

Criptografía y Seguridad de Datos

Autenticación de mensajes y Resumen criptográfico (*hash*)

Carlos Figueira.

Universidad Simón Bolívar

Basado en láminas del Profesor

Henric Johnson (<http://www.its.bth.se/staff/hjo/>

henric.johnson@bth.se)

Contenido

- Enfoques de Autenticación de mensajes
- Funciones de resumen criptográfico seguro y HMAC

Autenticación

- Requerimientos. Debe ser capaz de verificar que:
 1. Mensaje provino del aparente autor o fuente
 2. El contenido no ha sido alterado
 3. Fue enviado en cierto orden o fecha (a veces)
- Protección contra ataques activos (falsificación de datos y transacciones)

Enfoques de autenticación de mensajes

- Usando cifrado convencional
 - Requiere clave compartida únicamente por emisor y receptor
- Autenticación sin cifrado
 - Una etiqueta agregada a cada mensaje
- Código de autenticación de mensaje (*Message Auth. Code MAC*)
 - Se calcula un MAC como una función del mensaje y la clave. $MAC = F(K, M)$

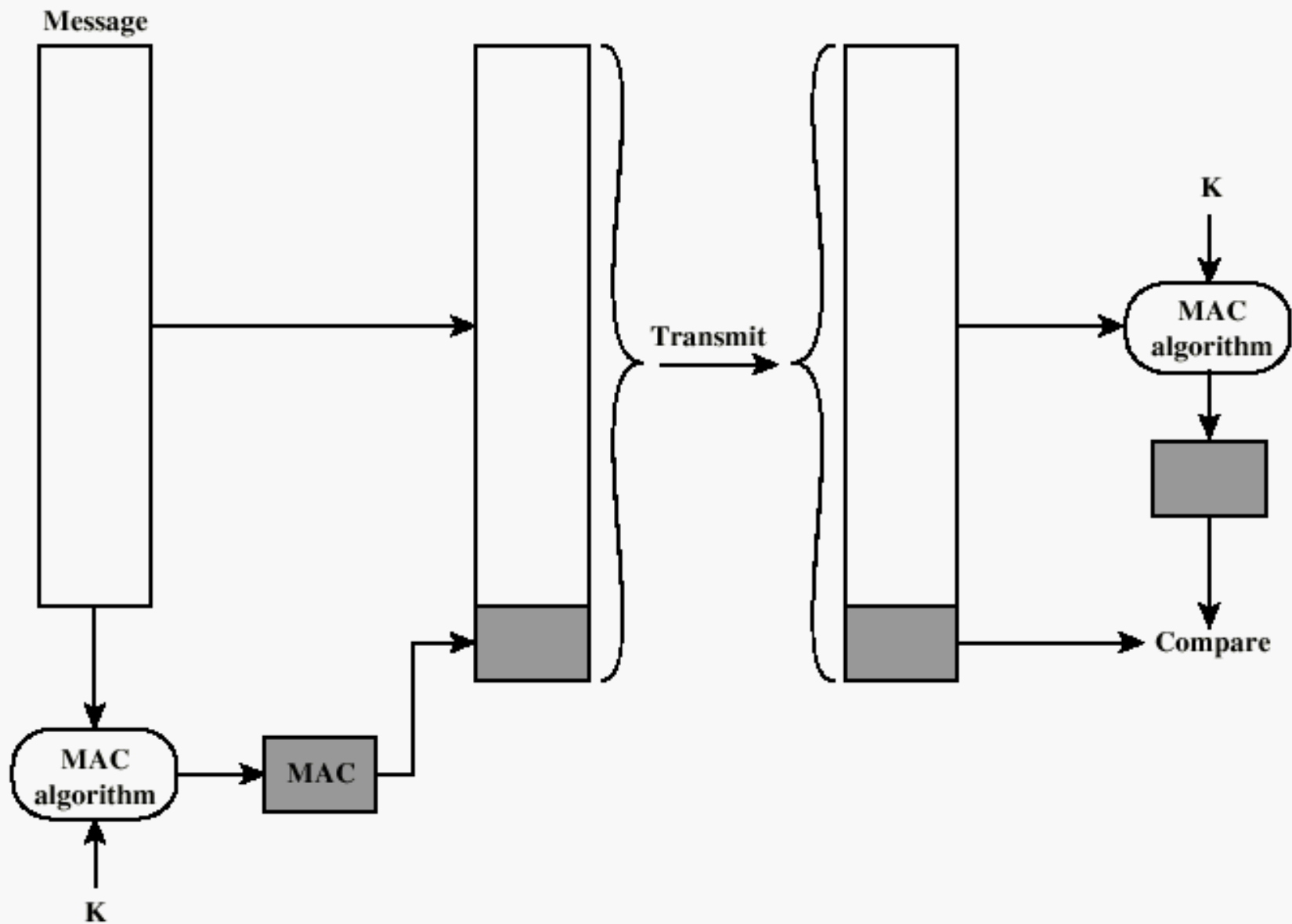
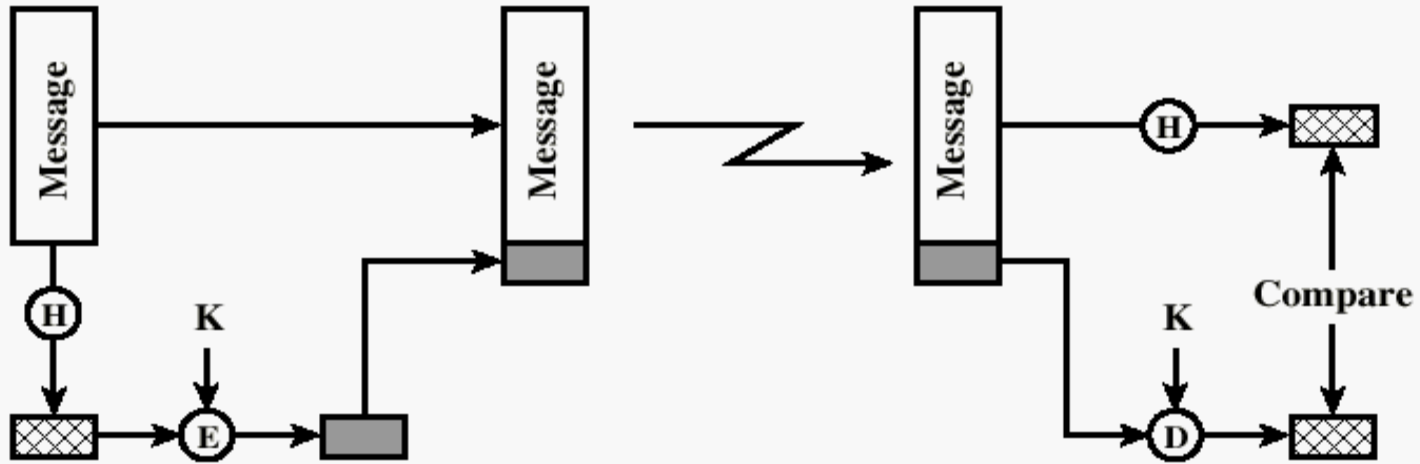
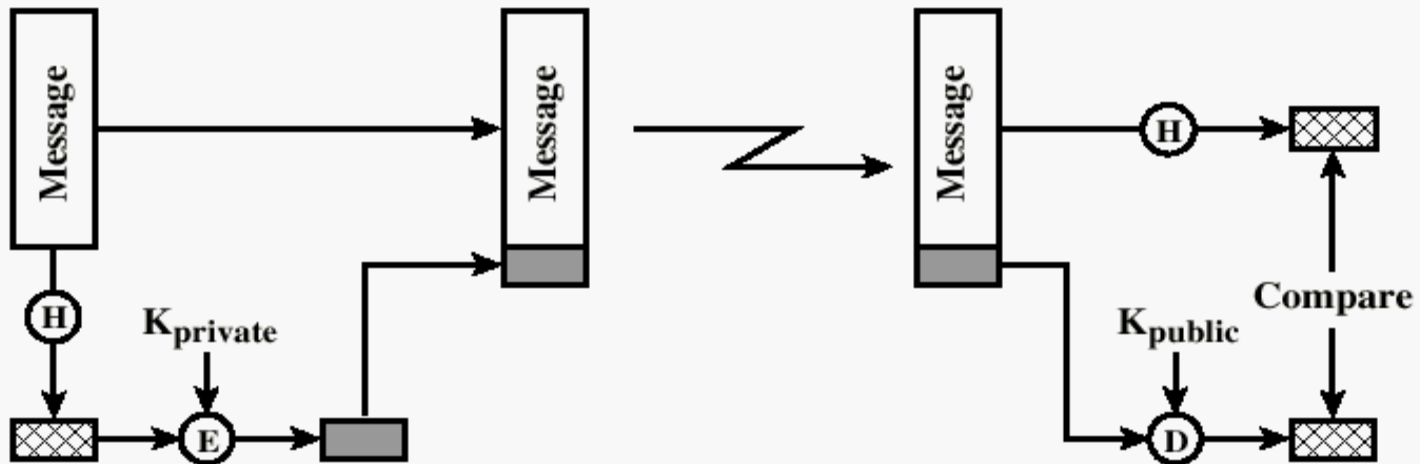


