Seguridad computacional

Práctica 3 – Diseño de un algoritmo de Cifrado Simétrico

El cifrado simétrico es el núcleo de cualquier sistema de seguridad contemporáneo, lo usamos todos los días cuando realizamos cualquier transacción segura y es la base fundamental y el pilar de la seguridad en internet, de ahí la importancia de que conozcas de una forma muy general como se diseñan estos algoritmos.

Objetivos de aprendizaje:

- Conocer las diferentes técnicas de generar difusión en un algoritmo de cifrado simétrico.
- Conocer las diferentes técnicas de generar confusión en un algoritmo de cifrado simétrico.
- Diseñar un algoritmo de cifrado simétrico que cuente con técnicas de difusión y confusión.
- Implementar mediante un lenguaje de programación el algoritmo de cifrado y probarlo con diversos textos y archivos.

Herramientas y software requerido

- Apuntes o libros que indiquen que se requiere para generar difusión y confusión.
- Lenguaje de programación instalado (se sugiere lenguaje C++ o cualquier lenguaje que facilite la manipulación a nivel de bits).

Diseño e implementación del algoritmo de cifrado

1. Con su equipo haga una discusión sobre cuáles son las características fundamentales que debe tener un algoritmo de cifrado simétrico para ser robusto, y enumérelas en una lista.
2. Diseñe un pequeño algoritmo de cifrado simétrico didáctico elemental que incluya operaciones básicas para lograr las características fundamentales que debe tener un algoritmo de cifrado básico. Indique en este paso que tipo de operaciones aplicará para lograr cada característica de las deseables en un algoritmo de cifrado.
3. Recuerde que un buen diseño deberá incluir operaciones como desplazamiento de bits, transposición, sustitución y XOR. Si lo logra hacer más sofisticado podrían incluir multiplicaciones y operaciones más complejas, solo verifique que las operaciones las pueda revertir. Es importante verificar el diseño del algoritmo antes de implementarlo.
4. Implemente su diseño y programe su pequeño algoritmo de cifrado en el lenguaje de su preferencia, se recomienda hacer uso de un lenguaje como C/C++ que facilita la manipulación con operaciones a nivel de bits, no obstante puede seleccionar el lenguaje de su preferencia. Para probar su funcionamiento, el programa deberá de pedir una cadena alfanumérica a cifrar de hasta 100 caracteres y una clave simétrica de máximo 20, tras ejecutar el algoritmo generara un texto cifrado. Posteriormente se le proporcionará al

programa el texto cifrado y la misma clave y deberá generar el texto original al volver a pasar por el algoritmo de descifrado.

5. El entregable de esta práctica son el diseño mediante una presentación de 5 minutos y la demostración del programa funcionando. Para que sea válido el entregable deberá al menos realizar 2 operaciones diferentes que generen difusión (como transposición, rotación o desplazamientos de bits) y dos operaciones que generen confusión (sustitución, XOR, sumas, multiplicaciones, etc) y útiles para los algoritmos simétricos.
6. La calificación dependerá del funcionamiento correcto del algoritmo de cifrado y de la complejidad del diseño, a mayor complejidad mayor calificación. La evaluación será grupal (es decir la práctica no la revisará el profesor solo sino con el grupo). La evaluación se llevará a cabo con la siguiente rúbrica:

Equipo Evaluado:	
Nombre del Algoritmo:	
Diseño del algoritmo (10/10)	
Funcionamiento e implementación(30/30)	
Técnicas para generar difusión(22/22)	
Técnicas para generar confusión(22/22)	
Interfaz Gráfica(10/10)	
Presentación(6/)	
TOTAL PUNTOS:	

Entregables

- Algoritmo de cifrado simétrico.
- Evidencias de correcto funcionamiento.
- Manual técnico del diseño del algoritmo.