

## Bibliografía básica

---

La **bibliografía básica es imprescindible para el estudio de la asignatura**. Cuando se indica que no está disponible en el aula virtual, tendrás que obtenerla por otros medios: librería UNIR, biblioteca...

### Tema 1:

Lucena, M. (2010). *Criptografía y seguridad de computadores*. Recuperado el 14 de febrero de 2013, en:

<http://wwwdi.ujaen.es/~mlucena/wiki/pmwiki.php?n=Main.LCripto>

Capítulo 2 «Conceptos Básicos» y capítulo 5 «Aritmética Modular».

Los capítulos se pueden consultar en el aula virtual.

Caballero Gil, P. (2002). *Introducción a la criptografía*. Madrid: Editorial Ra-Ma. ISBN: 84-7897-520-9.

Las páginas 20-30 están disponibles en el aula virtual (licencia CEDRO\*) para su consulta, descarga e impresión.

### Tema 2:

Lucena, M. (2010). *Criptografía y seguridad de computadores*. Recuperado el 14 de febrero de 2013, en: <http://wwwdi.ujaen.es/~mlucena/wiki/pmwiki.php?n=Main.LCripto>

Capítulo 10 «Cifrados por bloques» y el capítulo 13 «Funciones resumen».

Los capítulos se pueden consultar en el aula virtual.

### Tema 3:

Lucena, M. (2010). *Criptografía y seguridad de computadores*. Recuperado el 14 de febrero de 2013, en:

<http://wwwdi.ujaen.es/~mlucena/wiki/pmwiki.php?n=Main.LCripto>

Capítulo 12 «Cifrados asimétricos» y el capítulo 17 «Autenticación, certificados y firmas digitales».

Los capítulos se pueden consultar en el aula virtual.

**Tema 4:**

Fuster Sabater, A. (2004). *Técnicas criptográficas de protección de datos*. Madrid: Editorial Ra-Ma. ISBN: 84-7897-594-2

El capítulo 4 «Gestión de claves simétricas» (páginas 103-124) está disponible en el aula virtual (licencia CEDRO\*) para su consulta, descarga e impresión.

**Tema 5:**

Lucena, M. (2010). *Criptografía y seguridad de computadores*. Recuperado el 14 de febrero de 2013, en: <http://wwwdi.ujaen.es/~mlucena/wiki/pmwiki.php?n=Main.LCripto>

Capítulo 10 «Cifrados por bloques».

El capítulo se pueden consultar en el aula virtual.

VV. AA. (2001). *Criptografía digital*. Zaragoza: Editorial Prensas Universitarias de Zaragoza. ISBN: 84-7733-558-3

El capítulo 1 «Generalidades» (páginas 19-22) está disponible en el aula virtual (licencia CEDRO\*) para su consulta, descarga e impresión.

\* Esta obra está protegida por el derecho de autor y su reproducción y comunicación pública, en la modalidad puesta a disposición, se han realizado con autorización de CEDRO. Queda prohibida su posterior reproducción, distribución, transformación y comunicación pública en cualquier medio y de cualquier forma, con excepción de una única reproducción mediante impresora por cada usuario autorizado.

## **Bibliografía complementaria**

---

Caballero Gil, P. (1996). *Introducción a la criptografía*. Madrid: Ra-Ma.

Carracedo Gallardo, J. (2004). *Seguridad en redes telemáticas*. Madrid: McGraw-Hill.

Fúster Sabater, A. [et al.]. (2004). *Técnicas criptográficas de protección de datos*. Madrid: Ra-Ma.

Menezes, A. J., Van Oorschot, P. C. and Vanstone, S. A. (1996). *Handbook of Applied Cryptography*. CRC Press.

Pastor Franco, J. (1998). *Criptografía digital: fundamentos y aplicaciones*. Zaragoza: Prensas Universitarias de Zaragoza.

Singh, Simon (2000). *Los códigos secretos*. Madrid: Debate.