Figure 3.1 Message Authentication Using a Message Authentication Code (MAC)

Resumen (*hash*)



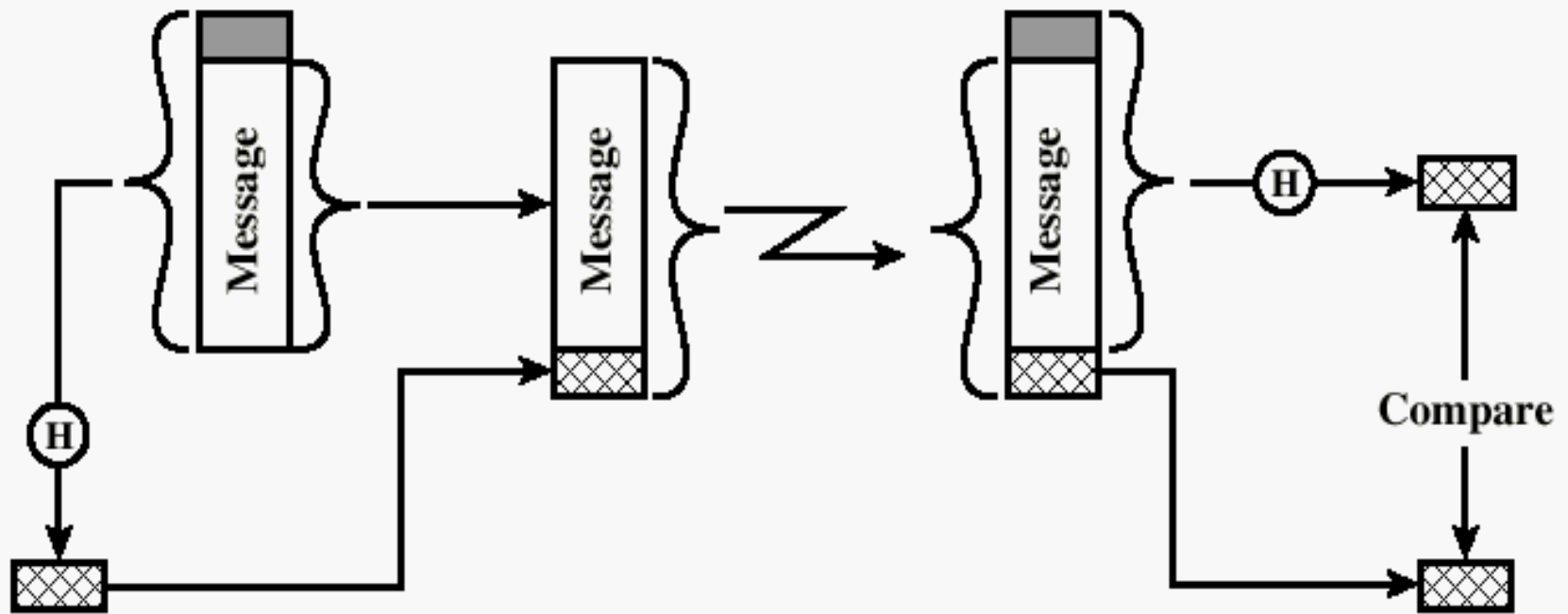
(a) Using conventional encryption



(b) Using public-key encryption

Resumen sin cifrado

- El valor secreto se agrega antes del resumen, pero no se envía



(c) Using secret value

Funciones de resumen seguro

- Objetivo: generar *huella*. Propiedades:
 1. Aplicable a bloques de cualquier tamaño
 2. Salida de tamaño fijo
 3. $H(x)$ fácil de calcular para cualquier x
 4. (*Inversa*) Para un resumen h , que no sea *computacionalmente factible* encontrar x tal que $H(x) = h$
 5. (*Colisión*) Que no sea computacionalmente factible encontrar un par (x,y) tal que
$$H(x) = H(y), \text{ para } y \neq x$$

