Matemática contemporánea por matemáticas contemporáneas,

Desde la RSME queremos visibilizar el papel de las mujeres en las matemáticas. Para ello, y aprovechando la celebración del Día de la Mujer Trabajadora, vamos a difundir semanalmente el perfil de una mujer matemática en el Boletín de la RSME. Estos perfiles han sido elegidos para una exposición, coordinada por Rosa María Pardo San Gil del departamento de Matemática Aplicada de la Universidad Complutense de Madrid, que se exhibirá en las facultades de las bibliotecas de todas las facultades españolas que cuenten con estudios de matemáticas, y queremos colaborar con su difusión.

Paz Morillo Es licenciada en Ciencias Exactas desde 1983 por la Universitat de Barcelona y doctora en Informática desde 1987 por la Universitat Politècnica de Catalunya. Desde septiembre de 1987 es profesora titular en el Departamento de Matemáticas de la UPC. Desde 1992 ha dirigido ocho tesis doctorales. Su área de investigación es la criptografía, y en la actualidad se centra en la criptografía aplicada a la votación electrónica.La votación electrónica hace referencia a la posibilidad de votar desde nuestro ordenador, tableta o móvil. Esto tiene una gran importancia para las personas que están en el extranjero o incapacitadas, pero también la tiene para la sociedad en general. No solo supondría un ahorro económico, sino que también aumentaría la posibilidad de consultar a los ciudadanos sobre diversos temas. La votación electrónica necesita confianza en que todos los procesos van a ser seguros: la confianza en que un voto particular haya sido contado, que nadie sepa qué se ha votado o que nadie manipule ese voto. Todo ello requiere el uso de criptografía: cifrado, firma digital, pruebas de conocimiento nulo…Artículos:

- P. Morillo y C. Ràfols. “The Security of All Bits Using List Decoding”. International Workshop on Public Key Cryptography 2009, Lecture Notes in Computer Science 5443 (2009). Págs. 15-33.
- P. Bibiloni, A. Escala y P. Morillo. “Vote validatability in Mix-Net-based eVoting”. International Conference on E-Voting and Identity 2015, Lecture Notes in Computer Science, 9269 (2015). Págs. 92-109.
- N. Costa, R. Martínez y P. Morillo. “Proof of a Shuffle for Lattice-Based Cryptography”. Nordic Conference on Secure IT Systems 2017, Lecture Notes in Computer Science, 10674 (2017). Págs. 280-296.