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
49	**TSTC / AM**	Rafael Alejandro Rodríguez Gómez	Francisco Javier Meri de la Maza	Complementario de profundización / Iniciación a la investigación	La función zeta de Riemann, criptografía de clave pública y el criptosistema de curvas elípticas	Manuel Vicente Bolaños Quesada	En este TFG se propone estudiar la influencia de la elección de diferentes suites criptográficas de TLS dentro del protocolo HTTP en concreto en HTTP/3 [I1]. Esta tercera versión de HTTP supone un cambio importante respecto a su predecesora ya utiliza QUIC que viaja sobre UDP en lugar de TCP que había sido el protocolo de capa de transporte utilizado por el servicio web desde su creación. Se propone también investigar la seguridad asociada al uso de diferentes curvas elípticas en este contexto [I2].	En este TFG se propone desarrollar las herramientas necesarias para construir la función zeta de Riemann, presentar sus propiedades fundamentales y su relación con los números primos, presentando el teorema del número primo. Se propone también explicar la relación de los números primos con la criptografía de clave pública y tratar de analizar si algunos de los resultados teóricos conocidos sobre la existencia garantizada de un número primo en un intervalo dado pueden permitir encontrar empíricamente algunos primos [M1,M2].	Variable Compleja I y II, Teoría de números y criptografía, Fundamentos de Redes y Seguridad y Protección de Sistemas Informáticos.	[M1] S. Patterson, An introduction to the theory of the Riemann zeta-function, Cambridge studies in advanced mathematicss 14, Cambridge University Press 1988. [M2] E. Titchmarsh, The theory of the Riemann zeta-function, Oxford University Press 1951 [I1] M. Bishop, 'HTTP/3', no. 9114. RFC Editor, Jun-2022. https://www.rfc-editor.org/rfc/rfc9114.html [I2] Tibor Jager, Jörg Schwenk, and Juraj Somorovsky. 2015. On the Security of TLS 1.3 and QUIC Against Weaknesses in PKCS#1 v1.5 Encryption. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications