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
3	**ALG**	Gabriel Navarro Garulo		Trabajos de profundización que sirvan de suplemento a algunas materias de la titulación	Implementación y criptoanalisis del criptosistema GLN	Carmen Azorín Martí	**Descripción:** Esta propuesta consiste en la implementación del criptosistema asimétrico GLN, basado en el problema de la suma de subconjuntos, y su criptoanálisis. **Actividades:** 1. Implementar un sistema de encriptación/decriptación asimétrico basado en el criptosistema GLN. 2. Estudiar e Implementar los ataques usuales a los criptosistemas basados en el problema de la suma de subconjuntos. Aplicarlos al criptosistema implementado.	**Descripción:** Esta propuesta consiste en estudiar los fundamentos matemáticos del criptosistema GLN. **Actividades:** 1. Estudiar las nociones básicas de criptografía y teoría de códigos. 2.Estudiar la deocdificación mediante códigos Goppa. 3. Estudiar el criptosistema asimétrico GLN y la base de los ataques por baja densidad al problema de la suma de subconjuntos	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. C. Lagarias and A. M. Odlyzko. Solving low-density subset sum problems. Journal of the Association for Computing Machinery, 32(1) (1985), 229-246. 5. C. P. Schnorr and M. Euchner. Lattice basis reduction: Improved practical algorithms and solving subset sum problems. Math. Program., 66(1-3):181–199, 1994.