B. Segundo trabajo o práctica.

Una vez implementado correctamente el algoritmo S-DES, se les propone a los alumnos que completen su pequeña aplicación permitiendo una entrada de texto a cifrar de cierta longitud (un documento de texto ASCII) y generando una cadena de longitud similar a la entrada de bloques cifrados. Se les plantea que elijan entre uno de los cuatro modos de operación de cifrado de bloque que se les ha presentado en clase (ECB, CBC, CFB, OFB comentados anteriormente) y se les pide también justifiquen su elección. Con esta práctica se pretende que el alumno vea el cifrado de un documento completo, y su posterior descifrado. También deben enfrentarse a la decisión del modo de operación de cifrado, aunque frecuentemente el alumno determina usar el modo CBC por ser más seguro que el inmediato ECB y notablemente más sencillo de implementar que los modos CFB y OFB. El tiempo empleado en la implementación de esta práctica ha sido también variable de un trabajo a otro; además de las causas indicadas antes en el apartado anterior, en este caso el alumno ha podido elegir diferentes modo de cifrado. Para el caso más habitual de elección, el modo CBC, el alumno ha empleado también entre dos y cuatro horas de trabajo. Esta práctica, además de ayudar a comprender bien el concepto de los modos de cifrado, ha exigido a algunos alumnos algunas modificaciones en el código de la práctica anterior: les ha enseñado que, además de saber implementar el algoritmo, un criptosistema requiere de la construcción de un protocolo de proceso. Además, todos los modos de cifrado (excepto el modo ECB) requieren de un valor inicial de tantos bits como el tamaño de bloque del criptosistema. Ese valor es aleatorio y, por tanto, supone una incertidumbre más en el uso del criptosistema: se comporta como una subclave añadida a la clave del criptosistema. Ahora el ataque por fuerza bruta antes implementado ya no sirve: los alumnos comprueban que así pueden incrementar la seguridad del criptosistema.