Campus Monterrey

Mónica Andrea Ayala Marrero	*A01707439*
José Eduardo Puentes Martínez	*A01733177*
Hedguhar Domínguez González	*A01730640*
Axel Uzeta Gomez	*A00829417*

HW 03 - Hash Functions

Análisis y diseño de algoritmos avanzados (Gpo 570)

Profesor:

Salvador E. Venegas-Andraca

Julio 13, 2023

A lo largo de este documento se analizará la estructura y comportamiento del algoritmo SHA-512(Secure Hash Algorithm 512 bits), explicando detalladamente el funcionamiento del mismo y sus características, así como de dar una introducción sobre qué son las funciones Hash para así poder entender todo el tema en general.

Primeramente y a manera de introducción al tema explicaremos qué son las funciones Hash estas entran principalmente en el área de la criptografía, una función Hash es un algoritmo que puede ser presentado en código, dicho algoritmo recibe "x" entrada ya sean datos de cualquier tipo presentados en mensajes o archivos para posteriormente transformar esta "x" entrada en una cadena de longitud fija ya sea de tamaño 128 bits, 256 bits etc. o 512 bits que sería el que posteriormente analizaremos, esta cadena sería la salida que la función hash daría, la longitud de dicha salida no tiene que ver necesariamente con la "x" entrada que dimos sino que tiene que ver la función hash que se utilice, a esta salida la cual es la cadena de longitud fija que mencionamos anteriormente es lo que conocemos como un "Hash".

Las funciones hash cuentan con distintas características principales por ejemplo al nosotros obtener la salida la cual es una cadena de longitud fija, posteriormente será prácticamente imposible el poder hacer el procedimiento en reversa, es decir será muy poco probable el poder obtener la entrada original a partir del hash, esto va de la mano con que las funciones hash tienen la característica de generar un hash distinto para cada entrada ingresado lo cual provoca una relación uno a uno en la cual para cada entrada existe un hash distinto y en caso de que se realice una modificación aunque sea mínima esto provocará un cambio total en el cadena resultante.

Ahora bien una vez explicado de manera general cómo funcionan las funciones hash es importante mencionar las áreas en las cuales es aplicado este algoritmo, como mencionaba al principio estas funciones son utilizadas principalmente en el área de la criptografía y seguridad, de manera que se puedan verificar y mantener la integridad de los datos, gracias a que como mencionamos anteriormente al nosotros realizar un cambio en la entrada se generará una cadena totalmente distinta. Además se emplea en el uso de contraseñas con mayor seguridad de manera que en lugar de usar la contraseña tal cual esta sea reemplazada por el hash generado.

Ya que explicamos en general las funciones hash como funcionan, el cómo generan distintas longitudes de cadenas fijas según el tipo que se utilice, conociendo esto es que damos entrada a uno de los tipos de funciones Hash más utilizado el cual es el SHA-512 el cual produce un Hash de 512 bits lo cual es una gran longitud para una función hash, siendo así uno de los algoritmos más seguros a utilizar, dicho algoritmo de igual manera entra en el área del minado de criptomonedas por su gran eficiencia.

Ahora bien ya adentrándonos más en el hash SHA-512 y el cómo este funciona y se estructura, a continuación explicaremos la serie de pasos que este algoritmo sigue para funcionar:

- **Mensaje de entrada**

    - Se envía el mensaje de entrada del cual se desea generar el Hash.
    - Se realiza una división en bloques del mensaje (Hash Buffer), cada bloque correspondiente a 1024 bits cada uno. (En caso de que el mensaje no cumpla las condiciones para hacer la división en bloques de 1024 bits el mensaje se rellenará para hacerlo múltiplo de 1024).

- **Valores iniciales**

    - Se definen los puntos de partida para realizar el proceso, conocido como hash inicial.
    - Para este escenario en el cual estamos con el SHA-512 se utiliza un hash inicial 512 bits, el cual se divide en 8 secciones cada una de 64 bits.

