D. Cuarto trabajo o práctica.

De forma sencilla, para valores enteros admitidos en el dominio del tipo de dato ***unsigned long*** del C o del Java (lenguajes que mayoritariamente han elegido los alumnos para confeccionar sus prácticas), se les ha propuesto a los alumnos que implementen un sencillo generador de bits aleatorios por entrada de teclado con el que generar una secuencia de bits para, a partir de ella, tomar dos enteros primos, generar las claves pública y privada del criptosistema RSA y firmar documentos mediante la transformación RSA sobre su correspondiente hash con la clave pública. También han realizado el proceso de obtención de la clave privada de otro usuario mediante la factorización del módulo de la trasformación RSA.
Esta práctica ha resultado quizá demasiado sencilla, pero ha permitido a los alumnos comprender y verificar el cambio de filosofía presente en los criptosistemas que deben su robustez no tanto al tamaño de las claves como sí a la dificultad actual para resolver en un tiempo aceptable determinados retos matemáticos por desconocer un algoritmo que sea computacionalmente eficiente. El tiempo medio dedicado para la implementación de esta práctica ha sido de dos horas.