SEGURIDAD EN SISTEMAS INFORMÁTICOS

Cátedra Institucional en Ciberseguridad Binter
Universidad de La Laguna

https://www.ull.es/catedras/catedra-ciberseguridad-binter/

https://pcaballe.webs.ull.es

CryptULL

Horario:

Teoría: Lunes 12:00-13:50. Aula 1.3

Prácticas: Martes, Miércoles, Jueves 9:30-11:20. C. de Cálculo (Sala 2.1)

Profesoras:

- Teoría:

  Pino Caballero Gil

  Tutorías: El que aparece en la guía docente

  2ª planta Edificio Ingeniería Informática. Dto. Ing. Informática.

- Prácticas:

  Candelaria Hernández Goya

  Tutorías: El que aparece en la guía docente

  2ª planta Edificio Ingeniería Informática. Dto. Ing. Informática.

  Jezabel Molina Gil

  Tutorías: El que aparece en la guía docente

  2ª planta Edificio Ingeniería Informática. Dto. Ing. Informática.

SEGURIDAD EN SISTEMAS INFORMÁTICOS

- Centro: **Escuela Superior de Ingeniería y Tecnología**
- Titulación: **Grado en Ingeniería Informática**
- Departamento: **Ingeniería Informática y de Sistemas**
- Curso: **Tercero**
- Carácter: **Obligatoria**
- Itinerario: **Tecnologías de la Información**
- Créditos: **6.0 ECTS**

CryptULL

CONTENIDOS

Módulo I: Preliminares y conceptos básicos.

- Tema 1: Conceptos Básicos: Amenazas y vulnerabilidades
- Tema 2: Evolución histórica

Módulo II: Comunicaciones seguras.

- Tema 3: Protección de la confidencialidad
- Tema 4: Cifrados de clave secreta
- Tema 5: Distribución de claves

Módulo III: Esquemas de control de accesos y autenticación

- Tema 6: Esquemas básicos de control de accesos.
- Tema 7: El problema de la autenticación y sus variantes
- Tema 8: Esquemas de identificación
- Tema 9: Esquemas de autenticación para información multimedia

Módulo IV: Infraestructura de clave pública.

- Tema 10: Introducción al funcionamiento de las PKI (Public Key Infrastructure)
- Tema 11: Esquemas de cifrado de clave pública
- Tema 12: Firma electrónica
- Tema 13: Políticas y estándares de certificación de claves públicas

Módulo V: Comercio electrónico.

- Tema 14: Medios de pago en Internet
- Tema 15: Dinero electrónico

Módulo VI: Evaluación y protección de la información

- Tema 16: Protocolos criptográficos
- Tema 17: Seguridad en redes inalámbricas
- Tema 18: Introducción a las auditorías de seguridad

EVALUACIÓN

- En la evaluación continua el **50% de la nota se consigue con un examen final, mientras que el 50% restante se logra** con diferentes actividades (prácticas, tareas virtuales y participación en clases).
- La Calificación Final (CF) se obtiene de: nota en Examen Final (EF), Calificación de Prácticas (CP) y Calificación de Informes (CI):

CF=50%EF+25%CP+25%CI, si EF>=5 y CP>=5 y CI>=5

CF=mínimo{50%EF,25%CP,25%CI}, si EF<5, o CP<5, o CI<5

- Si se renuncia a la evaluación continua, la evaluación única consistirá en dos exámenes globales finales de teoría y de prácticas, y para aprobar hace falta tener en cada uno >=5, siendo la nota obtenida la media.

Prácticas Previstas

1. Módulo I: Preliminares y conceptos básicos. **Cifrado de Vernam**
2. Módulo I: Preliminares y conceptos básicos. **Cifrado de Vigenere**
3. Módulo II: Comunicaciones seguras. **Cifrado ChaCha20 de TLS**
4. Módulo II: Comunicaciones seguras. **Generador C/A de GPS**
5. Módulo II: Comunicaciones seguras. **Multiplicación en SNOW 3G y AES**
6. Módulo II: Comunicaciones seguras. **Advanced Encryption Standard**
7. Módulo II: Comunicaciones seguras. **Modos de cifrado en bloque**
8. Módulo II: Comunicaciones seguras. **Algoritmos de Diffie-Hellman y ElGamal**
9. Módulo III: Esquemas de control de accesos y autenticación. **Fiat-Shamir**
10. Módulo IV: Infraestructura de clave pública. **Cifrado RSA**
11. Módulo IV: Infraestructura de clave pública. **Cifrado de ElGamal Elíptico**
12. Módulo IV: Infraestructura de clave pública. **GPG**
13. Módulo IV: Infraestructura de clave pública. **Generar una AC con OpenSSL**
14. Módulo IV: Infraestructura de clave pública. **Firma RSA**

