Titulación Ingeniero En Informática **Curso** 4º
Cuatrimestre Segundo **Tipo** Optativa
Duración Cuatrimestral **Créditos ECTS** 5.11
Créd. teoría 3 **Créd. prácticas** 3

Departamento Álgebra
Área Álgebra
Tipo de clases Teoría y práctica
Método de evaluación Examen de teoría (30%), entrega y defensa de prácticas (50%) y exposición pública (20%).
Recomendaciones Matemática discreta

Programa de Teoría

- **Tema 1:** Introducción: Criptosistemas abstractos. Criptosistemas clasicos. Criptoanálisis
  - **1.1:** *Introducción a la Criptografía.*
  - **1.2:** *Descripción de los criptosistemas clásicos.*
  - **1.3:** *Criptoanálisis.*
  - **1.4:** *Descripción de problemas.*
- **Tema 2:** Criptografía simétrica: DES, IDEA y AES. Modos de operación.
  - **2.1:** *Algoritmos simétricos: bloque y flujo.*
  - **2.2:** *Aspectos de eficiencia e implementación.*
  - **2.3:** *Generación de secuencias aleatorias.*
- **Tema 3:** Cifrado en bloque simétrico.
  - **3.1:** *Modos de cifrado en bloque.*
  - **3.2:** *Descripción de criptosistemas simétricos: DES, IDEA, AES.*
  - **3.3:** *Aspectos de eficiencia e implementación.*
- **Tema 4:** Criptografía asimétrica.
  - **4.1:** *Protocolo de Diffie-Hellman.*
  - **4.2:** *Algunos aspectos de teoría de números.*
  - **4.3:** *Algoritmos simétricos: RSA, ElGamal.*
  - **4.4:** *Criptografía con curvas elípticas.*
- **Tema 5:** Firmas digitales.
  - **5.1:** *Autenticidad del contenido de los mensajes.*
  - **5.2:** *Funciones Resumen (Hash).*
  - **5.3:** *El estándar de firma digital (DSA).*
  - **5.4:** *Esquemas arbitrados.*
- **Tema 6:** Certificados digitales.
  - **6.1:** *Esquemas de certificación.*
  - **6.2:** *Autoridades de certificación.*
  - **6.3:** *Listas de revocación.*
  - **6.4:** *El Estándar X509.*
- **Tema 7:** Protocolos criptográficos.
  - **7.1:** *Definición de protocolo.*
  - **7.2:** *Distribución de llaves.*
  - **7.3:** *Protocolos de transferencia inconsciente. Lanzamiento de una moneda.*

- **7.4:** *Protocolos de conocimiento cero.*
- **7.5:** *Protocolos de secreto compartido.*
- **7.6:** *Póker mental y voto electrónico.*

Programa de Prácticas

- **Práctica 1:** Aritmética modular.
- **Práctica 2:** Criptosistemas clásicos.
- **Práctica 3:** Cifrado en bloque (AES)
- **Práctica 4:** Criptografía asimétrica y firma digital.

Bibliografía

- **1. Título:** Introducción a la criptografía. 2ª edición.
  - **Autor/es:** *P. Caballero*
    - **Más info:** *RA-MA 2002*
- **2. Título:** Moderm Cryptography, a tutorial
  - **Autor/es:** *Brassard, Guiles*
    - **Más info:** *Springer-Verlag, 1988.*
- **3. Título:** Cryptography: policy and algorithms
  - **Autor/es:** *Dawson; Golic*
    - **Más info:** *1996*
- **4. Título:** A course in number theory and cryptography
  - **Autor/es:** *Koblitz, Neal*
    - **Más info:** *Springer-Verlag, 1979.*
- **5. Título:** El criptosistema RSA
  - **Autor/es:** *R. Duran, L. Hernández, J. Muñoz*
    - **Más info:** *RA-MA 2005*
- **6. Título:** Criptografia y Seguridad en Computadores
  - **Autor/es:** *Manuel Lucena López*
    - **Más info:** *Universidad de Jaén.*
    - **Más info:** *http://wwwdi.ujaen.es/~mlucena/lcripto.html*
- **7. Título:** Técnicas cirptográficas de protección de datos. 3ª ed. actualizada.
  - **Autor/es:** *A. Fúster*
    - **Más info:** *Ed. RA-MA 2004.*
- **8. Título:** Cryptography: Theory & Practice
  - **Autor/es:** *D.R. Stinson*
    - **Más info:** *CRC 1995*
- **9. Título:** Criptografía Digital: Fundamentos y aplicaciones.
  - **Autor/es:** *J. Pastor Franco, M.A. Sarasa López, J.L. Salazar Riaño.*
    - **Más info:** *Prensas Universitarias de Zaragoza.*
- **10. Título:** Introducción a la criptografía: Historia y actualidad.
  - **Autor/es:** *Jesús Ortega, M.A. López Guerrero, Eugenio C. García del Castillo.*
    - **Más info:** *Cuenca: Universidad de Castilla la Mancha.*
- **11. Título:** Protocolos criptográficos y seguridad en redes.
  - **Autor/es:** *Jaime Gutiérrez, Juan Tena*
    - **Más info:** *Universidad de Cantabria.*

- **12. Título:** Fundamentals of Criptology
    - **Autor/es:** *Henk C. A. van Tilborg*
- **13. Título:** The design of Rijndael: AES - The Advanced Encryption Standard.
    - **Autor/es:** *Joan Daeman, Vinvent Rijmen.*