# Parte 1, Investigación

**Juan Fernando De León - 17822**
**Jose Amado Garcia - 181469**
**Edgar Andree Toledo - 18439**
**Ricardo Antonio Valenzuela - 18762**
**Sara Zavala - 18893**

# Raw-mac y cascade

a. ¿Por qué el raw-mac es inseguro dentro de la construcción del CBC-MAC?

   CBC-MAC es seguro para mensajes de una longitud fija, por lo tanto por su cuenta no es seguro para mensajes de longitud variable. Esto quiere decir que una clave sólo debe usarse para mensajes de una longitud conocida, esto es inseguro ya que le brinda al atacante información para conocer el comportamiento de nuestro cifrado.

b. ¿Por qué el cascade function es inseguro dentro de la construcción HMAC?

   HMAC depende del tamaño de la clave que se utiliza, por eso el ataque más común en su contra es la fuerza bruta para averiguar dicha clave. HMAC también es mejors afectado por las colisiones. Se ha encontrado que es posible encontrar una cadena larga de ASCII y un valor aleatorio cuyo hash también será una cadena ASCII y ambos valores producir la misma salida HMAC, na cascade function perjudica la construcción de la HMAC debido a esta vulnerabilidad.

# PMAC (parallel MAC)

a. ¿Cómo se define su construcción?

   Es un método que agarra un cifrado de bloque y crea un eficiente código de autentificación de mensajes, que sea probablemente reducido en seguridad al cifrado de bloque padre. Utiliza dos claves de cifrado, la primera se usa en las funciones P, los bits de salida de las funciones P se les hace XOR, el resultado es encriptado con una función F que utiliza la segunda clave.

   Las funciones F son pseudo aleatorias, y las funciones P no deben ser tan complicadas y deben ser más rápidas que las F.

b. ¿Qué ventajas puede mencionar sobre esta construcción?
   i. Elimina colisiones.
   ii. Es completamente paralelizable
   iii. Funciona para todos los block ciphers.

c. ¿Qué desventajas puede mencionar sobre esta construcción?
   i. Depende mucho de la seguridad del block cipher que se esté utilizando.

# Carter-Wegman MAC

a. ¿Cómo se define su construcción?

   Este se basa en la idea de MAC una sola vez,  se usa una función pseudoaleatoria para permitir el uso de una clave secreta muchas veces para futuros mensajes. Se suele utilizar una función “universal” hash para convertir el mensaje de entrada en una cadena corta.

b. ¿Qué ventajas puede mencionar sobre esta construcción?
   i. Utilización de un hash universal.
   ii. Es bastante rápido por su hash universal.
   iii. Es seguro y se evitan colisiones.
   iv. Se toma como referencia para crear otras implementaciones con la misma idea de un Hash Universal.

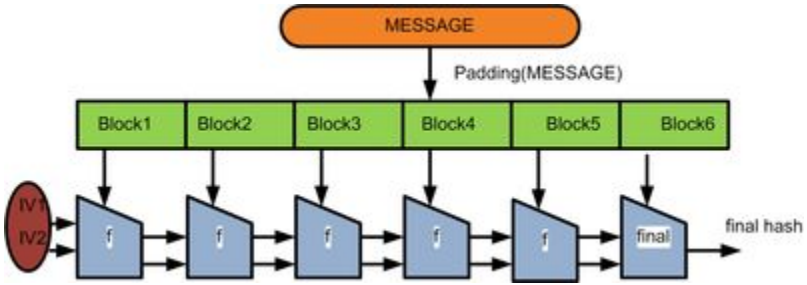
c. ¿Qué desventajas puede mencionar sobre esta construcción?
   i. Es bastante rápido en procesadores modernos, sin embargo es poco eficiente en sistemas antiguos.

# Relación el SHA-256 con:

Una función hash es un algoritmo que transforma un conjunto arbitrario de elementos de datos, como puede ser un fichero de texto, en un único valor de longitud fija (el "hash"). El valor hash calculado puede ser utilizado para la verificación de la integridad de copias de un dato original sin la necesidad de proveer el dato original. Esta irreversibilidad significa que un valor hash puede ser libremente distribuido o almacenado, ya que sólo se utiliza para fines de comparación

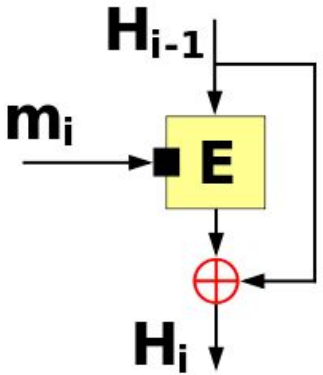
# Merkle-Damgard function

La construcción Merkle-Damgård mostró que la seguridad de la función hash depende de la seguridad de la función de compresión. Varios ataques a las funciones hash basadas en la construcción de Merkle-Damgård motivaron a los investigadores a proponer diferentes construcciones criptográficas para mejorar la seguridad de las funciones hash contra los ataques diferenciales y genéricos.



