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
1	**ALG**	Francisco Javier Lobillo Borrero		Trabajos de profundización que sirvan de suplemento a algunas materias de la titulación	Criptografía basada en retículos	Mario Rodríguez López	La parte informática de este TFG comprende el desarrollo de software asociado al cryptosistema KRM. El alumno deberá implementar una versión operativa del KEM (Mecanismo de encapsulamiento de clave) construida en Kyber	Los criptosistemas basados en retículos constituyen una de las herramientas más exitosas en el desarrollo de criptografía post-cuántica. La idea original se remonta al esquema de cifrado basado en aprendizaje con errores (LWE), y la mejora aritmética basada en el criptosistema NTRU. Este TFG comprenderá el estudio del ganador del concurso del NIST Post-quantum cryptography, llamado Kyber, basado en module LWE. Para ello el alumno deberá estudiar y conocer las ideas previas que han conducido al diseño de este criptosistema.	Teoría de Números y Criptografía. Álgebra I, Metodología de la programación, Fundamentos de Ingeniería del Software.	CRYSTALS-Kyber (version 3.02) – Submission to round 3 of the NIST post-quantum project. Roberto Avanzi, Joppe Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, Gregor Seiler, and Damien Stehlé. Worst-Case to Average-Case Reductions for Module Lattices Adeline Langlois and Damien Stehle https://ia.cr/2012/090