INSTITUTE OF ENGINEERING
PULCHOWK CAMPUS

Network Security and Analysis

M.Sc in Information and Communication Engineering

HASH FUNCTION

Presented by:

Bibek Gautam (080msice005)

Sujal Subedi (080msice018)

Submitted to:

Asst. Prof. Anku Jaiswal
Department of Electronics and Communication Engineering, Pulchowk Campus

Agenda

- Background
- Hash function
- Properties
- Popular Hash Function
- Applications
- Creating a digital signature
- Secure Hash Algorithm(SHA)
- SHA-512
- Steps For SHA-512 Logic

Message Authentication

- Authentication is concerned with protecting, confidentiality, integrity, authentication and non-repudiation
- Three methods used for message authentication:
  - message encryption
  - message authentication code (MAC)
  - hash Function

Hash Function

- Hash function are mathematical function used in cryptography.
- It takes various inputs (messages or data) and transforms them into fixed-length strings of characters
- Hash function generate a unique “fingerprint” for each input.

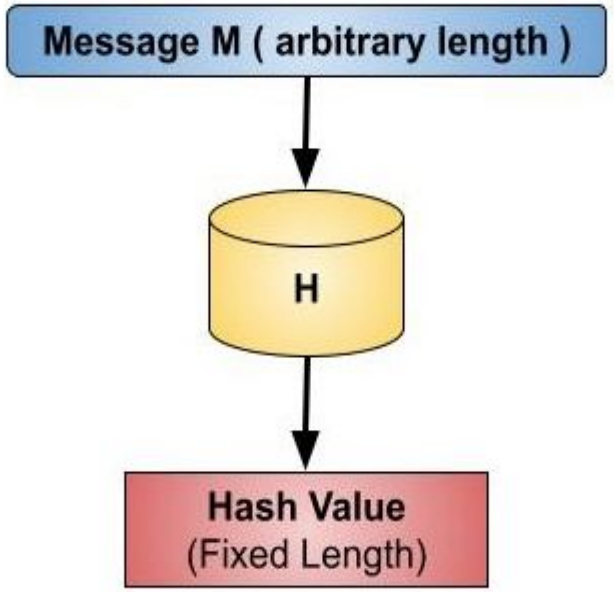


Figure: Hash Generation process

Hash Function

Properties of Hash Function

- **Fixed Output Size:** Produces a fixed length output for any arbitary input size.
- **Pre-Image Resistance** (one-way trip)**:**computationally infeasible to find x such that H(x)=h
- **Second Pre-Image Resistance:** given an input and its hash, it is computationally infeasible to find $y \neq x$ such that $H(y) = H(x)$
- **Collision Resistance:** computationally infeasible to identify two different inputs of any length that produce the same hash.
- **Efficiency of Operation:** For any given x Computation of h(x) is relatively easy and considerably faster than symmetric encryption.

Hash Function

Popular Hash Functions

- **Message Digest (MD):** MD2, MD4, MD5, and MD6 are members of the MD family. It was adopted as the RFC 1321, Internet Standard. It is a 128-bit hash function.
- **Secure Hash Function (SHA):** four SHA algorithms which make up the SHA family are SHA-0, SHA-1, SHA-2, and SHA-3. SHA-512 is one of the four SHA variants in the SHA-2 family.
- **CityHash:** non-cryptographic hash function that is designed for fast hashing of large amounts of data. It is optimized for modern processors and offers good performance on both 32-bit and 64-bit architectures.
- **BLAKE2:** a fast and secure hash function that improves upon SHA-3. widely used in applications like cryptocurrency mining that need fast hashing.

