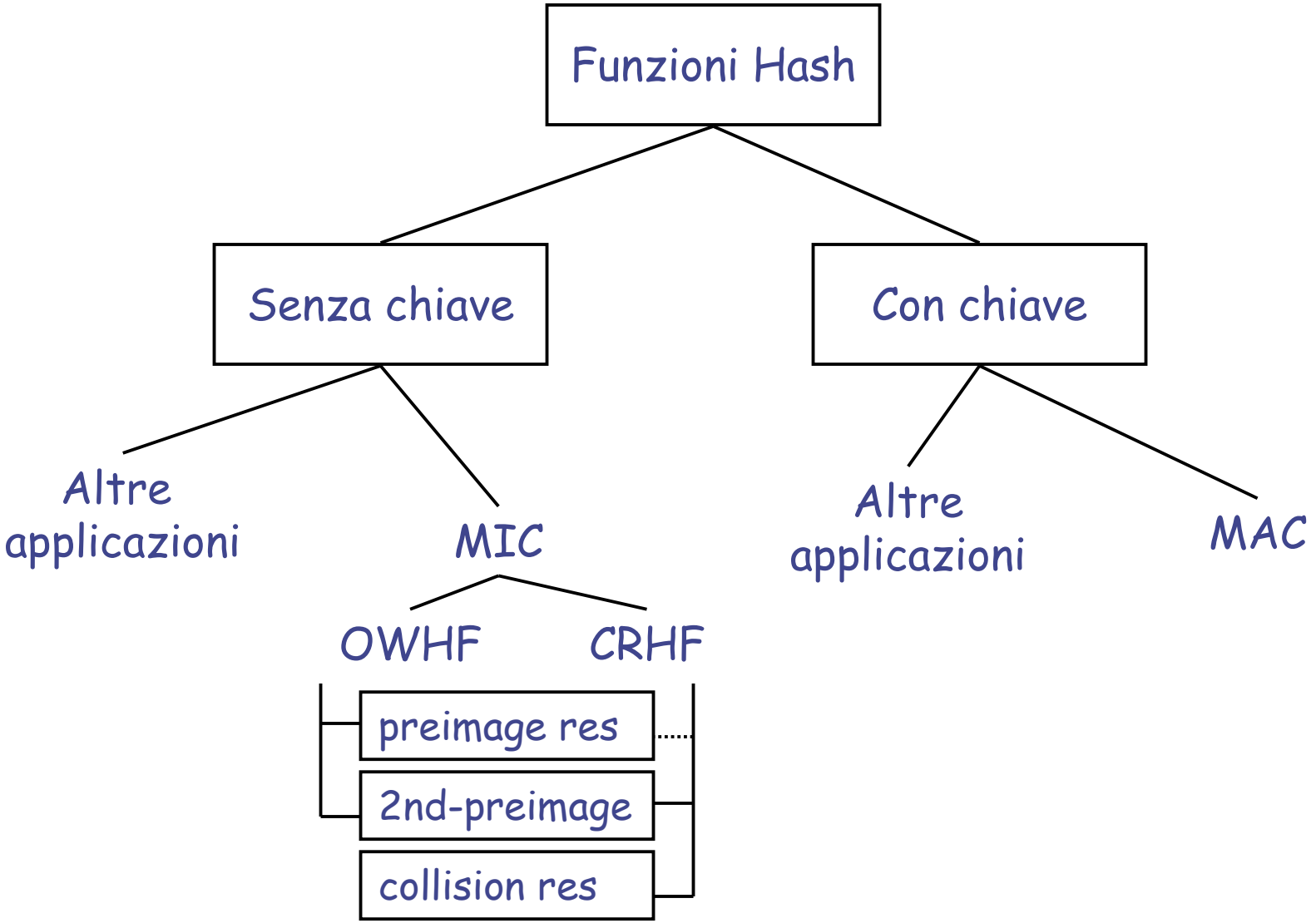
Funzioni HASH

- Classificazione e proprietà
- Attacchi
- Alcune funzioni Hash
- Autenticità ed integrità
- Conclusioni

Classificazione

- MDC (Manipulation Detection Codes) o MIC (Message Integrity Codes), non fa uso di chiave
  - Funzioni Hash One-Way (OWHFs)
  - Funzioni Hash Collision Resistant (CRHFs)
- MAC (Message Authentication Codes)
  - sia autenticazione che integrità
  - Fa uso di chiave
  - Non richiede meccanismi ulteriori

