Cryptography and Network Security Chapter 11

Fifth Edition

by William Stallings

Chapter 11 – Cryptographic Hash Functions

Each of the messages, like each one he had ever read of Stern's commands, began with a number and ended with a number or row of numbers. No efforts on the part of Mungo or any of his experts had been able to break Stern's code, nor was there any clue as to what the preliminary number and those ultimate numbers signified.

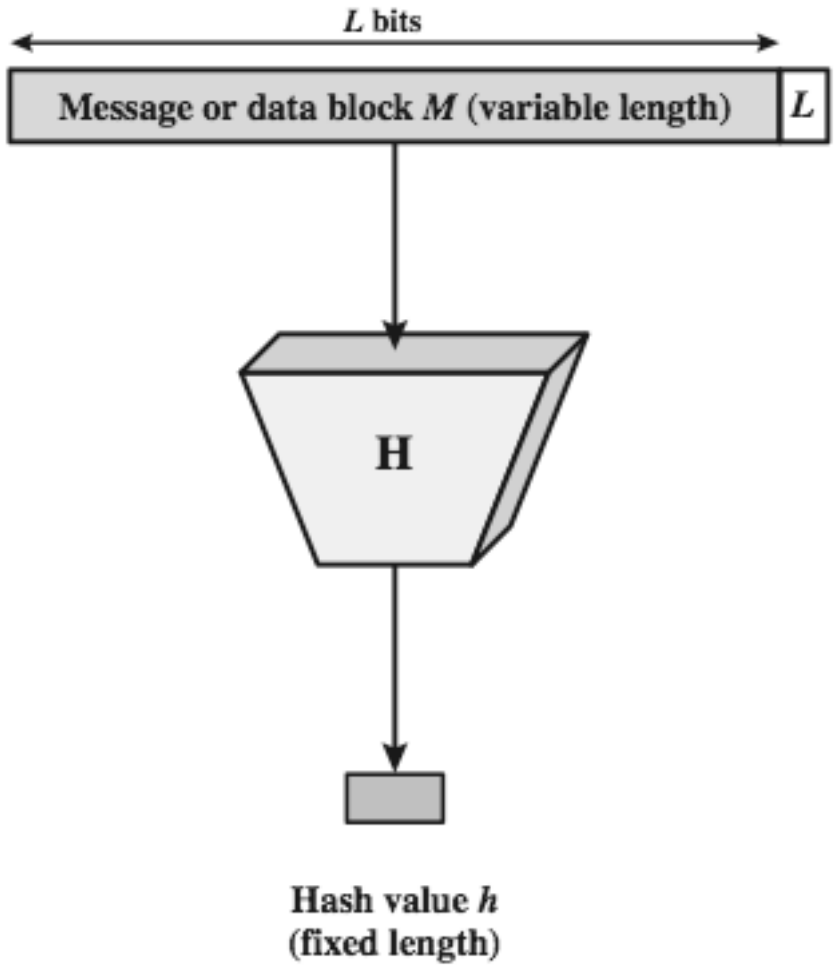
***—Talking to Strange Men,* Ruth Rendell**