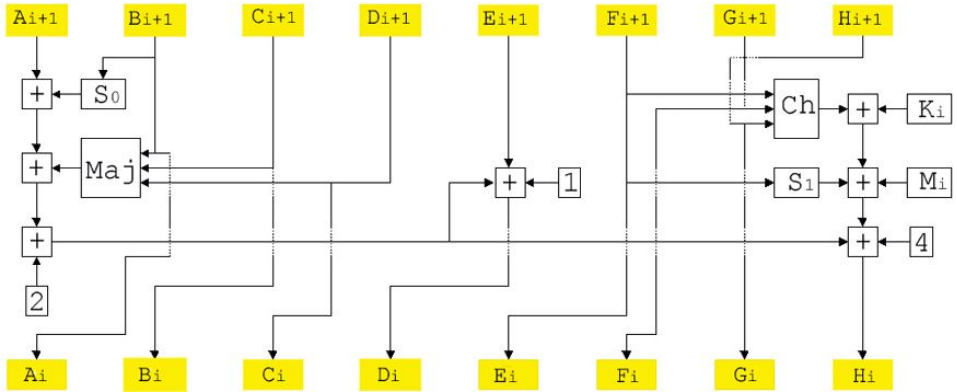
# Devies-Meyer compression function

La función hash de Davies-Meyer es una construcción para una función hash basada en un cifrado de bloque, donde la longitud en bits del resultado del hash es igual a la longitud del bloque del cifrado de bloque. Una función hash es un algoritmo criptográfico que toma cadenas de entrada de longitud arbitraria o muy grande y las asigna a cadenas de salida cortas de longitud fija.



# SHACAL-2

SHACAL-1 y SHACAL-2 son cifrados en bloque basados en el estándar Secure Hash. Fueron propuestos por Helena Handschuh y David Naccache mientras ambos trabajaban para la ahora desaparecida compañía de tarjetas inteligentes, Gemplus International. SHACAL-1 es un cifrado de 80 bloques redondos construido sobre la función de compresión SHA-1. Admite un bloque de 160 bits con tamaños de clave de entre 128 y 512 bits. SHACAL-2 es un cifrado de 64 bloques redondos construido sobre la función de compresión SHA-256 y admite un bloque más grande de 256 bits.



# SHA1

a. ¿Es el SHA1 seguro? ¿Por qué?

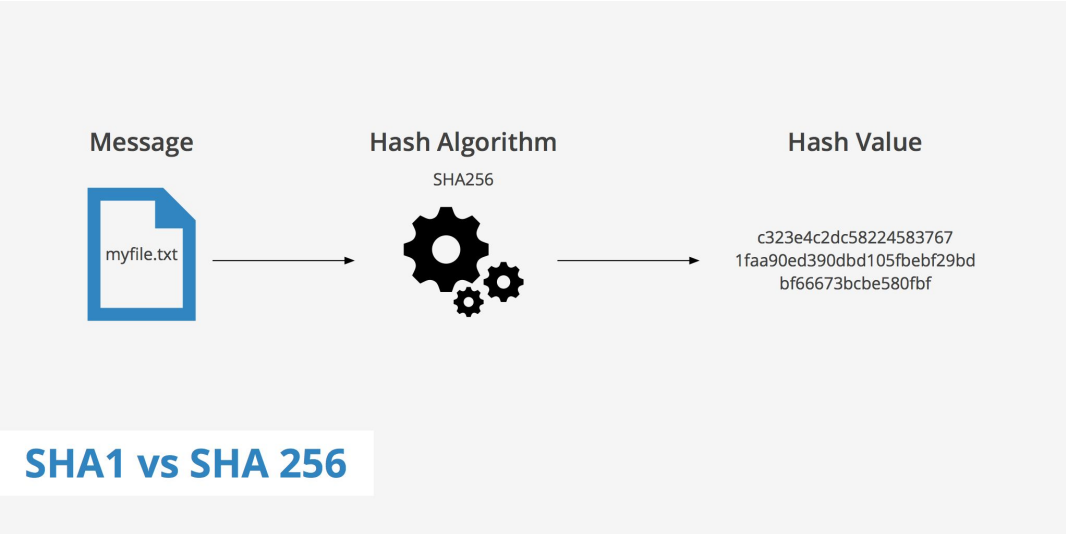
**SHA-1**, abreviatura de Secure Hash Algorithm 1, **fue creado en 1995 por la NSA,** ganando mucha popularidad en los años posteriores. A pesar de esto, el SHA1 **no es seguro.**

Un grupo de investigadores de Google y del CWI de Amsterdam han realizado el primer ataque de colisión de hash a SHA-1.

Al igual que cualquier algoritmo de cifrado, SHA-1 transforma un mensaje a una larga ristra de números y letras que sirven como huella criptográfica (hash) para ese mensaje. El problema es cuando **ese mismo valor de hash es producido para dos mensajes diferentes**, lo cual puede ser explotado para falsificar firmas digitales y poder interceptar y descifrar comunicaciones cifradas con este cifrado.

# HMAC-SHA1-96

SHA1-96 es lo mismo que SHA1, ambos calculan un hash de 160 bits, es solo que SHA1-96 trunca e incrusta un valor de hash de 96 bits en el paquete. Por esto, podemos concluir que este no es seguro debido a las razones que hacen SHA1 poco seguro,  demostradas previamente



# Bibliografía


- https://www.geeksforgeeks.org/hmac-algorithm-in-computer-network/
- https://www.cs.ucdavis.edu/~rogaway/ocb/pmac-bak.htm
- https://pdfs.semanticscholar.org/5837/89c89b0f8abfe0751679a4a330121b9b7f4c.pdf
- https://www.wil.waw.pl/art_prac/Message_Authentication.pdf

# Referencias:


Leurent, G., Bouillaguet, C. y Fouque, PA (2009). SIMD es un resumen de mensajes. Envío a la competencia NIST SHA-3 (Ronda 2) .

Hong, S., Kim, J., Kim, G., Sung, J., Lee, C., & Lee, S. (2003, December). Impossible differential attack on 30-round SHACAL-2. In International Conference on Cryptology in India (pp. 97-106). Springer, Berlin, Heidelberg.

Gilbert, H., & Handschuh, H. (2003, August). Security analysis of SHA-256 and sisters. In International workshop on selected areas in cryptography (pp. 175-193). Springer, Berlin, Heidelberg.