BIBLIOGRAFÍA

- Avoine, G.,Oechslin, P., Junod, P.. Computer System Security: Basic Concepts and Solved Exercises, CRC Press, 2007
- Caballero, P. Introducción a la Criptografía. Editorial Ra-Ma, 2ª Edición. 2002.
- Chin, SK., Beth Older, S., Access Control, Security, and Trust: A Logical Approach, CRC Press, 2010
- Domigo, J. Herrera. J. Criptografía per las serveis telematics. Edicions de la Universitat Oberta de Catalunya. 1999
- Fúster, A.; De la Guía, D.; Hernández, L.; Montoya, F.; MuñozTécnicas Criptográficas de Protección de Datos. , J. Ra-Ma, 2000.
- Katz, J.,Lindell, Y., Gan, R., Introduction to Modern Cryptography: Principles and Protocols, CRC Press, 2007.
- Morant J.L; Ribagorda A.; Sancho J. Seguridad y Protección de la Información. Editorial Centro de Estudios Ramón Areces; 1994.
- Pastor, José; Sarasa, Miguel Angel. Criptografía Digital. Colección Textos Docentes; Prensas Universitarias de Zaragoza; 1998.
- Ramió Aguirre, Aplicaciones Criptográficas. Segunda Edición. Jorge. Dpto. de Publicaciones EUI-UPM, 1999.
- Schneier, BruceApplied Cryptography. Protocols, Algorithms, and Source Code in C. 2nd ed. . John Wiley & Sons, Inc., 1996.
- www.criptored.upm.es

LIBROS DIVULGATIVOS Y NOVELAS

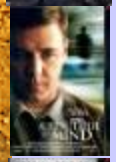
- Simon Singh: “Los Códigos Secretos”, Debate Editorial, 2000. Título Original: The Code Book (descarga gratis en www.simonsingh.net)
- Neal Stephenson: “Criptonomicón”
- Susana Mataix: “Lee a Julio a Verne”
- Steven Levy: “Cripto”
- Andrea Sgarro: “Códigos secretos”. Pirámide, 1990
- Edgar Allan Poe: “El escarabajo de oro”
- Conan Doyle,:“La aventura de los hombres danzantes”.
- Julio Verne: “Viaje al centro de la Tierra”, "Mathias Sandorf“, “La Jangada”.
- Robert Graysmith: ”Zodiac: El Asesino del Zodiaco” Ed. Alba.
- Guillermo Martínez: ”Los crímenes de Oxford”. Ed. Destino.
- Dan Brown: “El Código da Vinci”, ”La Fortaleza Digital”
- Javi Padilla: “Mara Turing: El Despertar de los Hackers”

PELÍCULAS

- WarGames (1983) Un joven encuentra una puerta trasera en un ordenador militar central en el que la realidad se confunde con un juego.

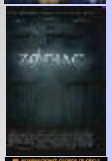
- Sneakers (1992) Película de suspense sobre ordenadores y criptografía.

- The Matrix (1999) Un hacker descubre la verdad de la realidad.



- A Beautiful Mind (2001) Un brillante matemático acepta un trabajo secreto en criptografía, y su vida da un giro.

- Enigma (2001) Un joven genio trata de romper el cifrado de la máquina Enigma usada por los alemanes en la IIGM.



- Zodiac (2007) Un detective amateur se obsesiona con un asesino en serie que usa mensajes cifrados.

- The Imitation Game (2015) Basada en 'Alan Turing: The Enigma'

- Snowden (2016) Sobre secretos de la CIA y la NSA

- Enola Holmes (2020) Muestra bastantes cifrados clásicos.