Las matemáticas de la criptología [: secretos demostrables y demostraciones secretas /

González Vasco, María Isabel.

Catarata,
2018.

Recurso Electrónico

Aunque las técnicas criptográficas se conocen desde antiguo, solo a mediados del siglo pasado la criptología definida como ciencia y práctica del diseño de sistemas de comunicación que son seguros en presencia de adversario pudo adquirir sus bases científicas gracias a la fundamentación que le proporcionó la matemática, dando un vuelco en sus planteamientos y desarrollos a partir de los años setenta. En la actualidad, con el uso masivo de las tecnologías de la información y comunicación, el modo en que compartimos, gestionamos y almacenamos la información plantea para esta ciencia nuevos y fascinantes retos en el diseño de sistemas de seguridad que garanticen, entre otros aspectos, la confidencialidad y autenticidad en los intercambios. Este libro es una introducción a la criptología desde una perspectiva moderna. Pretende acercar al lector, de manera amena y divulgativa, a las principales ideas y conceptos matemáticos que subyacen en diferentes construcciones criptográficas, con un doble propósito: aprender matemáticas a través de la criptología y desarrollar la inquietud por la criptología moderna desde el placer del formalismo matemático. Los profesores de educación secundaria encontrarán en él ejemplos novedosos y ejercicios sencillos para estudiantes de este nivel.

Título: Las matemáticas de la criptología Recurso electrónico] : secretos demostrables y demostraciones secretas María Isabel González Vasco.

Editorial: Madrid Catarata 2018.

Descripción física: 1 archivo il.

Mención de serie: Miradas matemáticas

Bibliografía: Índice: p. 10. Bibliografía: p. 100-101.

Contenido: [Cap. 1-5]: Criptografía simétrica. Al César lo que es del César ; Criptografía asimétrica. Alice y Bob tienen que hablar ; Sistemas de prueba. Solo sé que no he aprendido nada ; Compartición de secretos. Cuadrados latinos, polinomios y otras herramientas para la conspiración ; Criptografía omnipresente. Emparejamiento online, votaciones electrónicas y otras historias magníficas y aterradoras.

Restricciones de acceso: Acceso restringido a los usuarios de la Universidad Nebrija. Limitaciones de impresión, copia y descarga.

Detalles del sistema: Ordenador con navegador de Internet

ISBN: 978-84-9097-505-3

Materia: Criptografía (Informática)- En línea.

Baratz Innovación Documental

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