Classificazione



Proprietà

- Preimage Resistance: dato y è computazionalmente impossibile determinare un valore x tale che h(x)=y
- 2-nd Preimage Resistance: dato x e y=h(x) è computazionalmente impossibile determinare un valore x'≠x tale che h(x')=h(x)
- Collision Resistance: è computazionalmente impossibile determinare due qualunque valori differenti x',x tali che h(x')=h(x)

Proprietà Hash nelle applicazioni

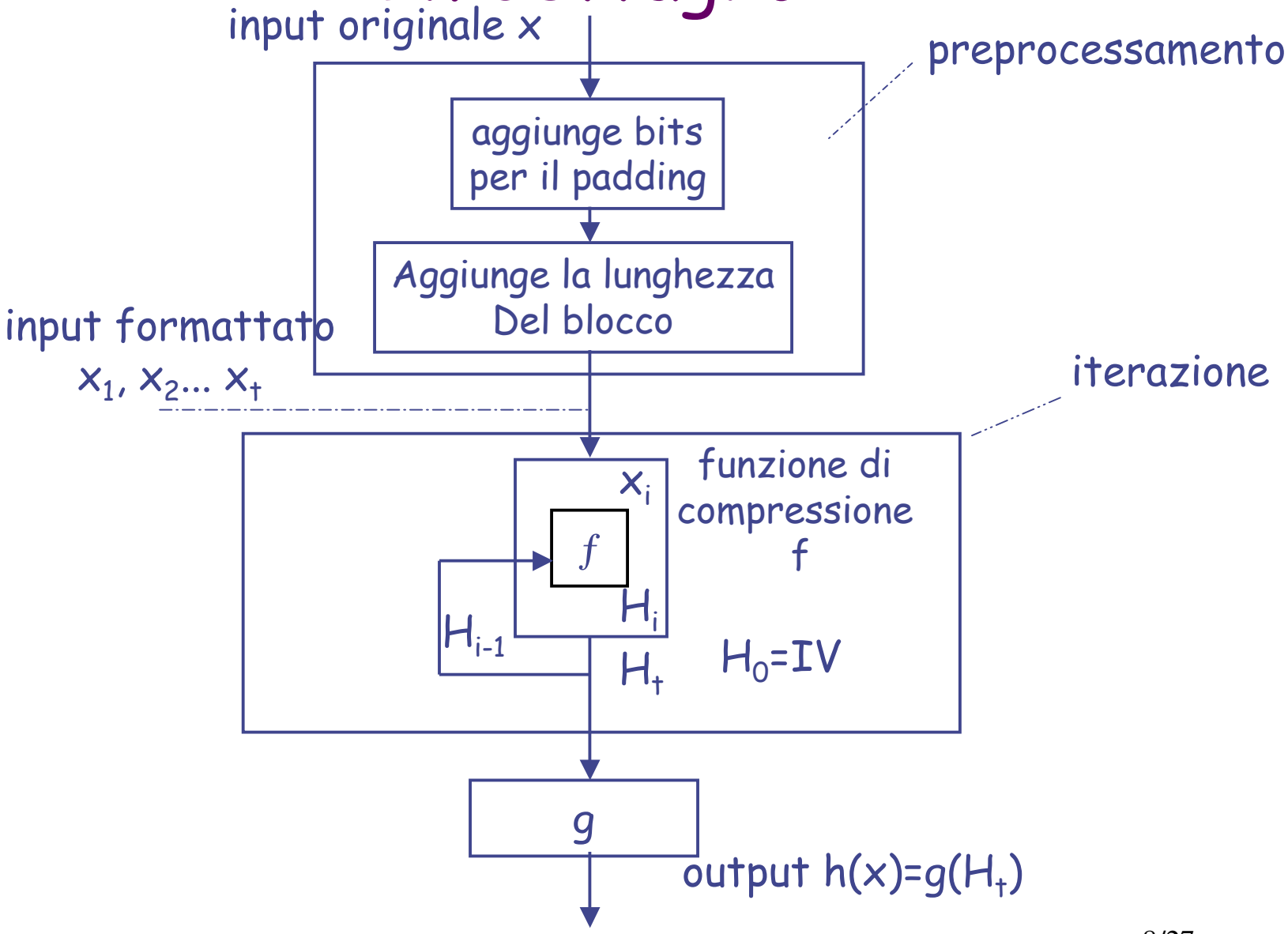
Proprietà	preimage	2nd preimage	Collision resistance
MDC+ firme asimmetriche	SI	SI	SI*
MDC+ autenticità del canale		SI	SI*
File delle Password (MDC)	SI		
MAC (chiave non nota)	SI	SI	SI*

