Criptografía

TEMARIO

Tema 1
Introducción a la criptografía

Tema 2
Preliminares matemáticos

Tema 3
Cifrado en flujo

Tema 4
Cifrado simétrico en bloque

Tema 5
Primalidad. Factorizacion

Tema 6
Criptografía de clave pública

Tema 7
Protocolos de autenticación

BIBLIOGRAFÍA BÁSICA

P. Caballero Gil. *Introducción a la Criptografía*. Ra-Ma, 2002.

M. J. Lucena. *Criptografía y Seguridad en Computadores*. Univ. Jaen, 2005. http://criptografiayseguridad.blogspot.com.es/p/criptografia-y-seguridad-en.html

Martin, B. *Codage, cryptologie et applications*. Presses polytechniques et univertiaires normandes, 2004.

A. J. Menezes, P. C. Oorschot, S. A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996. http://www.cacr.math.uwaterloo.ca/hac/

J. Pastor, M.A. Sarasa, J. L. Salazar. *Criptografía Digital. Fundamentos y Aplicaciones*. Prensas Universitarias de Zaragoza. Colección textos docentes, 2001.

B. Schneier. Applied Cryptography. John Wiley and Sons, Inc. 1996.

BIBLIOGRAFÍA DE PROFUNDIZACIÓN

H. Delfs, H. Knebl. *Introduction to Cryptography*. Springer, 2007.

N. Ferguson, B. Schneier, T. Kohno. *Cryptography Engineering: Design Principles and Practical Applications*. Wiley Publishing, 2010.

S. Goldwasser, M. Bellare. *Lecture notes on Cryptography*, 2008.