RESPONSABLE(S) DE TUTORIZACIÓN				TRABAJO FIN DE GRADO			DETALLE DEL TFG			
Número	DPTO	RESPONSABLE DE TUTORIZACIÓN	RESPONSABLE DE COTUTORIZACIÓN si procede	TIPOLOGÍA	TÍTULO	ESTUDIANTE	Descripción, resumen de contenidos y actividades a desarrollar en el ámbito de la Informática	Descripción, resumen de contenidos y actividades a desarrollar en el ámbito de las Matemáticas	Materias del Grado relacionadas	HARDWARE/SOFTWARE/BIBLIOGRAFÍA
2	**ALG**	Gabriel Navarro Garulo		Trabajos de profundización que sirvan de suplemento a algunas materias de la titulación	Construcción y decodificacón de códigos Goppa sesgados	Aarón Jerónimo Fernández	**Descripción:** Esta propuesta consiste en la implementación de un sistema de codificación/decodificación utilizando códigos Goppa sesgados, y su inserción en el esquema de McEliece para obtener un criptosistema de clave pública resistente a ataques cuánticos **Actividades:** 1. Implementación de un sistema de encriptación/decriptación utilizando códigos Goppa sesgados 2. Implementación de un criptosistema de clave pública, basado en el criptosistema de Mceliece, utilizando códigos de Goppa sesgados	**Descripción:** Esta propuesta consiste en el estudio de los códigos Goppa sesgados y un algoritmo de decodificación eficiente de dichos códigos. También se estudiara el esquema de McEliece para obtener criptosistemas de clave pública utilizando familias de códigos que son decodificables de forma eficiente. **Actividades:** 1. Estudiar las nociones básicas de criptografía, criptografía post-cuántica y teoría de códigos. 2.Estudiar de las propiedades básicas de los polinomios de Ore 3. Estudio de los códigos Goppa sesgados, su construcción y decodificación. Estudio del criptosistema de McEliece	Álgebra I, Geometría I, Álgebra II, Fundamentos de Programación, Metodología de la Programación, Algoritmica, Teoría de la Información y la Codificación, Teoría de Números y Criptografía.	1. SageMath, the Sage Mathematics Software System (Version 7.6), The Sage Developers, 2017, http://www.sagemath.org 2. W. C. Huffman, V. Pless. Fundamentals of error-correcting codes, 2003. 3. A. Betten, M. Braun, H. Fripertinger, A. Kerber, A. Kohnert and A. Wassermann, Error-Correcting Linear Codes. Classification by Isometry and Applications. Algorithms and Computation in Mathematics 18, 2006. Springer. 4. J. Gómez-Torrecillas, F.J. Lobillo, and Gabriel Navarro, Skew differential Goppa codes and their application to McEliece cryptosystem, Designs, codes and cryptography 91 (2023), 3995–4017 5. Robert J. McEliece, A public-key cryptosystem based on algebraic coding theory, JPL DSN Progress Report (1978), 114–116.