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
4	**ALG**	Gabriel Navarro Garulo		Trabajos de profundización que sirvan de suplemento a algunas materias de la titulación	El criptosistema de Mc	Higinio Paterna Ortiz	**Descripción:** Esta propuesta consiste en la implementación del criptosistema asimétrico de McEliece utilizando códigos de Reed-Solomon generalizados y su criptoanálisis mediante el ataque de Sidelnikov y Shestakov. **Actividades:** 1. Implementar un sistema de codificación-decodificación con códigos de Reed-Solomon generalizados 2. Implementar el esquema de McEliece utilizando códigos Reed-solomon 3. Implementar el ataque de Sidelnikov y Shestakov.	**Descripción:** Esta propuesta consiste en estudiar la teoría de códigos básica, los códigos de Reed-Solomon generalizados, el esquema de McEliece, y el ataque de Sidelnikov y Shestakov. **Actividades:** 1. Estudiar las nociones básicas de criptografía y teoría de códigos. 2.Estudiar la noción códigos de cíclicos, códigos de Reed-Solomon, y su decodificación. 3. Estudiar el esquema de McEliece, y el ataque de Sidelnikov y Shestakov.	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. H. Niederreiter, Knapsack-type cryptosystems and algebraic coding theory, Problems of Control and Information Theory 15 (2), 159-166. 4. 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. 6. V.M. Sidelnikov and S.O. Shestakov. On the insecurity of cryptosystems based on generalized Reed- Solomon codes. Discrete Mathematics and Applications, 1(4):439–444, 1992.