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
5	**ALG**	Gabriel Navarro Garulo		Trabajos de profundización que sirvan de suplemento a algunas materias de la titulación	Information set decodi	Noura Lachhab Bouhmadi	**Descripción:** Esta propuesta consiste en la implementación del criptosistema clásico de McEliece y algunos ataques al sistema utilizando information set decoding. **Actividades:** 1. Implementación de un sistema de encriptación/decriptación utilizando el criptosistema de McEliece 2. Implementación de ataques al sistema mediante técnicas de information set decoding 3. Realización de pruebas para evaluar la fortaleza del sistema.	**Descripción:** Esta propuesta consiste en el estudio del criptosistema clásico de McEliece y de los ataques al mismo mediante information set decoding **Actividades:** 1. Estudiar las nociones básicas de criptografía, criptografía post-cuántica y teoría de códigos. 2.Estudiar la deocdificación mediante códigos Goppa y el criptosistema de McEliece. 3. Estudiar las técnicas básicas de information set decoding	Álgebra I, Geometría I, Álgebra II, Fundamentos de Programación, Metodología de la Programación, Algorítmica, 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. Nicholas J. Patterson, The algebraic decoding of Goppa codes, IEEE Transactions on Information Theory 21 (1975), 203–207 5. Robert J. McEliece, A public-key cryptosystem based on algebraic coding theory, JPL DSN Progress Report (1978), 114–116. 6. Daniel J. Bernstein, Johannes Buchmann, Erik Dahmen (editors), Post-