Hash Functions

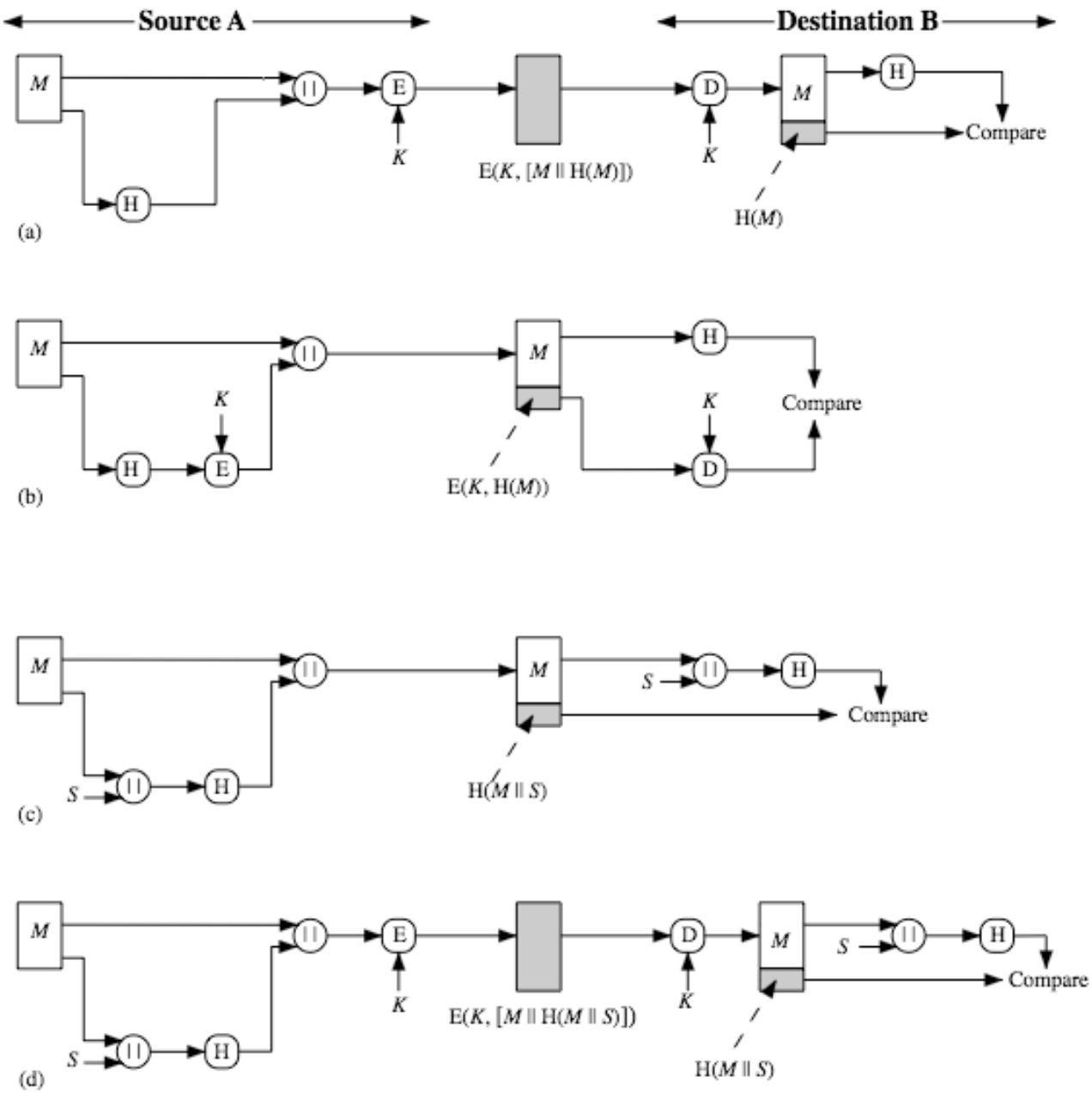
- Συρρικνωνει μηνυμα οποιουδηποτε μηκους σε σταθερο μεγεθος

  `h = H(M)`
- Συνηθως θεωρουμε οτι η hash function ειναι γνωστη σε ολους
- Το hash χρησιμοποιειται για να ανιχνευσει τυχον αλλαγες στο μηνυμα
- Θελουμε μια κρυπτογραφικη hash function τετοια ωστε:
  - Να ειναι υπολογιστικα ανεφικτο να βρεθει μηνυμα που να ταιριαζει στο συγκεκριμενο hash (one-way property)
  - Να ειναι υπολογιστικα αδυνατο να βρεθουν δυο μηνυματα που να δινουν το ιδιο hash (collision-free property)