Relazioni tra le proprietà

- collision resistance $\Rightarrow$ 2nd preimage resistance
- la collision resistance non garantisce la preimage resistance
- sia h_k un MAC. Allora h_k nei confronti del chosen-text attack è sia:
  - 2nd preimage che collision resistant
  - preimage resistant

Modello generale per l'iterazione di funzioni hash

In dettaglio



Padding

- Padding Ambiguo : Aggiunge al messaggio dei bits 0 per ottenere una stringa che trasformi la sua lunghezza in un multiplo della dimensione di un blocco
- Padding non ambiguo
  - Aggiunge un bit 1 al messaggio
  - Esegue il Padding Ambiguo

Obiettivi per la sicurezza

Tipo di hash	Obiettivo di progettazione	Str. ideale	Obiettivo per l'Attaccante
OWHF	preimage res; 2nd-preimage res	2^n 2^n	prod. preimg; prod. 2 nd-preimg
CRHF	collision res	$2^{n/2}$	prod. collision
MAC	key non-recovery; computation res	2^n Pf	trova la chiave MAC; prod. una nuova MAC

* $P_f = \max(2^{-n}, 2^{-t})$, t: lunghezza della chiave

Attacchi

- Attacchi a MDC
  - OWHF: dato y trova x tale che h(x)=y; dati (x,h(x)) trova x' ≠ x tale che h(x')=h(x)
  - CRHF: trova qualunque x' ≠x tale che h(x')=h(x) (attacco del compleanno – birthday attack)
- Attacchi a MAC
  - senza conoscere k calcola (x, $h_k(x)$) dati (x_i,$h_k(x_i)$) con $x_i \neq x$
  - known-text attack, chosen text-attack, adaptive chosen text-attack
  - manipolazione selettiva ed isolata

Attacco di base

- Attacco hash di base (per tentativi successivi)
  - una funzione hash a n-bit senza chiave ha una sicurezza ideale se soddisfa gli upper bounds per OWHF e CHRF
- Chiave MAC, ricerca esaustiva della chiave (known-text attack), richiede 2^t operazioni
- Indovinare il MAC richiede 2^n operazioni

Attacco di base (cont.)

- precomputazione dei valori hash (compromesso spazio-tempo)
- parallelizzazione di 2^{nd}-preimage
- attacco a messaggi lunghi per 2^{nd}-preimage.
  - Se h è iterata e non c'è un rafforzamento MD.
  - 2^{nd}-preimage può essere trovato nel tempo $(2^n/s)+s$, con occupazione di spazio di memoria pari a $n(s+\log s)$ bits, per $1 \leq s \leq \min(t, 2^{n/2})$
  - Attacco del compleanno sui risultati intermedi

Lunghezza necessaria in termini di bits

- OWHF n>=80
- CHRF n>=160 (attacco del compleanno)
- MAC n>=64 con l'utilizzo di una chiave di almeno 64 bits
  - Attacchi off-line possibili dato un testo ed il MAC corrispondente, ma le proprietà dipendono dalla segretezza della chiave (la scelta di t è importante)
  - Occorre limitare il numero delle queries per evitare gli attacchi on-line

Funzioni Hash ottenuta dai cifrari a blocchi

- I cifrari a blocchi sono disponibili (senza scriverne uno dall'inizio)
- Lunghezza singola (n bit) oppure lunghezza doppia (2n bit)
  - singola per generare funzioni hash OWHF
  - doppia per generare funzioni hash CHRF (in genere n=64, quindi per la collision resistance abbiamo bisogno di 128 bit)