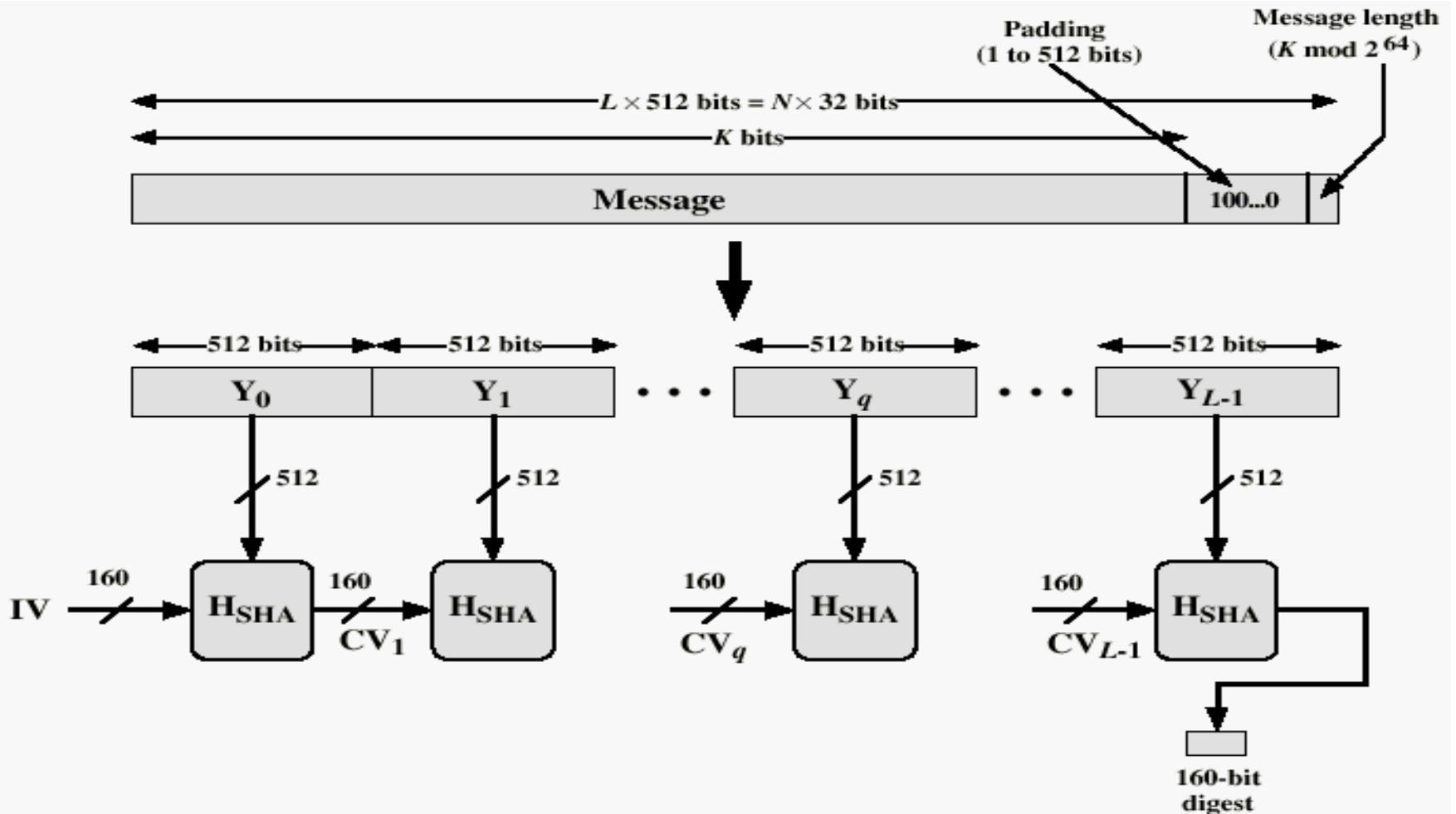
Función simple: XOR

	bit 1	bit 2	• • •	bit n
block 1	b_{11}	b_{21}		b_{n1}
block 2	b_{12}	b_{22}		b_{n2}
	•	•	•	•
	•	•	•	•
	•	•	•	•
block m	b_{1m}	b_{2m}		b_{nm}
hash code	C_1	C_2		C_n

Figure 3.3 Simple Hash Function Using Bitwise XOR

- Mejora si aplicamos desplazamiento circular de 1-bit del resumen después de procesar cada bloque.