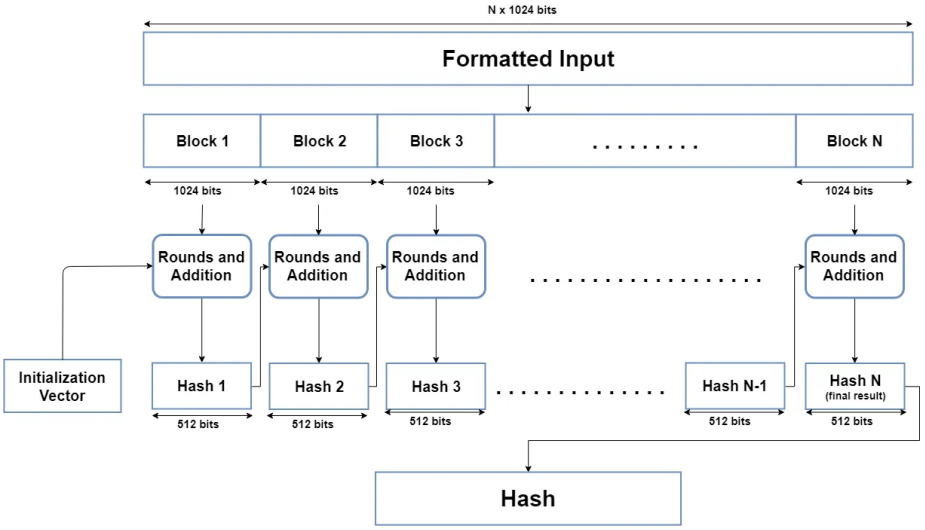
- **Procesado de mensajes y operaciones**

    - Cada bloque de los mencionados anteriormente se procesa en secuencia, la manera en la que se realizará el procesamiento en cada bloque será por rondas.
    - El procesamiento será desde el primer bloque hasta finalizar los bloques.
    - En cada ronda a realizar se aplican distintas operaciones matemáticas como combinaciones lógicas, aplicación de funciones no lineales, sumas modulares y rotaciones a nivel de bits, de esta manera se podrán transformar y hacer el procesamiento para cada bloque.
    - El proceso de rondas se hará por cada bloque una vez se finalice el proceso para un bloque se parara al siguiente, repitiendo esto hasta llegar al final.

- **Finalización del proceso**

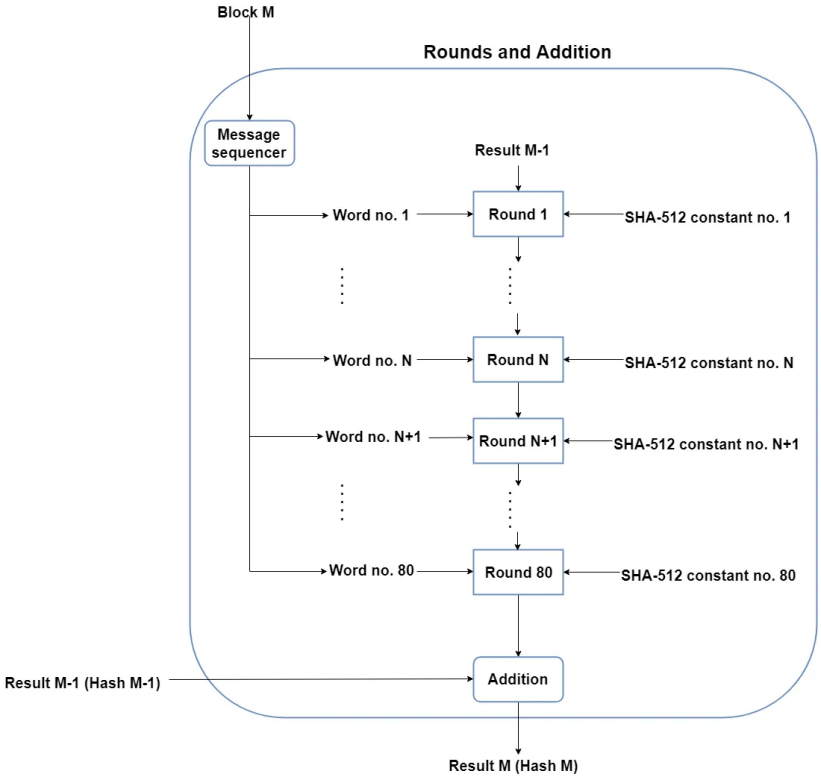
    - Ya que se ha finalizado los pasos anteriores para cada bloque, sólo queda un paso final el cual es hacer una vez más la mezcla y transformaciones para generar la cadena fija de 512 bits que caracteriza al SHA-512. Una vez dada esta cadena el proceso ha sido finalizado.

A continuación nos gustaría citar un par de imágenes las cuales muestran de manera más visual estos pasos, para poder comprender a qué nos referimos con los bloques y las rondas:



William Stallings, Cryptography and Network Security - Principles and Practise (Seventh Edition) referred for diagram. Diagram obtained from: medium.com by (Khaishagi, 2021). (Image 1.1)

Como podemos ver en la imagen 1.1 se visualiza la entrada recibida y como esta se divide en distintos bloques de 1024 bits como se mencionaba anteriormente en los pasos, posteriormente podemos ver la implementación de las rondas para cada bloque, pero para poder observar más las múltiples rondas que se realizan a un bloque es necesario dirigirnos a la imagen 1.2.



