Pág. Web Magistral A.G.)
4. Evaluación
   1. Test individual (cuestiones cortas, cuestiones de respuesta objetiva, desarrollo de código, preguntas sobre la teoría asociada…)

Prácticas

- Prac-1: Criptoanálisis con **Cryptool** y análisis de aleatoriedad con **ENT**

- Prac-2: Prácticas con librerías criptográficas (funciones de aleatoriedad, funciones resumen, MAC, cifradores simétricos y asimétricos) (Librería **BouncyCastle** para Java)

- Prac-3: Firma digital y PKI con **OpenSSL**

Prácticas: Desarrollo de las sesiones

- Enunciados publicados la semana antes de las sesiones
- El alumno debe TRABAJAR LA PRÁCTICA (**TRABAJO DEL ALUMNO**) de forma previa a la sesión de prácticas
- **FORO** para cada práctica donde dirigir las **DUDAS**

- **TEST** individual de la práctica

Semanas reales	Lunes	Viernes	Sesión magistral	Sesión reducida (horario normal)	CLASES MAGISTRALES EN HORARIO EXTRA o SEGUNDO PROFESOR
Semana 1	27-ene	31-ene	1 Presentación. Fundamentos matemáticos (INTRO)	Fundamentos matemáticos. Problemas	
Semana 2	03-feb	07-feb	3 Fundamentos matemáticos. Problemas	Fundamentos matemáticos. Problemas	
Semana 3	10-feb	14-feb	5 Introducción a los criptosistemas	Criptografía clásica. Problemas	
Semana 4	17-feb	21-feb	7 Criptografía clásica. Problemas	Cifradores simétricos de bloque (Feistel. Modos de operación)	
Semana 5	24-feb	28-feb	9 Cifradores simétricos de bloque (DES). Problemas.	Cifradores simétricos de bloque (AES). Problemas.	
Semana 6	02-mar	06-mar	11 Cifradores simétricos de flujo. Problemas.	Intercambio de claves (Diffie-Hellman). Problemas de Diffie-Hellman. Introducción a la criptografía de clave pública. RSA cifrado	
Semana 7	09-mar	13-mar	13 Problemas de RSA. ElGamal cifrado. Problemas El Gamal cifrado. MAGISTRAL	Problemas Diffie-Hellman, RSA y El Gamal cifrado de examen. CIFRADO HÍBRIDO	
Semana 8	16-mar	20-mar	15 EXAMEN 1 (CIFRADO)	intro de integridad y autenticación. Funciones resumen y MAC	
Semana 9	23-mar	27-mar	17 Firma digital (RSA, DSS). Problemas firma digital. función resumen y MAC.	Problemas firma digital. función resumen y MAC.	
Semana 10	30-mar	03-abr	19 Problemas firma digital. función resumen y MAC. Introducción al problema de distribución de claves públicas. Enlace con PKI - MAGISTRAL	PRÁCTICAS	PRÁCTICAS
SEMANA SANTA	06-abr	10-abr	———	———	———
Semana 11	13-abr	17-abr	21 Infraestructuras de clave pública (PKI).	PRÁCTICAS	PRÁCTICAS
Semana 12	20-abr	24-abr	23 Problemas Infraestructuras de clave pública (PKI)	PRÁCTICAS	PRÁCTICAS
Semana 13	27-abr	01-may	25 PROBLEMA DE EXAMEN	PRÁCTICAS	PRÁCTICAS
Semana 14	04-may	09-may	27 LAB EXAM	26 Autenticación de usuarios	
Semana 15	11-may	15-may	28 REPASO - PROBLEMAS EXAMEN		
			EXAMEN FINAL		

Evaluación (visión general - pruebas)

- **EVALUACIÓN CONTINUA (60%):**

1. **Examen Parcial** (teoría y problemas): **30%**
2. **Test Laboratorios**: **30%**

- **EXAMEN FINAL (40%):**

1. **Examen Final** (teoría y problemas): **40%**
    1. puntuación mínima de 2 sobre 4; es decir, el 50%

- **EXAMEN COMPENSATORIO (DE E.C.) (60%):**

1. Equivalente al **"Examen Parcial"**: **30%**
2. Equivalente a "**Test Laboratorios**": **30%**

Evaluación (visión general - opciones)

- **Modalidad de continua**
  - 2 convocatorias: Mayo (ordinaria) y Junio (extraordinaria)
    - **Mayo:** NOTA FINAL =

    = NOTA EVALUACIÓN CONTINUA + NOTA EXAMEN FINAL ORDINARIA
    - **Junio**: NOTA FINAL =

    = NOTA EVALUACIÓN CONTINUA + NOTA EXAMEN FINAL EXTRAORDINARIA

- **Modalidad de NO continua**
  - 2 convocatorias: Mayo (ordinaria) y Junio (extraordinaria)
    - **Mayo**: NOTA FINAL =

    = **0.6** * (NOTA EXAMEN FINAL + NOTA EXAMEN COMPENSATORIO ORDINARIA)
    - **Junio**: NOTA FINAL =

    = **1.0** * (NOTA EXAMEN FINAL + NOTA EXAMEN COMPENSATORIO EXTRAORDINARIA)

Bibliografía

- **BÁSICA:**
  - **W. STALLINGS, "CRYPTOGRAPHY AND NETWORK SECURITY". (5ª o 4ª EDICIÓN). PRENTICE HALL.**
  - **A.I. González-Tablas Ferreres y P. Martín González. Recopilación de problemas de examen 2010-2015. Criptografía y Seguridad Informática. ~~CopyRed~~. 2016**
- **COMPLEMENTARIA:**
  - **A.J. MENEZES; P.C. van Oorschot; S.A. Vanstone, "HANDBOOK OF APPLIED CRYPTOGRAPHY". CRC PRESS** *[Capítulos disponibles de libre acceso en Internet]*

Bibliografía (otros)

- B. SCHNEIER, "APPLIED CRYPTOGRAPHY. PROTOCOLS, ALGORITHMS AND SOURCE CODE IN C". (2ª EDICIÓN) JOHN WILEY & SONS, INC

- C. PFLEEGER, "SECURITY IN COMPUTING". (3ª EDICION) PRENTICE HALL

- J. PASTOR; M.A. SARASA; J.L. SALAZAR, "CRIPTOGRAFÍA DIGITAL. FUNDAMENTOS Y APLICACIONES". (2ª EDICIÓN) PRENSAS UNIVERSITARIAS DE ZARAGOZA