# Criptografía Simétrica Avanzada: Diseño y Análisis de Eficiencia en Mejoras Avanzadas del Estándar de Cifrado Simétrico DES

Fernández Pallarés, V. y Roca Martínez, A.

Dpto. de Matemática Aplicada y Comunicaciones
U.P. de Valencia

**Resumen**

Nuestro objetivo, en nuestros trabajos, han consistido en el Diseño y Análisis de una propuesta de mejora del estándar clásico de cifrado simétrico, el ya clásico DES (Data Encryption Standard), llegando así a los detalles de Implementación y CriptoAnálisis. Todo ello se basa en nuestra investigación en torno a los distintos métodos de securización de la información en sus diversas transferencias, en especial, en lo concerniente a las aplicaciones de Comercio Electrónico.

En nuestro trabajo, comenzamos, a modo introductorio, con un capítulo donde presentamos los antecedentes históricos de estos sistemas criptográficos, con una exposición de la base matemática necesaria para una buena comprensión de las distintas especificaciones y requerimientos del diseño funcional y técnico. Todo ello con objeto de su posterior implementación en distintas plataformas.

Tras nuestras investigaciones, hemos considerado interesante exponer en estas Jornadas los avances conseguidos en la mejora a estos estándares superados del DES. Por ello, presentamos un breve compendio de los resultados analítico-algebraicos más importantes utilizados en el establecimiento de las bases de este sistema de encriptación simétrico.

En el diseño de nuestros sistemas de cifrado simétrico en bloque, diferenciaremos el diseño funcional, en donde se analiza su estructura y se detallan todos y cada uno de los procesos a implementar, y el diseño técnico, en donde quedan reflejados los aspectos de implementación en distintas plataformas, así como la reutilización de los mismos para llevar a cabo el sistema inverso, en las situaciones que aplique, según los protocolos criptográficos tomados en cada situación.