



Manual de criptografía [: fundamentos matemáticos de la Criptografía para un estudiante de Grado /

Plaza Martín, Francisco José.

Universidad de Salamanca,
2021.

Recurso Electrónico

Detrás de la comunicación cifrada de WhatsApp, del DNI electrónico y de los protocolos de navegación seguros <https://> encontramos la criptografía. Este libro, concebido como un manual, pretende ser una introducción a los fundamentos matemáticos sobre los que se apoya la criptografía moderna y está orientado a estudiantes universitarios tanto de matemáticas y física como de informática e ingeniería. El texto presenta aspectos teóricos de forma accesible y los ilustra y complementa con ejercicios y algoritmos que pueden ser programados fácilmente. Entender la base matemática subyacente a la criptografía proporcionará al lector la capacidad de analizar las fortalezas y debilidades de un criptosistema, así como de comprender el diseño y los ataques de un protocolo criptográfico. Debido al carácter intrínsecamente interdisciplinar de esta materia y con vistas a una capacitación profesional plena, un ulterior estudio debería incorporar aspectos de probabilidad, de algoritmia, de diseño de hardware, etc.

<https://rebiunoda.pro.baratznet.cloud:28443/OpacDiscovery/public/catalog/detail/b2FpOmNlbGVicmF0aW9uOmVzLmJhcmF0ei5yZW4vMzc1ODQxNjQ>

Título: Manual de criptografía [Recurso electrónico] : fundamentos matemáticos de la Criptografía para un estudiante de Grado Francisco José Plaza Martín.

Editorial: Salamanca Universidad de Salamanca 2021.

Descripción física: 1 archivo.

Mención de serie: Documentos Didácticos 169

Bibliografía: Bibliografía: p. 111.

Contenido: Introducción ; [Cap. I-VI]: Criptografía Simétrica ; Complejidad, Factorización y Logaritmo Discreto ; Números Primos ; Criptografía Asimétrica ; Criptografía con Curvas Elípticas ; Funciones Resumen (Hash): Aplicaciones.

Restricciones de acceso: Dominio público.

Programa de estudio: A1175.

Detalles del sistema: Disponible en formato .pdf Ordenador con navegador de Internet ; Adobe Acrobat Reader

ISBN: 978-84-1311-463-7 PDF) 978-84-1311-464-4 POD)

Materia: Criptografía (Informática)- En línea.

Baratz Innovación Documental

- Gran Vía, 59 28013 Madrid
- (+34) 91 456 03 60
- informa@baratz.es