Hash Function

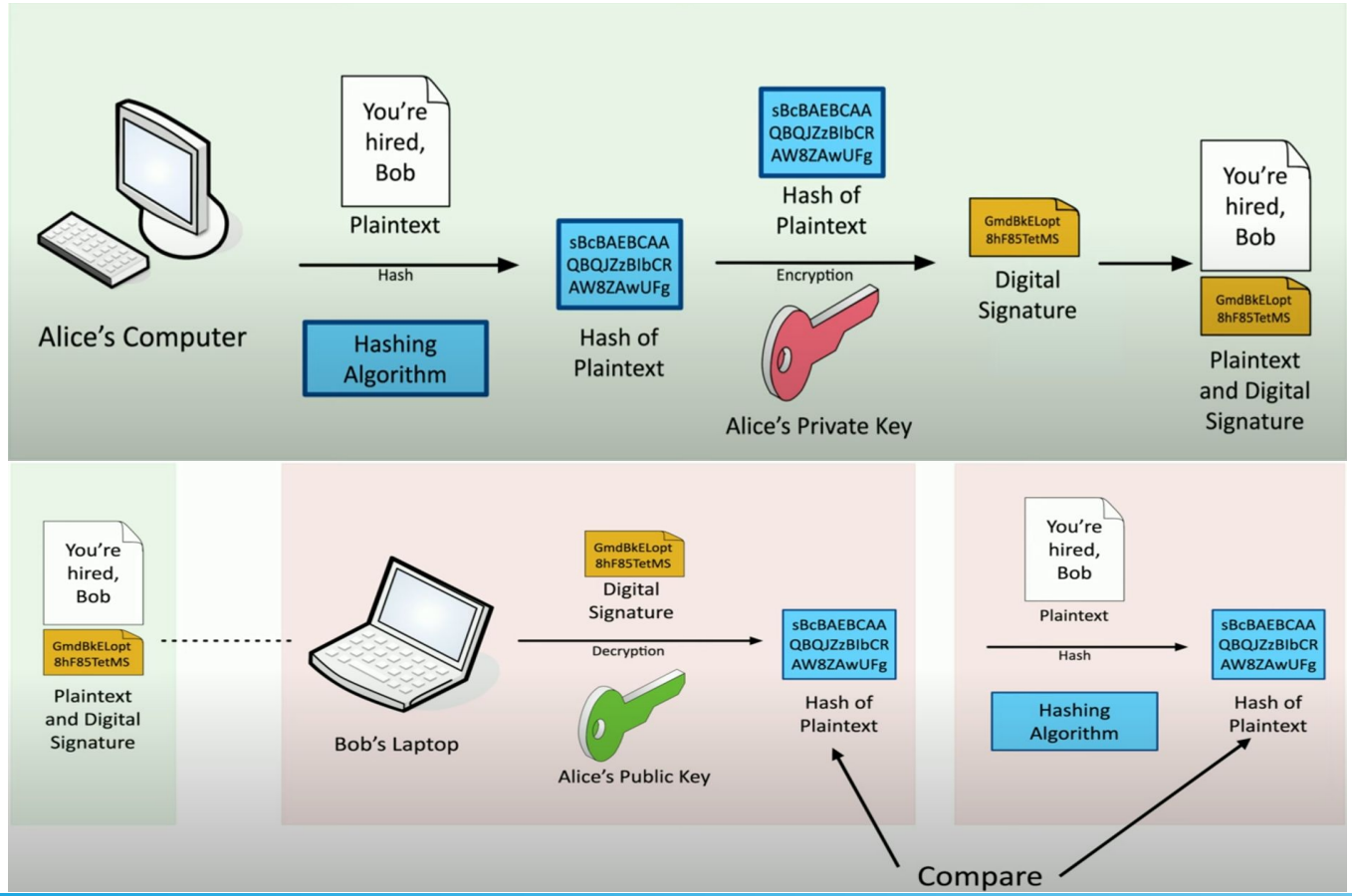
Applications:

- Password: Hash of the password is stored by operating system
- **Intrusion detection:** store H(f) for each file on the system and secure the hash value.
- **Digital Signature**

Hash Function Application in Digital Signature

Sender side

Receiver side



Secure Hash Algorithm(SHA)

- Developed by National Institute of Standards and Technology (NIST) as an U.S. Federal Information Processing Standard (FIPS)
  - SHA-0 (1993 AD)
  - SHA-1 (1995 AD)
  - SHA-256(2002 AD)
  - SHA-384(2002 AD)
  - SHA-512 (2002 AD)
- Developed in 1993 AD and based on hash function MD4
- SHA is designed to provide a different hash even if only one character in the message changes

