Caso 0: Codificación RSA

Debido a que la codificación RSA es un método de cifrado de gran interés en este tiempo y además la estamos estudiando en otra asignatura llamada *Seguridad y Sistemas Distribuidos*, pienso que es de gran interés para estudiarla.

Lo más interesante de este tipo de codificación es que además de ser una codificación asimétrica, es que permite el intercambio de una clave pública a través de una red no fiable y aun así no es posible en principio averiguar las claves privadas de los extremos. Cabe destacar que gracias al algoritmo matemático, se puede cifrar con la clave pública (conocida tanto por el usuario al otro extremo de la red no segura y todos aquellos que hayan capturado esa clave), y el usuario al otro extremo con su clave privada puede descifrar el mensaje original, impidiendo así que ningún otro usuario lo descifre.

El estudio de este caso que aunque no tiene demasiado que ver con la asignatura, si está relacionado con otra de la titulación por lo que merece la pena poder estudiarlo. Además no es conceptualmente complicado de entender y es fácilmente simularlo en *Mathematica*. Es un caso que cabe destacarlo.