Resumen usando SHA-1 (desarrollado por NSA)



Otras f. de resumen seguro

	SHA-1	MD5	RIPEMD-160
Longitud	160 bits	128 bits	160 bits
Unidad bás. de proc.	512 bits	512 bits	512 bits
Pasos	80 (4 rondas de 20)	64 (4 rondas de 16)	160 (5 pares de rondas de 16)
Tam. máx. entrada	$2^{64}-1$ bits	∞	∞

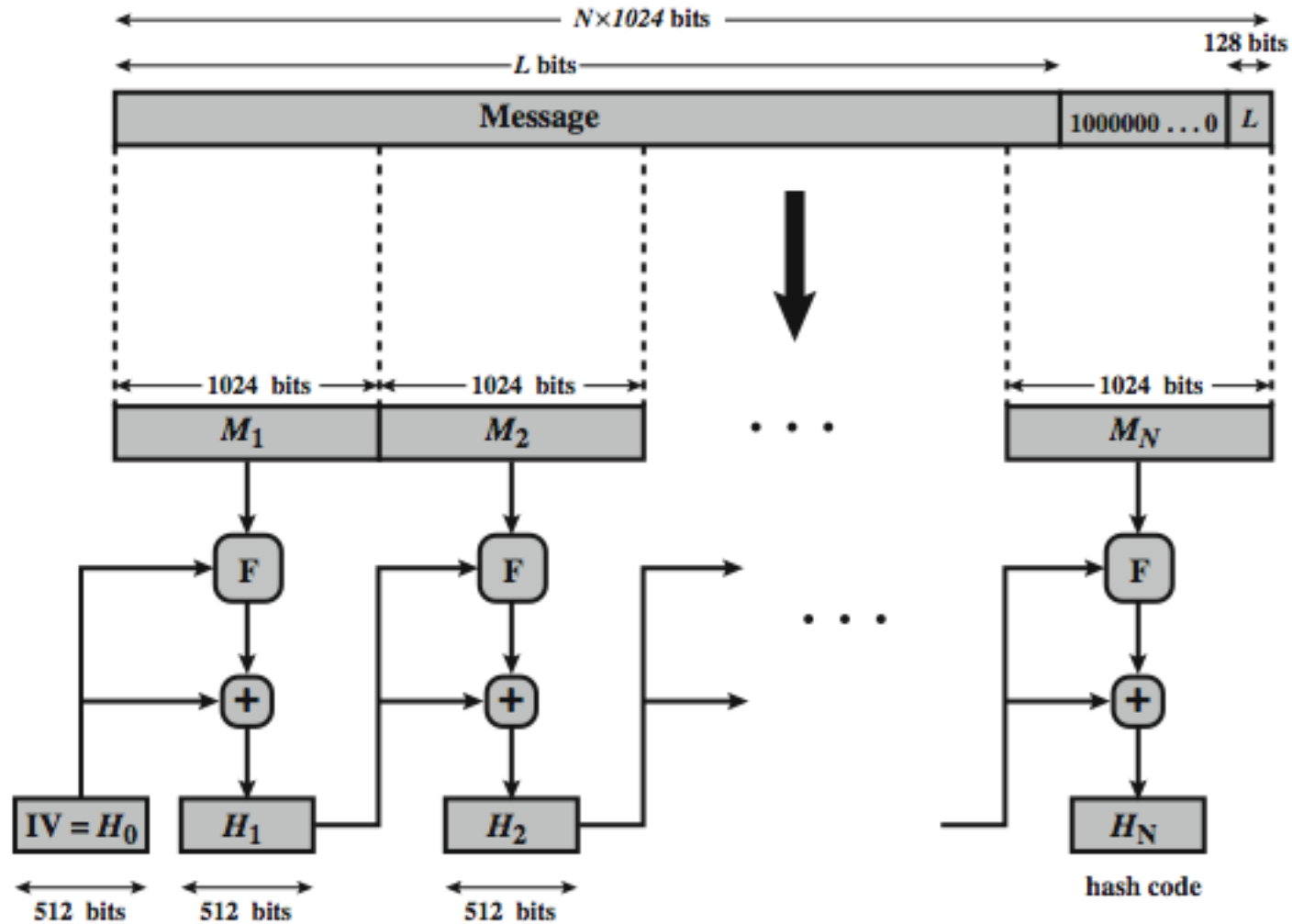
Estándar de resumen criptográfico revisado

