Práctica 3. Algoritmos Simétricos.

1. Descargarse el conjunto de algoritmos **appliedc** (en código fuente y ejecutables) comprimidos. Descomprimirlos y obtener la lista de ficheros.
2. Descargar y leer el archivo **00_INFO** para comprender la descripción, funciones y ejecución común en línea de comandos del paquete de algoritmos en C suministrado.
3. Descargarse un **editor Hexadecimal** (**HexEdit, WinHex, Hexplore, HxD**, …) y utilizarlo cuando sea conveniente para examinar el contenido de los ficheros cifrados a continuación.
4. Descargar y ejecutar el algoritmo **enigmawn** de cifrado simétrico. Comprender la solución dada en el mismo (KEYFILE) para funcionar con llaves de sesión distintas en cada ocasión a partir de unos parámetros de configuración de Llaves y una Llave maestra.
5. Descargar y ejecutar el algoritmo **TrueCrypt** (en su proceso de diseño e implementación participó *Julian Assange*).
6. Para implementación de algoritmos simétricos, puedes acudir a código fuente de algunos de ellos en Python en :
   https://code.google.com/p/ska/
   en C en:
   http://www.superstarcoders.com/blogs/posts/symmetric-encryption-in-c-sharp.aspx
   y en Java en:
   https://www.flexiprovider.de/examples/ExampleCrypt.html

Tareas a realizar:

7. Clasificar los algoritmos de 1 en “algoritmos clásicos”, “algoritmos de cifrado en bloque” y “algoritmos en flujo” para poder proceder con el resto de la práctica.

8. Hacer varios ejemplos de ejecución de los algoritmos, al menos con dos algoritmos de cada uno de los grupos anteriores. Describir en qué consiste la llave.

   Nota: Se puede hacer desde una extensión de Chrome: **DosBox**

9. ¿En qué consiste la opción de borrado seguro de los algoritmos? Hacer algún ejemplo con las diversas opciones de borrado seguro.

10. ¿Hay algoritmos con un tamaño de bloque distinto de 64 bits?. En caso afirmativo decir cuáles y dar el tamaño del bloque.

11. ¿Qué ocurre si con el algoritmo XOR ciframos una cadena de caracteres y utilizamos como llave la misma cadena? ¿Cuál es la salida? ¿Qué ocurre ahora si con el mismo algoritmo XOR ciframos una cadena de caracteres con llave caracteres ESPACIO de la misma longitud que la entrada como texto llano? ¿Cuál es la explicación?

12. Dar otros ejemplos de cifrado y descifrado, si encuentras que sean interesantes, de otros algoritmos en particular con otras llaves en particular.

13. Los algoritmos ejecutables con **nombre.exe** están implementados en modo ECB. Los algoritmos ejecutables con **nombre_C.exe** están implementados en modo CBC. ¿Cómo podemos distinguirlos atendiendo a la salida que ofrecen? Poner un ejemplo en uno y otro caso con un algoritmo seleccionado de entre ellos.
    Indicación: buscar texto llano con repetición por bloques.

14. Los algoritmos están implementados normalmente en modo de "**anotaciones al final**" o "**padding**". ¿Cómo podemos comprobarlo?. Poner un ejemplo de ello

15. ¿Cómo afecta el padding a un algoritmo en modo ECB con repetición por bloques de texto llano de 8, 16 o 32 bits? ¿Y cómo afecta en el caso anterior con bloques de 64 bits?

Práctica para entrega 3:

16. Realizar el análisis de aleatoriedad provisto en **CrypTool** para el Keyfile de **enigmawn** y el fichero de llaves de **TrueCrypt,** obteniendo ficheros de longitud adecuada por concatenación, si es necesario**.** Realizar los test de Frecuencias, Poker, Rachas y Series, así como el integrado FIPS-PUB-140-1. Hacer una tabla con los resultados y obtener las conclusiones pertinentes sobre la aleatoriedad en uno y otro algoritmos.

17. Examinar las opciones de cifrado simétricas en **CrypTool** con varios algoritmos. Probar un ataque sobre alguno de ellos en función de la longitud de la llave. Analizar los tiempos de ataque necesarios para determinar 32 bits, 40 bits, 48 bits, 56 bits y 64 bits de llave.

18. Con los códigos disponibles de algoritmos simétricos, que puedes encontrar en los enlaces de 6 (u otros que igualmente están disponibles en diversas páginas y blogs), construye tu propio ejemplo de ejecución de algoritmo simétrico con elección de Modo de Cifrado, Padding, Borrado Seguro, Generación de Llaves, etc. Muestra el código fuente, compila el mismo o da el código ejecutable y muestra algún ejemplo de utilización con un fichero de prueba.