Las matemáticas de la criptología

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.

IBIC. PDZ/GPJ
9 788490 975053
12 € | ISBN: 978-84-9097-505-3

ICMAT INSTITUTO DE CIENCIAS MATEMÁTICAS

Federación Española de Sociedades de Profesores de Matemáticas

María Isabel González Vasco Las matemáticas de la criptología

3

colección
MIRADAS MATEMÁTICAS

María Isabel González Vasco

Las matemáticas de la criptología

Secretos demostrables y demostraciones secretas

María Isabel González Vasco es profesora titular de Matemática Aplicada de la Universidad Rey Juan Carlos. Licenciada en Matemáticas y doctora por la Universidad de Oviedo, ha desarrollado su carrera investigadora colaborando con distintos centros públicos y privados (Philips Crypto, Instituto IAKS de la U. de Karlsruhe, CCIS Florida, Imdea Software, Madrid). Su trabajo se centra en la criptografía matemática, específicamente en el ámbito de la seguridad demostrable para cifrado de clave pública e intercambio de clave en entornos multiusuario. Ha publicado más de 40 artículos en revistas y congresos especializados. Es miembro de la Asociación Internacional de Investigación en Criptología y vocal de la Junta de Gobierno de la Real Sociedad Matemática Española.

CATARATA