Universidad de Los Andes Bogotá D.C.
Infraestructura computacional

Informe caso 3 - Seguridad

Juan Sebastián Pedraza - 202110301
Ana Sofía Padilla Daza - 202021748
Milton Andrés Mesa Manrique – 202025521

Pruebas

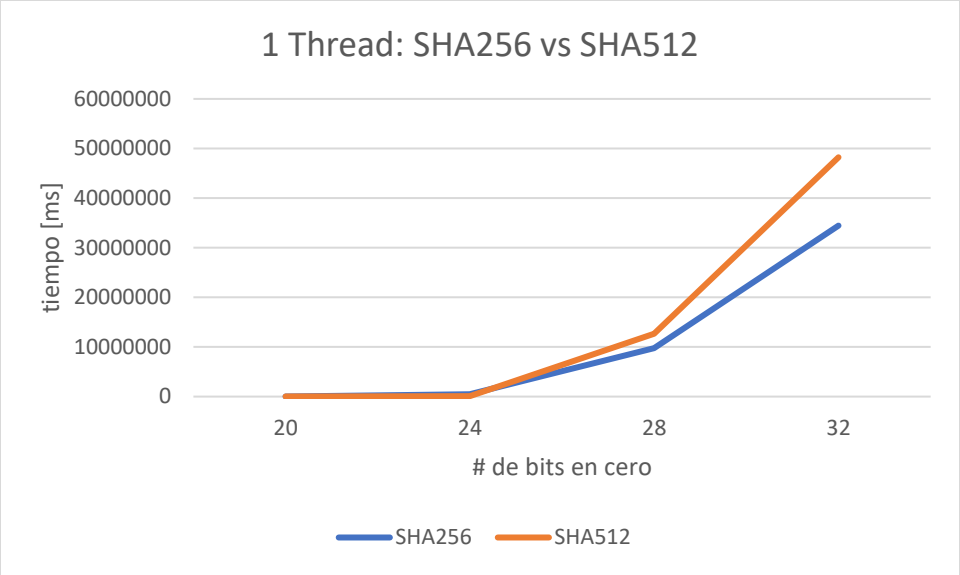
1. Algoritmo SHA 256

# de ceros	Tiempo con 1 thread	Tiempo con 2 threads
20	16516ms	11903ms
24	476556ms	158764ms
28	9756487ms	330184ms
32	34457098 ms	183446723 ms
36	ms	612885409 ms

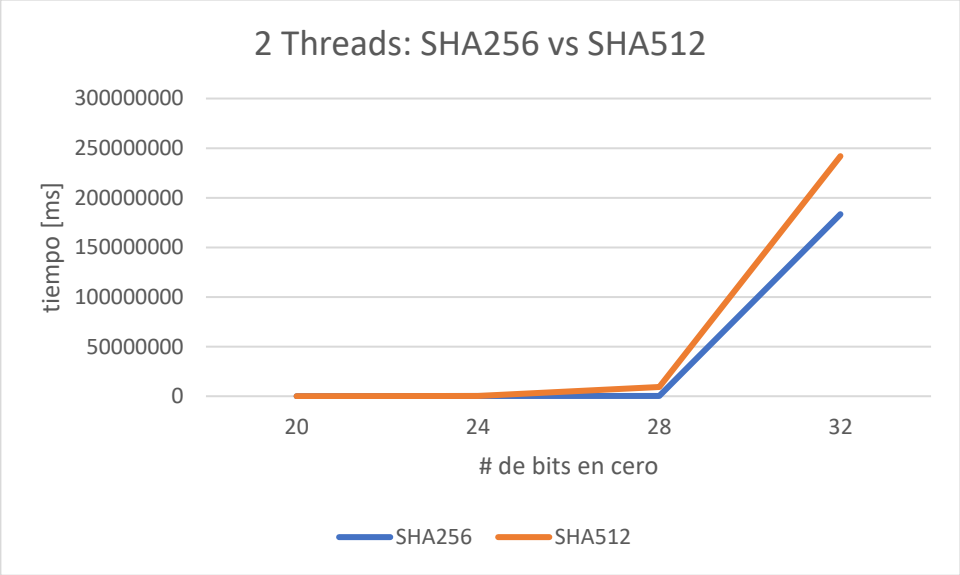
2. Algoritmo SHA 512

# de ceros	Tiempo con 1 thread	Tiempo con 2 threads
20	21429 ms	20345 ms
24	108957 ms	108677 ms
28	12653492 ms	9352783 ms
32	48230100 ms	24190978 ms
36	>1*10^7 ms	67370092 ms