SHA-1

- 160 bits, cinque variabili a 32-bit
- quattro cicli, f,g,h sono le stesse funzioni dell'MD4 ogni ciclo è composto da 20 passi
- espansione: ogni blocco del messaggio di 16 parole è trasformato in un blocco di 80 parole
- modifica nella rotazione
- più potente dell'MD5

RIPEMD-160

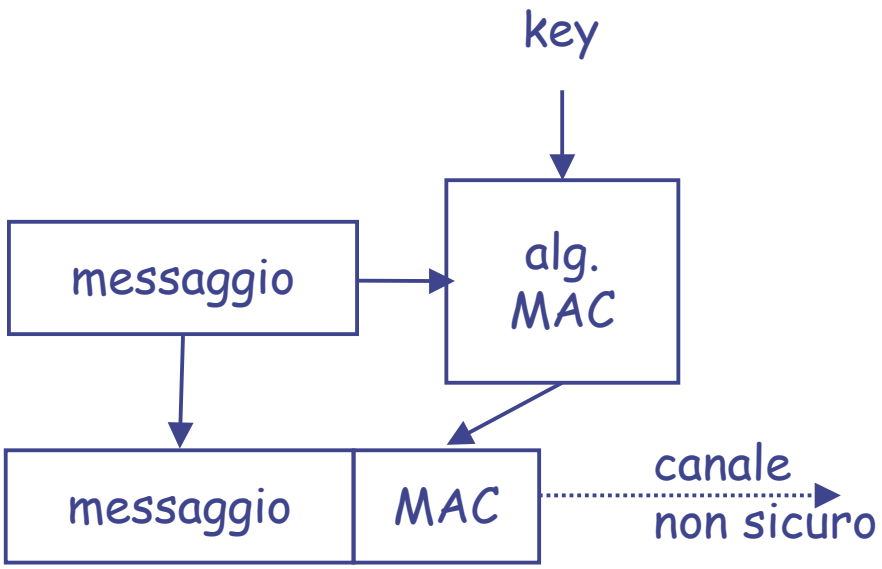
- la funzione di compressione mappa un input di 21 parole (variabile concatenata di 5 parole, blocco del messaggio di 16 parole, parole di 32 bit) ad un risultato di 5 parole
- più cicli dell'MD-4
- sicurezza paragonabile a SHA-1

Integrità e autenticazione

- *Data integrity*: i dati non sono stati modificati rispetto a come sono stati inizialmente creati
- *Data origin authentication*: una delle parti è corroborated come la fonte di dati specifici (include la data integrity)
- *Message authentication*: analogamente a data origin authentication
- MAC non garantisce la non-ripudiabilità
- Sono necessarie altre tecniche per garantire il tempo di vita (timeliveness) e l'unicità