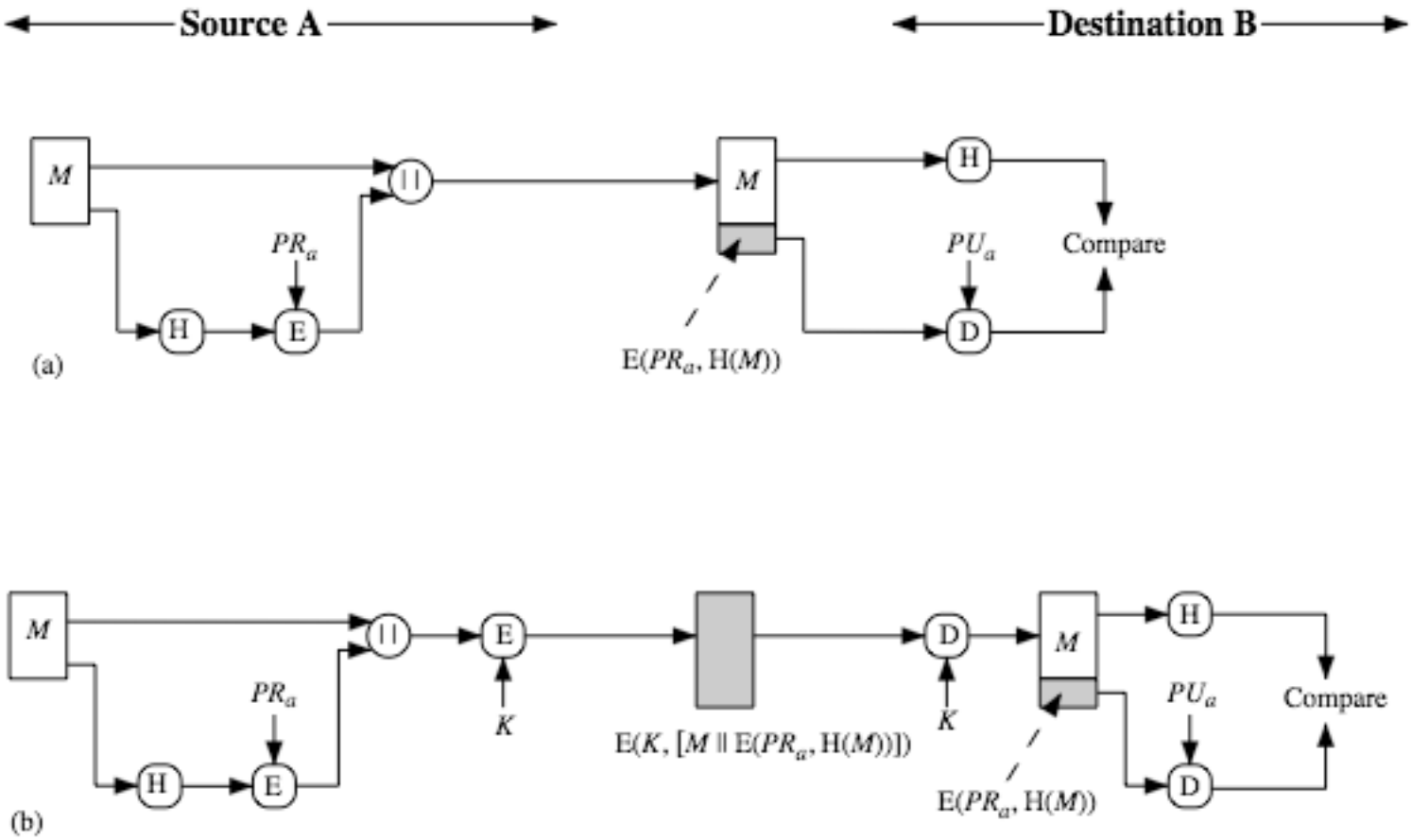
Cryptographic Hash Function



Hash Functions & Message Authent-ication



Hash Functions & Digital Signatures



Άλλες χρήσεις των Hash Functions

- Για τη δημιουργια ενος αρχειου με τα hash των passwords
  - ετσι αποθηκευουμε το hash του password και οχι το ιδιο το password
- Για ανιχνευση εισβολης (intrusion detection) και ανιχνευση ιων (virus detection)
  - Διατηρειται και ελεγχεται το hash των αρχειων σε ενα συστημα
- Ψευδοτυχαια συναρτηση (pseudorandom function, PRF) ή γεννητρια ψευδοτυχαιων αριθμων (pseudorandom number generator, PRNG)

Δυο απλες Μη Ασφαλεις Hash Functions

- bit-προς-bit exclusive-OR (XOR) για καθε μπλοκ
  - $C_i = b_{i1}\ xor\ b_{i2}\ xor\ .\ .\ .\ xor\ b_{im}$
  - Ειναι αποτελεσματικο για ελεγχο ακεραιοτητας (data integrity check)
- Κυκλικη ολισθηση ενος bit στη hash value
  - Για καθε συνεχομενο μπλοκ των *n-bits*
    - Περιστρεφεται η τρεχουσα hash value προς τα αριστερα κατα 1 bit και γινεται XOR με το μπλοκ
  - Καλο για ελεγχο ακεραιοτητας, αλλα αχρηστο για ασφαλεια

