UNIVERSIDAD DE ANTIOQUIA
Facultad de Ingeniería

LABORATORIO ELECTRÓNICA DIGITAL II
DEPARTAMENTO DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES
PRÁCTICA 1 – PROGRAMACIÓN EN LENGUAJE C (FUNCIÓN HASH SHAKE256)

OBJETIVOS

- Aplicar los conceptos de programación en lenguaje C en la implementación de aplicaciones reales.
- Implementar la función hash SHAKE256 del estándar de criptografía SHA3 (NIST-FIPS-202).
- Comprender y utilizar documentación técnica como estándares internacionales.

DESCRIPCIÓN

A diferencia de los algoritmos de encriptación que protegen la confidencialidad de los datos (AES, RSA, DES, etc.), las funciones hash protegen la integridad de los datos en un esfuerzo para garantizar que dichos datos, sin importar si han sido encriptados o no, no fueron modificados. Una función hash toma una cadena de datos de cualquier tamaño y produce una cadena de bits de tamaño fijo llamada valor hash. Si una función hash es segura, dos piezas distintas de datos siempre tendrán valores hash diferentes. Por lo tanto, el valor hash de un archivo sirve como identificador del mismo.

Las funciones hash son los algoritmos más versátil y más utilizado en criptografía. Existen innumerables ejemplos de aplicaciones que utilizan funciones hash: los sistemas de almacenamiento en la nube (Dropbox, Drive, OneDrive, etc.) utilizan funciones hash para identificar archivos y detectar si han sido modificados; los sistemas de control de versiones como Git utilizan funciones hash para identificar archivos en un repositorio; un sistema de detección de intrusos utiliza este tipo de funciones para detectar archivos modificados; los analistas informáticos forenses utilizan valores hash para probar que un objeto digital ha sido modificado; Bitcoin utiliza funciones hash en su sistema de validación del ledger o libro contable.

El estándar NIST-FIPS-SHA3 especifica el algoritmo de hash seguro 3 (SHA-3), una familia de funciones hash que trabajan sobre datos binarios. Cada una de las funciones de SHA3 está basada en el algoritmo KECCAK que fue seleccionado como ganador de la competencia realizada por el Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos en el marco del estándar SHA3. El estándar también especifica la familia de permutaciones matemáticas KECCAK-p, que incluye las permutaciones utilizadas por SHA3. La familia de funciones hash definidas en SHA3 consiste en cuatro funciones: SHA3-224, SHA3-256, SHA3-384 y SHA3-512, y dos funciones con salida extensible llamadas SHAKE128 y SHAKE256. Las funciones con salida extensible son diferentes de las funciones hash, pero pueden ser usadas de forma similar, con la flexibilidad de adaptarse (longitud del hash) a los requerimientos de aplicaciones individuales.

PROCEDIMIENTO

1. Estudiar el estándar NIST-FIPS-SHA3 y en particular el funcionamiento de la función hash extensible SHAKE256.
2. Dibuje un diagrama de flujo o escriba el seudocódigo para el algoritmo de la función SHAKE256 del estándar SHA3.
3. Desarrolle en lenguaje C un programa que reciba un archivo de cualquier tipo y genere un valor hash asociado a dicho archivo utilizando el algoritmo de la función SHAKE256 del estándar SHA3. El programa recibe como parámetros en consola el nombre de archivo, la longitud del hash que debe producir el algoritmo SHAKE256, y los demás parámetros que pueda requerir la función. El programa debe imprimir en consola el valor hash asociado al archivo en hexadecimal. El programa no deberá utilizar ninguna librería distinta a las provistas por la librería estándar. Adicionalmente, el programa debe correr en Linux sin necesidad de modificación por parte del profesor.
4. Mida el desempeño de su programa para diferentes tamaños de archivo (1KB, 1MB y 10MB) y diferentes longitudes de hash (64b, 128b, 256b y 512b).

5. Escriba un reporte que incluya: procedimiento de compilación y ejecución del programa desarrollado, una explicación del diagrama de flujo o seudocódigo realizado en el numeral 2, el resultado de las mediciones de desempeño realizadas en el numeral 4, la discusión de los resultados obtenidos y conclusiones.
6. Suba el reporte y el código en un solo archivo comprimido a la plataforma Moodle del laboratorio antes de las 23:55 del Domingo 18 de marzo de 2018. Por favor, marque el archivo comprimido con el primer apellido de los integrantes del grupo.

EVALUACIÓN

1. Funcionamiento (40%) – Se verificará el correcto funcionamiento del código y se evaluará el tiempo de ejecución. Un programa cuyos resultados sean erróneos tiene nota cero en los componentes de sustentación y funcionamiento.
2. Sustentación (30%) – preguntas sobre el funcionamiento del código o del estándar SHA3 y en particular de la función SHAKE256 definida en el estándar.
3. Estructura, documentación y organización del código C (20%) – la correcta estructuración del código en funciones y librerías, la correcta documentación de las funciones y el uso de tabulaciones serán tenidos en cuenta en este ítem de calificación.
4. Reporte (10%) – La calidad del reporte y en particular de las conclusiones será vital para una buena calificación en este ítem.