Proyecto Final

(Valor 30% del curso)

Se implementará un software/hardware que cifre y descifre archivos utilizando AES (Advanced Encryption Standard). El hardware consistirá en un microcontrolador 90USB1286, una memoria SD y una interfaz serial. El cifrado tendrá las siguientes características:

- La llave se dará por medio de un archivo binario de 128 bits (16 bytes) pre-almacenado en la SD. Este se puede crear en Hex Editor Neo.
- El archivo a cifrar deberá ser dividido en bloques de 128 bits y hacer el llamado "padding" o relleno del último bloque con bytes en ceros (00h). Los archivos a cifrar serán pre-almacenados en la SD. Es importante agregar un byte en el archivo (final) donde se almacene el número de bytes usados en el último bloque con el fin de que al descifrar el archivo quede idéntico al original.
- El cifrado/descifrado en se hará en modo EBC (Electronic Code Book).
- El descifrado deberá tener las mismas características del cifrado (EBC, AES inverso y 128 bits de llave)
- Se deberá tener una interfaz en la pantalla del puerto serial donde se le permita al usuario:

    a) Seleccionar la acción a realizar: cifrado o descifrado
    b) Nombre del archivo de entrada (con todo y extensión). Podrá ser cualquier archivo con cualquier extensión (por ejemplo MP3, PDF, etc).
    c) Nombre del archivo de salida sin extensión. Generar el archivo de salida con extensión .aes
    d) Nombre del archivo de la llave (archivo binario de 16 bytes)
    e) En cada cifrado y descifrado se deberá informar al usuario con la siguiente información:
        - Nombre del archivo de entrada y de salida
        - Número de bytes/bits cifrados o descifrados
        - Número de bloques de 128 bits
        - Tiempo total, en segundos, tomado en el proceso total
        - Tiempo del cifrado/descifrado
        - Tiempo de lectura/escritura
        - Tiempo total, en segundos, promedio por bloque

- En el LCD se deberá mostrar el estatus de lo que está haciendo el proyecto, por ejemplo:
    - Cifrando Nombre.txt
    - Descifrando Nombre.aes
    - Deberá mostrar el estatus del número de bloques cifrados o descifrados y el número de bloques en total (ejemplo 200/1355 bloques). Para no hacer tan lento la impresión del LCD, avanzar en bloques de 100 por ejemplo.

Se podrán utilizar las siguientes herramientas para desarrollar la aplicación:

- **Proteus:** todo el circuito se puede simular al 100%, sin embargo, se tendrá que entregar físicamente.
- **Hex Editor Neo**: para poder visualizar archivos binarios (las llaves y los archivos cifrados)
- **WinImage**: para poder accesar a la imagen de la SD en simulación de Proteus. Es decir poder ver los archivos generados o inyectar en la imagen de disco los archivos de entrada (llaves, textos a cifrar).
- **Cryptool**: aquí se puede revisar AES paso por paso (Procedimientos Individuales/Visualización de Algoritmos/AES/Inspector Rijndael (AES)) tanto para el cifrado como descifrado.

La entrega del proyecto debe ser física a través de Zoom. Además, entregar en CANVAS:

- Directorio completo del proyecto de CodeVision que contiene el proyecto y archivos fuente en ZIP o RAR
- Reporte que contenga:
    - Descripción del proyecto
    - Código fuente con comentarios funcionales
    - Diagrama Eléctrico
    - Liga de video demostrativo de funcionalidad total del proyecto
    - Conclusiones individuales

¡Mucho Éxito!