Απαιτησεις για τις Hash Functions

Requirement	Description
Variable input size	H can be applied to a block of data of any size.
Fixed output size	H produces a fixed-length output.
Efficiency	H(x) is relatively easy to compute for any given x, making both hardware and software implementations practical.
Preimage resistant (one-way property)	For any given hash value h, it is computationally infeasible to find y such that H(y) = h.
Second preimage resistant (weak collision resistant)	For any given block x, it is computationally infeasible to find y ! x with H(y) = H(x).
Collision resistant (strong collision resistant)	It is computationally infeasible to find any pair (x, y) such that H(x) = H(y).
Pseudorandomness	Output of H meets standard tests for pseudorandomness

Επιθεσεις στις Hash Functions

- Υπαρχουν κι εδω επιθεσεις brute-force και κρυπταναλυση
- Επιθεση preimage ή second preimage
  - Βρισκει ενα *y* τετοιο ωστε το *H(y)* ειναι ισο με μια δοθεισα hash value
- Αντισταση στη συγκρουση (collision resistance)
  - Βρισκει δυο μηνυματα x & *y* με το ιδιο hash, δηλαδη:

    `H(x) = H(y)`
- Αρα για μια hash value των *m* bits, η τιμη $2^{m/2}$ προσδιοριζει την ισχυ του hash code απεναντι σε επιθεσεις brute-force
  - 128-bits ειναι ανεπαρκη, ακομα και τα 160-bits δεν ειναι απολυτα ασφαλη

Επιθεσεις γεννεθλίων (Birthday Attacks)

- Ισως καποιος να θεωρουσε ενα hash των 64-bit ασφαλες
- Αλλα λογω του «Παραδοξου των γεννεθλιων» (**Birthday Paradox**) δεν ειναι.
- Η επιθεση γεννεθλιων (**birthday attack)** λειτουργει ως εξης:
  - Αν ο χρηστης ετοιμαζεται να υπογραψει ενα εγκυρο μηνυμα x παραγοντας το hash του, μεγεθους m bits και κρυπτογραφωντας το με το ιδιωτικο κλειδι του
  - Ο αντιπαλος δημιουργει $2^{m/2}$ παραλλαγες x' του x (ολες με ουσιαστικα το ιδιο νοημα), και τις αποθηκευει
  - Ο αντιπαλος δημιουργει $2^{m/2}$ παραλλαγες y' ενος επιθυμητου πλαστου μηνυματος y
  - Τα δυο συνολα μηνυματων συγκρινονται για να βρεθει ενα ζευγος με το ιδιο hash (μεγαλη πιθανοτητα, λογω του παραδοξου των γεννεθλιων)
  - Ο αντιπαλος δινει στον Α να υπογραψει το εγκυρο μηνυμα που εχει ιδιο hash με το πλαστο. Οταν ο χρηστης δημιουργησει hash για το εγκυρο μηνυμα, τοτε ο αντιπαλος το αντικαθιστα με το πλαστο μηνυμα που ομως εχει εγκυρο hash
- Αρα πρεπει να χρησιμοποιουμε hash μεγαλυτερου μεγεθους

Secure Hash Algorithm (SHA)

- Ο SHA σχεδιαστηκε αρχικα απο NIST & NSA το 1993
- Αναθωρηθηκε το 1995 ως SHA-1
- Ειναι προτυπο στις ΗΠΑ για χρηση με τον αλγοριθμο ψηφιακων υπογραφων DSA.
- Παραγει hash values των 160-bits
- Το 2005, αποτελεσματα για την ασφαλεια του SHA-1 δημιουργησαν αμφιβολιες για τη χρηση του σε μελλοντικες εφαρμογες

Αναθεωρημενος SHA

- Η NIST εξεδωσε αναθεωρηση του SHA το 2002
- Προσθετει τρεις ακομη versions του SHA
  - SHA-256, SHA-384, SHA-512
- Σχεδιαστηκε για συμβατοτητα με την αυξημενη ασφαλεια που παρεχεται απο τον αλγοριθμο κρυπτογραφησης AES
- Εχει δομη παρομοια με τον SHA-1
- Αλλα παρεχει υψηλοτερα επιπεδα ασφαλειας

