

L'autenticazione dei messaggi si occupa di:

- Proteggere l'integrità dei messaggi
- Convalida dell'identità del mittente
- Impossibilità di disconoscere la paternità di un messaggio.

Tutti i servizi di autenticazione o di firma digitale si basano su una funzione che genera un autenticatore, un valore per autenticare il messaggio.

3 funzioni:

- **MESSAGE ENCPYPTION:** significa che il testo cifrato è l'autenticatore stesso.
- **MESSAGE AUTH CODE:** messaggio + chiave segreta che produce un valore di lunghezza finita che fa da autenticatore.
- **CRIPTO HASH FUNCTION:** utilizzando solo il messaggio si ottiene un valore hash che è l'autenticatore.

• MESSAGE ENCRYPTION:

Perché questo metodo sia efficiente bisogna avere un mezzo per determinare in modo automatico se è possibile decifrare il testo criptato in testo in chiaro, per fare questo basta aggiungere un check-sum al messaggio prima della cifratura.

$C(M, K)$ = CODICE DI AUTENTICAZIONE

• MESSAGE AUTH CODE (mac);

Una funzione mac accetta un messaggio M di dim. variabile e una chiave segreta K , e produce come output a dim. fissa $C(M, K)$. Questa è una funzione uno-a-molti quindi potenzialmente molti messaggi hanno MAC, uno degli obiettivi di una buona funzione è appunto quello di renderlo computazionalmente impossibili da trovare.

• CRYPTO HASH FUNCTION:

Come la funzione MAC anche la funzione hash funziona in modo simile, ma in input ha bisogno solo del messaggio per produrre un output di dimensione fissa $H(M)$.

$$H(M) = \text{HASH CODE}$$

Lo scopo di una funzione hash fondamentalmente è produrre una impronta digitale di un file, un messaggio ...

CARATTERISTICHE di una funzione HASH

- ONE WAY PROTECTION: per ogni dato valori di y , è computazionalmente impossibile trovare M tale che $H(M)=y$.
- WEAK COLLISION RESISTANCE: per qualsiasi M è impossibile da calcolare $y \neq M$ tale che $H(y)=H(M)$
- STRONG COLLISION RESISTANCE: è computazionalmente impossibile trovare una coppia (M, y) tale che $H(M)=H(y)$
- H deve poter essere applicato ad un blocco di dati di qualsiasi dimensione.
- H produce output di dimensione FISSA.
- $H(x)$ è relativamente facile da calcolare per ogni M .

• LA STRONG... è utile per difendersi dal BIRTHDAY-ATTACK

Il paradosso del compleanno afferma che la probabilità che almeno due persone in uno stesso gruppo compiano gli anni lo stesso giorno è molto superiore di quanto ci possiamo immaginare.

Infatti in gruppo di 23 persone la probabilità è del 0,51, mentre in un gruppo di 50 è della 0,97.