3. Gráficas
    1. Gráfica de 1 thread:



2. Gráfica de 2 threads:



Cálculos

1. Identifique la velocidad de su procesador, y estime cuántos ciclos de procesador toma, en promedio, generar y evaluar un valor para determinar si cumple o no con la condición buscada. Escriba todos sus cálculos.

   Velocidad del procesador: 2.1 GHz

$$Frecuencia = \frac{1}{tiempo}$$

$$tiempo = \frac{1}{\text{Fequencia}}$$

$$tiempo\ de\ un\ ciclo\ de\ reloj = \frac{1}{2.1 * 10^9}$$

$$tiempo\ de\ un\ ciclo\ de\ reloj \approx 4.7619 * 10^{-10}\ segundos$$

Tiempo de generar y evaluar un valor: 820 ns

Cliclos de generar y evaluar = tiempo promedio/tiempo de 1 ciclo

$$ciclos\ de\ generar\ y\ evaluar = \frac{820 * 10^{-9} segundos}{4.7619 * 10^{-10} segundos}$$

$$ciclos\ de\ generar\ y\ evaluar \approx 1722\ ciclos\ de\ reloj$$

2. Con base en los cálculos del punto anterior, calcule cuánto tiempo tomaría un programa monothread, en el peor caso (explorar todo el espacio de búsqueda).

   Tiempo en el peor caso = tiempo promedio de generar y evaluar un valor * número de búsquedas totales

$$Tiempo\ peor\ caso = 820 * 10^{-9} segundos * 10862674479$$
$$Tiempo\ peor\ caso \approx 8907.393\ segundos$$
$$Tiempo\ peor\ caso \approx 148\ minutos$$
$$Tiempo\ peor\ caso \approx 2\ horas\ y\ media$$

   Ciclos en el peor caso = Ciclos promedio de generar y evaluar un valor * número de búsquedas totales

$$Tiempo\ peor\ caso = 1722 * 10862674479$$
$$Tiempo\ peor\ caso \approx 1.87 * 10^{13}$$

Análisis y Entendimiento del Problema

1. Busque información adicional sobre los algoritmos de generación de códigos criptográficos de hash y responda las siguientes preguntas:
   a. ¿cuáles se usan hoy día?

Al año 2023, existen muchísimos algoritmos de cifrado como los SHA256 y SHA512. También existen otros como el Advanced Encryption Standard (AES) el cual es usado por organismos gubernamentales de varios países para realizar encriptado de mensajes con ***llaves simétricas****,*

soportando encriptado llaves de 128, 192 y 256 bits. Este algoritmo se considera invulnerable para todo tipo de ataques excepto los de fuerza bruta.

Este algoritmo utiliza cifrado simétrico para encriptar y desencriptar información. La información debe estar repartida en bloques de 128 bits. Los datos son puestos a través de varias rondas de cifrado con operaciones como sustitución de bits, trasposición y mezcla, para que sea más difícil de comprometer. Si bien este algoritmo no es para generar códigos de hash únicos, si sirve para la generación de códigos criptográficos. (Advanced Encryption Standard (AES), 2001)

SHA256 y SHA512:

Estos algoritmos fueron diseñados por las NSA y publicados para uso público y privado asimismo por el NIST en 2001. Estos algoritmos no son llaves criptográficas simétricas, sino que digieren un conjunto de datos cualquiera y lo convierte a un número único de longitud fija lamado "hash", de forma irreversible, es decir, a partir del hash no es posible obtener el archivo original, y al mismo tiempo, dicho hash solo pudo haber sido obtenido partiendo del archivo original.

