C. Tercer trabajo o práctica.

Una vez los alumnos tienen implementado el algoritmo S-DES y en correcto funcionamiento, el siguiente trabajo que se les propone es el diseño e implementación de una función de compresión a partir de una función de cifrado. Y luego el diseño e implementación de una función hash a partir de una función de compresión. La idea de implementar una función Hash sin clave a partir de una función de compresión fue propuesta por Ralph Merkle. Queda descrita en "Introduction of Cryptography with coding theory". Wade Trappe and Lawrence C. Washington. Prentice Hall, 2002 , pp. 235 – 242.
Las funciones de compresión que se obtienen de los algoritmos de cifrado implementados por los alumnos en su primera práctica, serán:
g1: $\{0,1\}^m \rightarrow \{0,1\}^n$, con m=20 y n=8, creada a partir de S-DES1.
g2: $\{0,1\}^m \rightarrow \{0,1\}^n$, con m=21 y n=12, creada a partir de S-DES2.
A partir de estas funciones de compresión se diseñan e implementan las funciones hash. En "Introduction to Cryptography". Johannes A. Buchmann. Springer Verlag, 2004. Second Edition viene descrito el modo en que se puede definir esas funciones hash. A partir de g1 se puede llegar a la función hash h1: $\{0,1\}^* \rightarrow \{0,1\}^n$, con n=8. A partir de g2 se llega a una función hash h2 similar a h1, ahora con n=12. De nuevo el objetivo planteado a los alumnos con este segundo trabajo es doble. Por un lado, implementar una función hash y comprobar con él que se cumplen las propiedades funcionales básicas de estas funciones. Específicamente que al variar en un bit la entrada a la función sufre modificación aproximadamente del 50% de los bits de salida. Y además, los alumnos deben implementar una aplicación que, mediante el ataque de cumpleaños (*birthday attack*) (cfr. "Handbook of Applied Cryptography". A. Menezes, P. van Oorschot, and S. Vanstone. CRC Press, Inc. 1997 § 9.7.1., "Introduction to Cryptography". Johannes A. Buchmann. Springer Verlag, 2004. Second Edition § 11.2) construya dos documentos diferentes con el mismo hash. Evidentemente es posible plantear este ataque sobre nuestra función hash porque el tamaño del resumen es demasiado pequeño para evitarlo. El tiempo empleado para la implementación de la función de compresión a partir del S-DES1 o S-DES2, y la implementación de la función hash a partir de la previa función de compresión ha sido largo, de más de 4 horas. Los alumnos han encontrado dificultad en el diseño y posterior implementación de un procedimiento para la construcción de la cadena de entrada al algoritmo de resumen. Para la parte de criptoanálisis, los alumnos han tenido más problemas. La paradoja del cumpleaños es sencilla de comprender pero exige bastante programación para llevarla a la práctica. No todos los alumnos han llegado a terminar este ejercicio. Los trabajos entregados han resultado brillantes. Se han empleado en clase de teoría para que todos los alumnos pudieran ver el comportamiento del ataque. Aunque no todos los alumnos han logrado culminar este trabajo con éxito, el esfuerzo realizado sí ha merecido la pena desde un punto de vista didáctico: les ha permitido asimilar con precisión todos los conceptos presentados sobre las funciones hash. Hemos evaluado a los alumnos de manera que no se ha penalizado el no haber entregado la parte de ataque en esta práctica. El tiempo medio dedicado a esta parte ha sido elevado, en una media de entre 8 y 10 horas.