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
48	**TSTC**	Rafael Alejandro Rodríguez Gómez		Complementario de profundización / Iniciación a la investigación	Programación de Hardware Secure Module en la implementación de criptografía asimétrica	Javier Gómez López	El Trabajo de Fin de Grado (TFG) se centrará en el estudio y aplicación de los Módulos de Seguridad Hardware (HSM, por sus siglas en inglés). Se explorará su arquitectura y funcionamiento, destacando los algoritmos criptográficos y los protocolos de seguridad que implementan para garantizar la protección de datos. Además, se analizarán las principales aplicaciones de los HSM en distintos entornos, las infraestructuras de clave pública (PKI), la gestión de identidades y otros ámbitos relacionados. Las actividades a desarrollar incluirán la simulación y análisis de entornos seguros utilizando software especializado, la implementación de algoritmos criptográficos en HSM virtuales, y la evaluación de su rendimiento y eficacia en diversos escenarios.	El Trabajo de Fin de Grado (TFG) abordará los fundamentos matemáticos que sustentan la seguridad de los Módulos de Seguridad Hardware (HSM). Se estudiarán los principios de la criptografía moderna, incluyendo teorías de números, álgebra abstracta y complejidad computacional, que son cruciales para la robustez de los algoritmos implementados en los HSM. Se analizarán en detalle algoritmos criptográficos como RSA, ECC (Elliptic Curve Cryptography) y AES (Advanced Encryption Standard), entre otros, destacando las propiedades matemáticas que garantizan su seguridad. Las actividades incluirán la demostración matemática de la seguridad de estos algoritmos, la resolución de problemas relacionados con la factorización de enteros y el logaritmo discreto, y la simulación de ataques criptográficos para evaluar la resistencia de los HSM. Estas	Álgebra I, Álgebra II, Álgebra III, Tecnología y Organización de Computadores, Estructura de Computadores, Arquitectura de Computadores, Fundamentos de Redes, Curvas y Superficies, Criptografía y Computación, Teoría de Números y Criptografía	Simulador de HSM