Este algoritmo sirve para poder verificar la INTEGRIDAD y CONSISTENCIA del envío de información. Estos algoritmos son considerados ***FUERTES*** *debido a su poca probabilidad de que ocurran colisiones, es decir, de que haya un mismo hash para dos archivos originales distintos*.

b. ¿por qué dejamos de usar aquellos que se consideran obsoletos?

Hay que tener en cuenta que los ataques informáticos no son únicamente para afectar la confidencialidad o la autenticación, sino que también puede ser para afectar la integridad de la información.

Es por eso que la viabilidad de un algoritmo de Hash depende estrictamente de su capacidad para evitar colisiones. Con el conocimiento de las colisiones, un atacante podría elaborar archivos que generasen el mismo código de hash que el archivo original, y así comprometer ficheros o documentos valiosos. Los algoritmos que tienen alguna probabilidad media o alta de producir colisiones se consideran débiles. La mayoría de estas colisiones son accidentales o probabilísticas en principio, pero se debe evitar a toda costa que se puedan elaborar métodos computacionales para producir colisiones a propósito y a demanda, pues estos son los algoritmos que se consideran obsoletos de manera definitiva.

c. ¿qué referencias bibliográficas usó para responder esta pregunta?

Federal Information Processing Standards Publication 197

https://web.archive.org/web/20150407153905/http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

https://www.ciberseguridad.eus/ciberglosario/sha-512

d. ¿por qué esas referencias tienen autoridad sobre este tema?

Es una publicación del 2001 de ***NIST Computer Security Resource Center*** el cual es una agencia de estandarización de seguridad informática de Estados Unidos.

La otra fuente proviene de la página oficial de la agencia de seguridad del País Vasco, en España. Por ser fuentes oficiales de carácter gubernamental (sea para fines públicos o privados) sabemos que tienen validez.

2. La tecnología blockchain se construyó a partir de la propuesta de bitcoin. Busque información sobre blockchain y presente un caso de uso en el contexto de la Universidad de los Andes donde sea útil la tecnología blockchain. Justifique su respuesta con argumentos concretos, en particular, responda las siguientes preguntas:
    a. ¿cuál (o cuáles) de los cuatro problemas de seguridad, de los estudiados en clase, resuelve blockchain en el caso presentado?

La tecnología de blockchain básicamente consiste en generar bloques de códigos criptográficos únicos que mantienen la integridad de la información. Esta tecnología puede ayudar a proteger los derechos de autor y la propiedad intelectual de las publicaciones de los trabajos de los estudiantes y profesores, especialmente aquellos que poseen más valor como las tesis e investigaciones de nivel universitario; permitiéndole a los autores de estos trabajos incluso saber cuándo y en dónde han sido citadas sus obras. Esto resuelve principalmente los problemas vistos en clase de suplantación y adulteración, garantizando **autenticidad e integridad de la información** contenida en los trabajos de la comunidad de la Universidad de los Andes. (Santander, 2023)

    b. ¿cómo los resuelve? (es decir, divida la tecnología en componentes e identifique qué parte, o partes, de la tecnología están involucradas en la resolución del problema y cómo lo resuelven).

Los resuelve generando tokens únicos que se registran en la blockchain de manera irrepetible e irreversible, permitiendo que los autores del documento tengan control sobre la autoría de su trabajo y siempre sea posible verificar el momento y el lugar en la cadena de bloques en que se genero dicha “transacción” o certificado.

Referencias

1. *Advanced encryption standard (AES)*. (2001). https://doi.org/10.6028/nist.fips.197
2. Santander. (2023, July 11). *¿Para qué se usa “blockchain”?*

   https://www.santander.com/es/stories/blockchain-usos-futuros
3. *SHA-512*. (n.d.). BCSC. https://www.ciberseguridad.eus/ciberglosario/sha-512