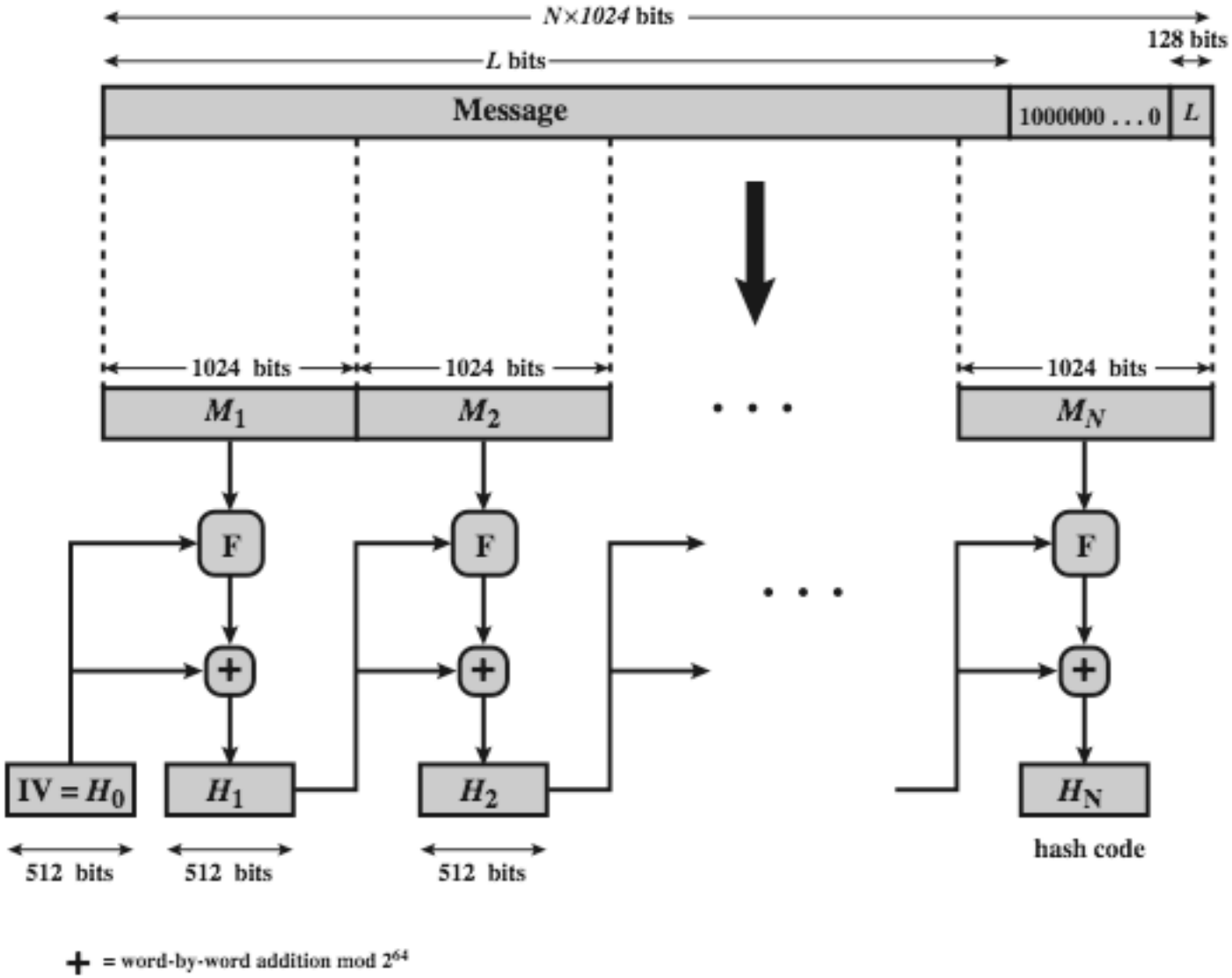
SHA Versions

Table 11.3 Comparison of SHA Parameters

	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

Note: All sizes are measured in bits.

