# *Test de primalidad y algoritmos de factorización en criptografía: aspectos matemáticos y computacionales*

## Resumen

En la década de 1970 Diffie, Hellman y Merkle concibieron un paradigma criptográfico cuya idea revolucionaria fue emplear dos claves, una pública y otra privada, donde se requiere que ambas sean fáciles de generar pero al mismo tiempo no debería ser posible descubrir la privada a partir de la pública. Siguiendo sus pasos, Rivest, Shamir y Adleman publicaron el algoritmo de cifrado "RSA" con la idea de que las claves podrían ser generadas a partir del producto de dos grandes números primos (privados), puesto que todas las técnicas que se conocían para descomponer un número entero de esas características (lo público) eran ineficientes. Actualmente el mayor avance en la materia se debe a Shor, quien descubrió un algoritmo cuántico eficiente con dicho propósito. Sin embargo, ante la escasez de otros avances contundentes en complejidad computacional clásica, y dado que la implementación de computadoras cuánticas de gran porte sigue siendo un desafío, el protocolo RSA goza de plena vigencia. Luego, disponer de buenos test para conseguir números primos, así como conocer qué opciones hay para factorizar un entero e intentar romper RSA por esa vía, resulta un tema de gran importancia.

En esta tesis se releva en profundidad algunos de los test de primalidad y algoritmos de factorización más importantes que se emplean actualmente en la computación clásica. Estos problemas presentan una amplia gama de desafíos matemáticos y computacionales, y en tal sentido se busca comprender las soluciones que integran armoniosamente ambos enfoques. Los test de primalidad más destacados incluidos en el relevamiento son: el test de Fermat (el cual ha inspirado numerosos métodos), el test de Miller-Rabin, el test de Goldwasser-Kilian (basado en curvas elípticas) y el test "AKS" de Agrawal-Kayal-Saxena, que como posee el contexto matemático más complejo, ha sido tratado con especial énfasis. Asimismo, los algoritmos de factorización presentados son: el método rho de Pollard, el método de curvas elípticas de Lenstra y la Criba cuadrática.