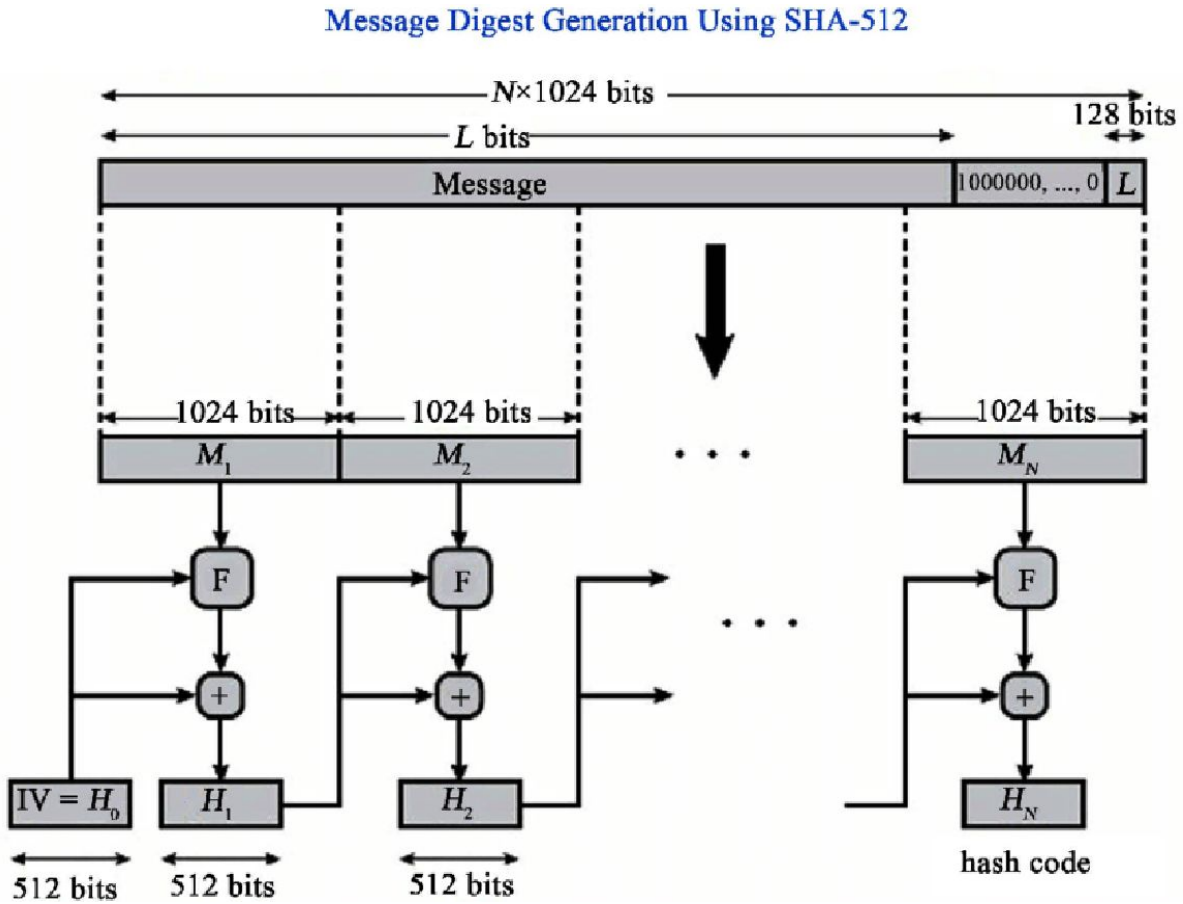
Secure Hash Algorithms(SHA)

	SHA-1	SHA-224	SHA-256	SHA-384	SHA-512
Message Digest Size	160	224	256	384	512
Message Size	$< 2^{64}$	$< 2^{64}$	$< 2^{64}$	$< 2^{128}$	$< 2^{128}$
Block Size	512	512	512	1024	1024
Word Size	32	32	32	64	64
Number of Steps	80	64	64	80	80

SHA-512

- Secure Hash Algorithm-512
- Message is divided in to plain text block of 1024 bits
- Each plain text block is sub-divided into 80 words of 64-bit
  - 16 words formed just by dividing the plain text block by 64 bit each
  - Rest 64 words are formed by conducting different operations like rotate, shifting, and, or on the plain text
- The words are processed 80 times on at a time and the result is stored in a hash buffer (a-g)
- The result in the buffer after the 80 round gives the immediate hash value

SHA-512


Message Digest Generation Using SHA-512
N×1024 bits
128 bits
L bits
Message
1000000, ..., 0
L
1024 bits
1024 bits
1024 bits
M1
M2
MN
F
F
F
+
+
+
IV = H0
H1
H2
HN
512 bits
512 bits
512 bits
hash code