William Stallings, Cryptography and Network Security - Principles and Practise (Seventh Edition) referred for diagram. Diagram obtained from: medium.com by (Khaishagi, 2021). (Image 1.2)

En esta imagen 1.2 se puede ver la generación de las palabras de 64 bits antes mencionadas para cada bloque y como se aplica 80 rondas de las antes mencionadas para cada bloque, la razón por la cual se aplican 80 rondas para cada bloque es por motivos de seguridad. Cabe

mencionar que la cantidad de rondas varía según la función hash que se utilice siendo algunos algoritmos más veloces pero menos seguros, en el caso del SHA-512 con 80 rondas lo vuelve un algoritmo extremadamente seguro. Finalmente se realiza la suma modular y se obtiene el Hash.

Ya que hablamos más del comportamiento del algoritmo y su flujo general, nos gustaría adentrarnos más en su estructura matemática y los distintos recursos que utiliza para funcionar, a continuación listamos las principales estructuras matemáticas utilizadas y el papel que juegan en el SHA-512:

- **Operadores lógicos**
    - El algoritmo SHA-512 hace uso de los clásicos operadores lógicos que todos conocemos como los or, and y xor.
    - Se utilizan en las rondas mencionadas para transformar los valores durante cada ronda.

- **Sumas modulares**
    - El principal uso de la suma modular en el SHA-512 es el de juntar las palabras de 64 bits que se separan al inicio del proceso como mencionamos más arriba. Las sumas modulares se realizan a lo largo de todo el proceso, durante rondas y al finalizar el proceso como se observa en los diagramas.

- **Rotación a nivel de bits**
    - Van de la mano con las sumas modulares y es que las rotaciones de igual manera influyen en las palabras generadas de manera que las rotaciones se encargan de cambiar la posición de las palabras de 64 bits.
    - Se ejecutan durante cada ronda del algoritmo incrementando la aleatoriedad del algoritmo y por ende su seguridad.

- **Funciones no lineales**
    - Durante el proceso del algoritmo SHA512 se hace uso de las funciones no lineales, manteniendo así la no linealidad para mayor seguridad teniendo mayor resistencia a ataques de fuerza bruta como los que hemos mencionado en clases y el no permitir la identificación de patrones. Básicamente su objetivo es el de aumentar la seguridad ante distintos tipos de ataques.
    - Estas funciones se aplican en conjunto con los operadores lógicos.

Para finalizar esta investigación acerca del SHA-512 definitivamente podemos concluir que es uno de los más seguros y robustos de los de su tipo en cuanto a los procesos que este tiene y los recursos matemáticos con los cuales se lleva a cabo, esto se respalda debido a lo que

hemos estado viendo a lo largo del documento primeramente que genera un Hash de 512 bits uno de los más largos en los hash siendo prácticamente imposible que se genere un mismo hash para dos mensajes o que se pueda descifrar el hash para encontrar el mensaje original. Además se vuelve bastante resistente contra los ya conocidos y mayormente aplicados ataques de fuerza bruta, gracias la gran variedad y aleatoriedad que maneja el SHA-512 se vuelve prácticamente imposible en cuestión de tiempo poder realizar un ataque basado en fuerza bruta.

Y finalmente como parte de la conclusión que no mencionamos anteriormente es que ya es un algoritmo con mucha historia por lo que múltiples organizaciones hacen uso del incrementando así la confianza en el mismo, el SHA-512 y a pasado por miles de pruebas y revisiones de expertos, además de obtener distintas certificaciones y reconocimientos a lo largo del mundo por lo que es sin duda una de las mejores opciones a tomar en cuenta en el mundo de la ciberseguridad y criptografía.

Referencias:

Khaishagi, Z. (2021, December 7). Cryptography: Explaining SHA-512 - Zaid Khaishagi - Medium. Medium.
https://medium.com/@zaid960928/cryptography-explaining-sha-512-ad896365a0c1

Stallings, W. S. (2016). CRYPTOGRAPHY AND NETWORK SECURITY PRINCIPLES AND PRACTICE (7th ed.) [PDF]. Pearson.
http://staff.ustc.edu.cn/~mfy/moderncrypto/crypto7ed.pdf

Sharma, A. K. S. (2019). Design and Mathematical Structure of Cryptographic Hash Function SHA-512 [PDF]. ISSN.
https://www.researchtrend.net/ijtas/pdf/6%20%20Design%20and%20Mathematical%20Structure%20of%20Cryptographic%20Hash%20Function%20SHA-512%20ARUN%20KUMAR%20SHARMA%201263.pdf