

# GIR Codificación de la Información y Criptografía

## 1. Datos del Instituto de Investigación/Grupo de Investigación/Investigador:

Grupo de Investigación:	GIR Codificación de la Información y Criptografía
Director/Persona de Contacto:	Ángela I. Barbero Díez
Teléfono:	3793
Correo electrónico:	angbar@wmatem.eis.uva.es
Número de investigadores:	9
Otros Participantes	M. Francisca Blanco Martín, Francisco Javier Galán Simón, Edgar Martínez Moro, Carlos Munuera Gómez, Alejandro Piñera Nicolás, Policarpo Abascal Fuentes, Daniel Sadornil Renedo, Juan Gabriel Tena Ayuso
Otra información relevante (web, redes sociales, etc.): <a href="http://www.uva.es/opencms/3.investigacion/3.03.gir/3.03.03.areadecienciasexperimentales/index.html?grupo=64&amp;area=3">http://www.uva.es/opencms/3.investigacion/3.03.gir/3.03.03.areadecienciasexperimentales/index.html?grupo=64&amp;area=3</a>	

## 2. Línea/s de investigación (enumerar y breve descripción, no más de 3-4 líneas por cada una de ellas, indicando el/los investigador/es responsable/s y datos de contacto)

1. Teoría de códigos: Códigos correctores de errores. Se usan para proteger la información frente a interferencias y otros problemas que puedan ocurrir durante la transmisión o almacenamiento introduciendo errores o pérdidas.
2. Codificación para dispositivos RFID: Los dispositivos RFID tiene muy reducida capacidad de cálculo y requieren códigos especialmente diseñados.
3. Codificación en red (network coding): Tradicionalmente al transmitir información a través de una red de nodos se usaba copy/forward, pero permitir que los nodos intermedios puedan codificar aumenta la capacidad de la red.
4. Códigos de convolución: especialmente útil para transmitir información en 'streaming'.
5. Protocolos criptográficos implementables en tarjetas inteligentes: también las tarjetas inteligentes tienen reducida capacidad de cálculo pero requieren elevada seguridad por su tipo de uso. Principalmente el grupo ha trabajado en criptografía con curvas elípticas.
6. Otros protocolos criptográficos: criptografía para ordenadores cuánticos, esteganografía, etc. ,
7. Matemática Discreta: herramientas teóricas necesarias para desarrollar las otras líneas.