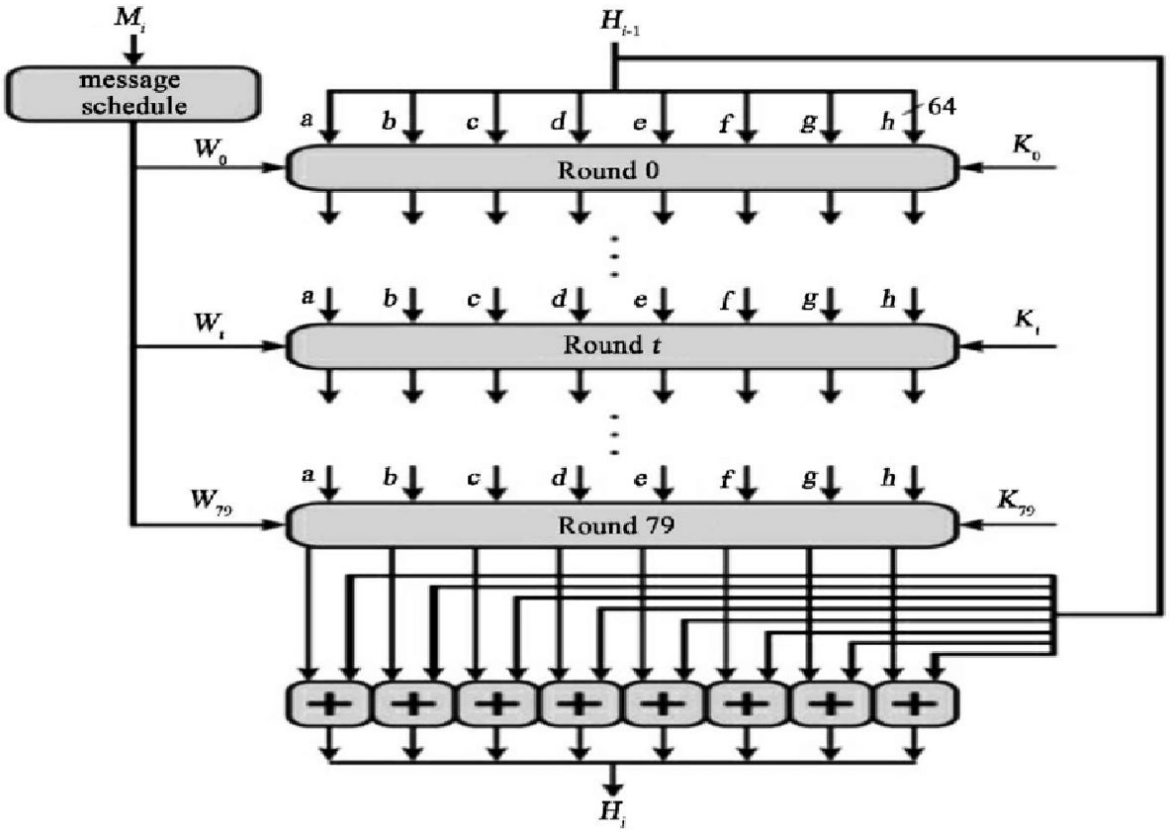
Steps for SHA-512 Logic-[1]

1. **Append padding bits**
   - Padding is done until the length of the string is < (message_length mod (1024 – 128))
   - Padding consists of a single-1 bit followed by the necessary number of 0-bits
2. **Append length**
   - A block of 128 bits is appended to the message
   - Sequence of 1024-bit plain text blocks $M_1, M_2, \ldots M_N$ are made
3. **Initialize hash buffer**
   - A 512-bit buffer is used to hold the hash function
   - The buffer can be represented as eight 64-bit registers (a,b,c,d,e,f,g,h)
   - These registers are initialized as hexadecimal values

Steps for SHA-512 Logic-[2]

4. Processing of the Plain text blocks

- Message block is divided into 80 words of 64-bit
- The hash buffers are processes with each word and updated
- On each round, different logical operations are performed
- Finally, after 80 rounds the immediate hash value is obtained



Steps for SHA-512 Logic-[3]

5. Output

- Each 1024-bit block generate a hash code for its block
- The hash code of the previous block is used for the next successive block
- After all N 1024-bit blocks have been processed, the output from the N^{th} stage is the 512-bit Final Hash Code

Thank You !