## criptografia moderna

# RSA

Uno de los avances más revolucionarios fue el algoritmo RSA, desarrollado en 1977 por Rivest, Shamir y Adleman. Este sistema introdujo el concepto de criptografía de clave pública, basado en la factorización de números primos muy grandes. RSA marcó el fin de los sistemas de clave simétrica como únicos estándares y dio lugar a internet seguro. Lo curioso es que RSA se inspiró en ideas propuestas por un matemático británico, Clifford Cocks, en la década de 1970, pero su trabajo permaneció clasificado en la agencia de inteligencia británica GCHQ

RSA (Rivest, Shamir y Adleman) es un sistema criptográfico de clave pública desarrollado en 1977 por los informáticos y criptógrafos Ron Rivest, Adi Shamir y Leonard Adleman en el MIT. Fue el primer algoritmo creado de su tipo. Utiliza factorización de números enteros y, a diferencia de métodos anteriores de clave pública como el Diffie y Hellman, es válido tanto para cifrar como para firmar digitalmente.

RSA funciona multiplicando dos números primos para generar un semiprimo, que crea una clave pública. Para que alguien pueda descifrar el mensaje, tendría que determinar los dos números primos utilizados para crear el semiprimo. Con números primos grandes, es extremadamente complejo y requiere mucho tiempo determinar esos dos números.

La base de la seguridad de este algoritmo es el problema de la factorización de números enteros. Se utiliza una representación numérica para los mensajes enviados y el funcionamiento utiliza el producto, conocido, de dos números primos grandes elegidos aleatoriamente y que se mantienen en secreto en todo momento. Actualmente, estos primos son del orden de 10200, y sigue aumentando debido al constante crecimiento en la capacidad de cálculo actual de los ordenadores.