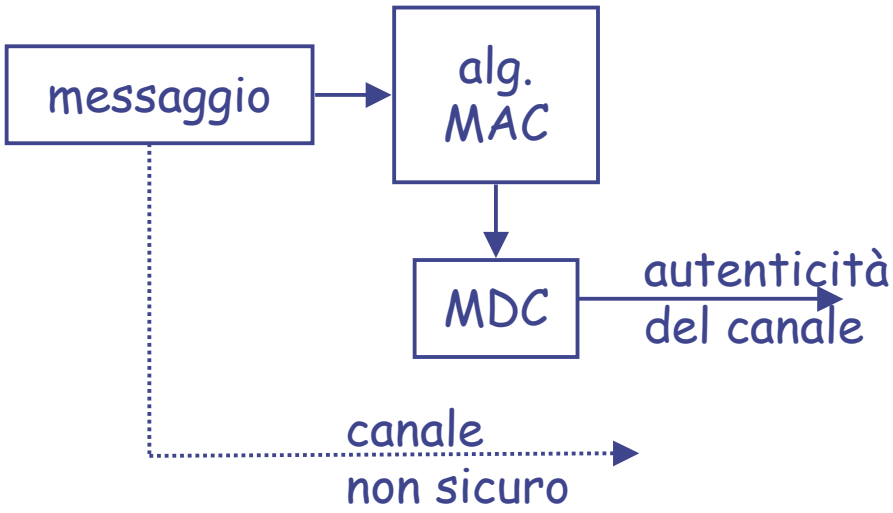
Metodi per l'integrità dei dati

1) solo MAC



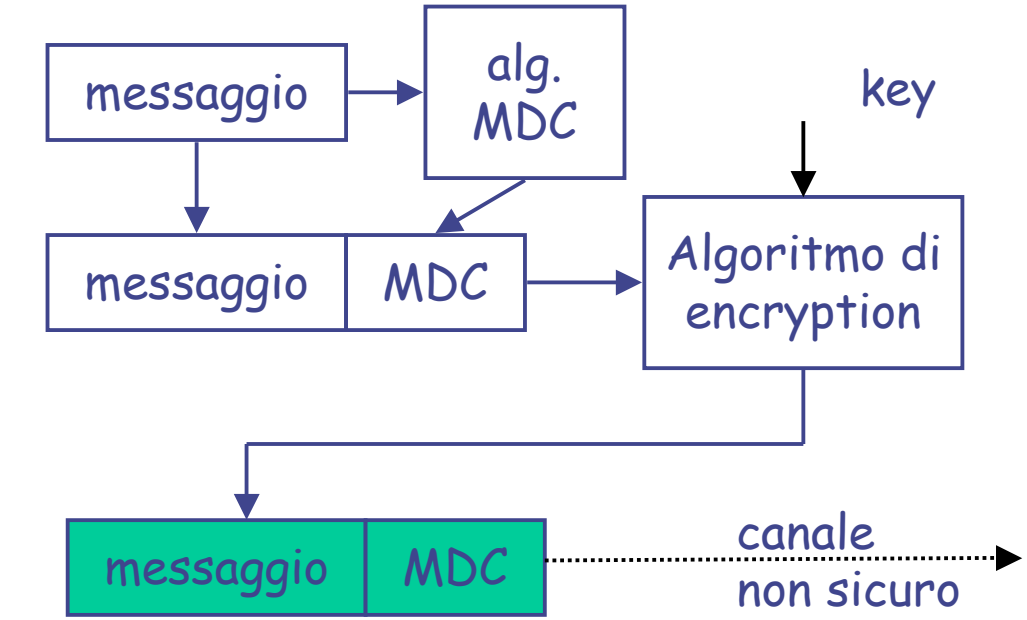
Metodi per l'integrità dei dati

2) MDC & autenticità del canale



Metodi per l'integrità dei dati

3) MDC & crittografia



Autenticazione di una transazione

- L'autenticazione del messaggio (*Message Authentication*) non garantisce l'autenticazione di una transazione.
  - eg. Replay Attack
- Uso di parametri varianti con il tempo (Time-variant-parameter – TVPs)
  - RNs nei protocolli challenge-response
  - Sequence Numbers
  - Time stamps

La cifratura dei dati, da sola, ne garantisce l'integrità ?

- Se nel messaggio c'è abbastanza ridondanza, l'integrità è mantenuta direttamente se la decifratura è eseguita correttamente (occorre conoscere la chiave k)
  - riordinamento ECB
  - encryption su dati random
  - manipolazione di bit nei cifrari a flusso di tipo additivo (specialmente known-plaintext)
  - manipolazione di bits nei blocchi cifrati con DES

MDC & encryption

- $C=E_k(x||h(x))$
- la sicurezza è strettamente connessa all' algoritmo usato per la cifratura a prescindere dalla robustezza dell'MDC
- i cifrari a flusso di tipo additivo non sono mai usati se attacchi di tipo known-plaintext sono possibili.
- variazioni
  - $(x, E_k(h(x))$. h deve essere CRHF
  - $(E_k(x),h(x))$

MAC & encryption

- usa un MAC al posto di MDC
- anche se qualcuno può violare la fase di encryption il MAC preserva l'integrità
- svantaggio principale: occorre gestire due chiavi
- preclude attacchi di tipo esaustivo sulla chiave del MAC
- Occorre scegliere accuratamente la combinazione di MAC e algoritmo per l'encryption
  - Cattiva scelta: MAC-CBC con CBC encryption

Per finire…attacco del compleanno

- si basa sul paradosso del compleanno
- tempo di esecuzione $O(2^{n/2})$
- Si può utilizzare su tutte le funzioni hash senza chiave

Sommario

- Funzioni hash caratterizzate da una elevata efficienza implementativa
- Standard affermato SHA-1
- Indispensabili ausili per protocolli crittografici
- Attacchi noti, ma ci si può difendere, a meno che…