A. Primer trabajo o práctica.

Programar un DES simplificado (llamado S-DES). Se han tomado como posibles algoritmos de DES simplificado dos presentados por Edward Schaefer, de la Universidad de Santa Clara. Uno de ellos (S-DES1) está presentado en "Cryptography and Network Security. Principles and practices". William Stallings. Prentice Hall. Pearson Education. Third edition. 2003 pp. 56 a 63. El otro (D-DES2), similar, lo hemos tomado de "Introduction of Cryptography with coding theory". Wade Trappe and Lawrence C. Washington. Prentice Hall, 2002 pp. 98 a 102. El primero de ellos cifra mediante una clave de 10 bits, y con un tamaño de bloque de 8 bits. El tamaño de las subclaves es de 8 bits. El segundo de ellos cifra mediante una clave de 9 bits, y con un tamaño de bloque de 12 bits. El tamaño de las subclaves es de 8 bits. En ambas referencias se describe el algoritmo pormenorizadamente. El objetivo de este primer trabajo es doble. Por un lado, el alumno debe implementar uno de los dos modelos de S-DES y realizar cifrado y descifrado de mensajes mediante bloques. Además, debe implementar la forma de ataque por fuerza bruta que le permita obtener la clave una vez tiene un bloque plano y su correspondiente cifrado. Evidentemente, con estos tamaños de clave (10 y 9 bits respectivamente) este ataque es eficaz y muestra la debilidad de estos criptosistemas.
La implementación de uno de estos algoritmos no es muy costosa para un alumno que ya tiene conocimientos de programación. Ha supuesto de dos a cuatro horas de trabajo del alumno por cada práctica presentada. No es sencillo determinar una duración estándar porque cada alumno realiza su trabajo con el lenguaje que prefiere y porque no es homogénea la pericia a la hora de crear el programa. La realización de esta práctica ayuda a caer en la cuenta de dos aspectos básicos de la criptografía simétrica: (1) que una vez implementado el algoritmo de cifrado, es casi inmediato, con las mismas funciones de cifrado, obtener la implementación del descifrado; y (2) que la implementación del ataque por fuerza bruta es también muy sencilla una vez se tiene implementado el algoritmo de cifrado. Los alumnos han podido obtener las claves de cifrado, en un ataque conocido como *Known plaintext attack* (ataque del que se conoce un mensaje original cualquiera y su correspondiente cifrado: cfr. "Handbook of Applied Cryptography". A. Menezes, P. van Oorschot, and S. Vanstone. CRC Press, Inc. 1997 § 1.13.1), en un tiempo mínimo, imperceptible en la ejecución.