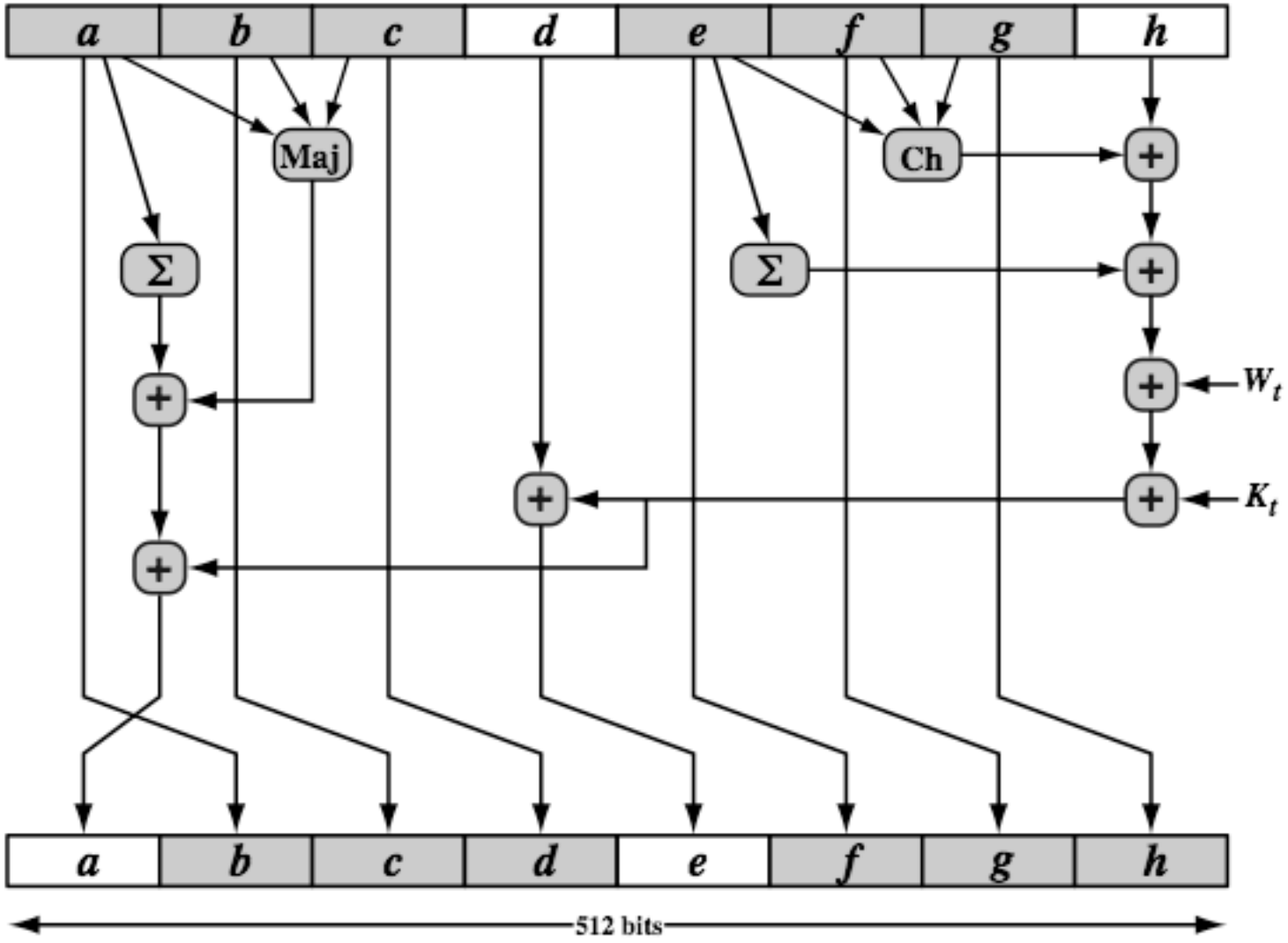
SHA-512 Overview



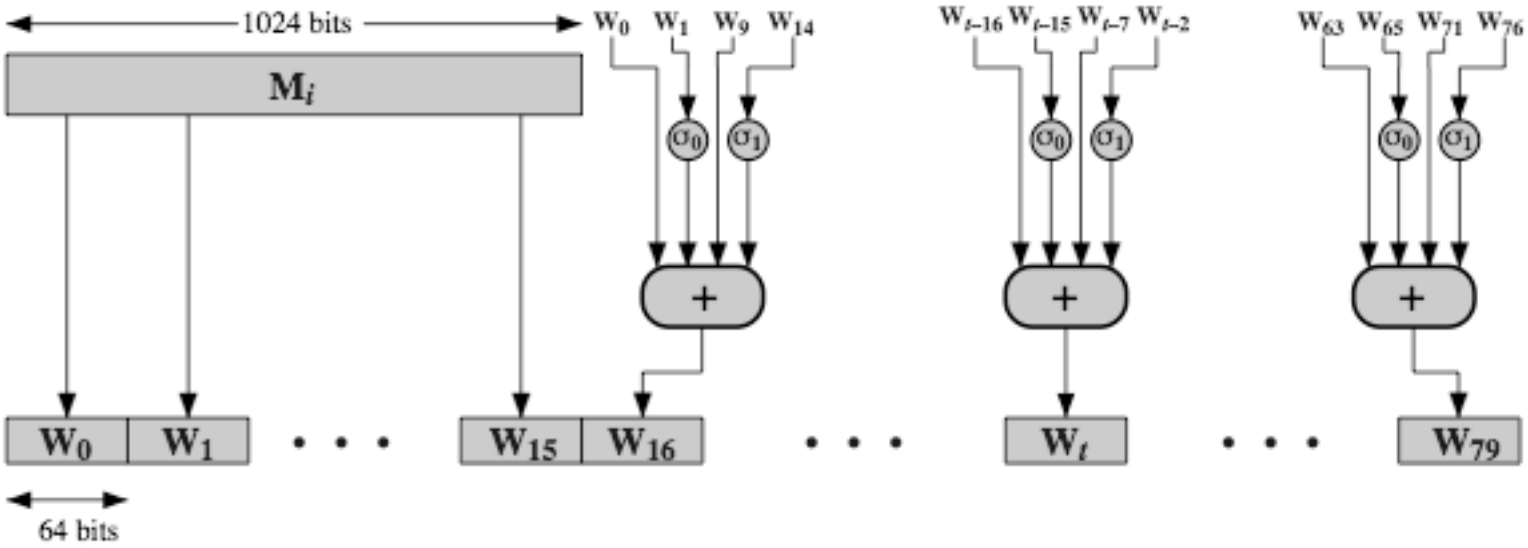
SHA-512 Compression Function

- Ειναι η καρδια του αλγοριθμου
- Επεξεργαζεται το μηνυμα σε τμηματα (blocks) των 1024-bits
- Αποτελειται απο 80 γυρους
  - Ενημερωνει μια buffer των 512-bits
  - Χρησιμοποιει μια τιμη Wt των 64-bits που παραγεται με βαση το τρεχον μπλοκ του μηνυματος
  - Και μια σταθερα γυρου (round constant) που βασιζεται στην κυβικη ριζα των πρωτων 80 πρωτων αριθμων (prime numbers)

SHA-512 Round Function



SHA-512 Round Function



SHA-3

- Ο SHA-1 δεν εχει σπασει ακομη
  - Αλλα δεν θεωρειται ασφαλης
- Ο SHA-2 (esp. SHA-512) φαινεται να ειναι ασφαλης
  - Μοιαζεται ομως την ιδια δομη και τις ιδιες μαθηματικες λειτουργιες με τους προγονους του και αυτο ειναι ενα θεμα
- Η NIST εξηγγειλε το 2007 εναν διαγωνισμο για το SHA-3, την επομενης γενιας hash function της NIST με χρονικο οριζοντα το 2012

Απαιτησεις απο τον SHA-3

- Να αντικαταστησει τον SHA-2 σε καθε χρηση
  - Ετδι χρησιμοποιει το ιδιο μεγεθος hash
- Διατηρει την online φυση του SHA-2
  - Ετσι μπορει να επεξεργαζεται μικρα μπλοκ (512 / 1024 bits)
- Κριτηρια αξιολογησης
  - Ασφαλεια κοντα στο θεωρητικο μεγιστο για τα συγκεκριμενα μεγεθη του hash size
  - Να εχει χαμηλο κοστος σε χρονο και μνημη
  - Χαρακτηριστικα: ευελιξια και απλοτητα

Συνοψη

- Εξετασαμε:
  - Τις hash functions
    - χρηση, απαιτησεις, ασφαλεια
  - Τους αλγοριθμους SHA-1, SHA-2, SHA-3