- NIST publicó revisión FIPS 180-2 in 2002
- Agrega 3 versiones adicionales de SHA
 - SHA-256, SHA-384, SHA-512
- Diseñado para compatibilidad con seguridad superior provista por AES
- Similar a SHA-1 en estructura y detalles =>
 - análisis debe ser similar
 - Pero niveles de seguridad mayores

Versiones de SHA

	SHA-1	SHA-224	SHA-256	SHA-384	SHA-512
Tamaño del resumen	160	224	256	384	512
Tamaño del mensaje	$< 2^{64}$	$< 2^{64}$	$< 2^{64}$	$< 2^{128}$	$< 2^{128}$
Tamaño del bloque	512	512	512	1024	1024
Tamaño de palabra	32	32	32	64	64
Num. De pasos	80	64	64	80	80

SHA-512



$+$ = word-by-word addition mod 2^{64}

Función de compresión (F)

SHA-512

- Procesa el mensaje en bloques de 1024 bits
- consiste en 80 rondas
 - Actualizan un registro de 512-bit
 - Usan un valor W_t de 64-bit derivado del bloque actual del mensaje
 - Y una ronda constante basada en raíz cúbica de los primeros 80 números primos

Ataques

- De *preimagen*: El atacante parte de un mensaje m , y calcula otro mensaje m' que colisiona con el primero.
- De *colisión* propiamente dicha: El atacante se limita a buscar dos valores m y m' que colisionen, pero desconoce tanto sus valores como el del resumen

Ataques (cont.)

- El primer ataque es más peligroso, pero difícil que funcione en suplantación (texto sin sentido!)
- Se conocen ataques del segundo tipo para MD5, SHA-1 y otros

HMAC

- Usa un *Código de Autenticación de Mensaje* (MAC) derivado de un resumen criptográfico, como SHA-1.
- **Motivación:**
 - Funciones de resumen cript. más rápidas en softw. que algoritmos de cifrado como DES
 - Librerías para funciones de resumen cript. ampliamente disponibles
 - No hay restricciones de exportación (EEUU)

Estructura HMAC

