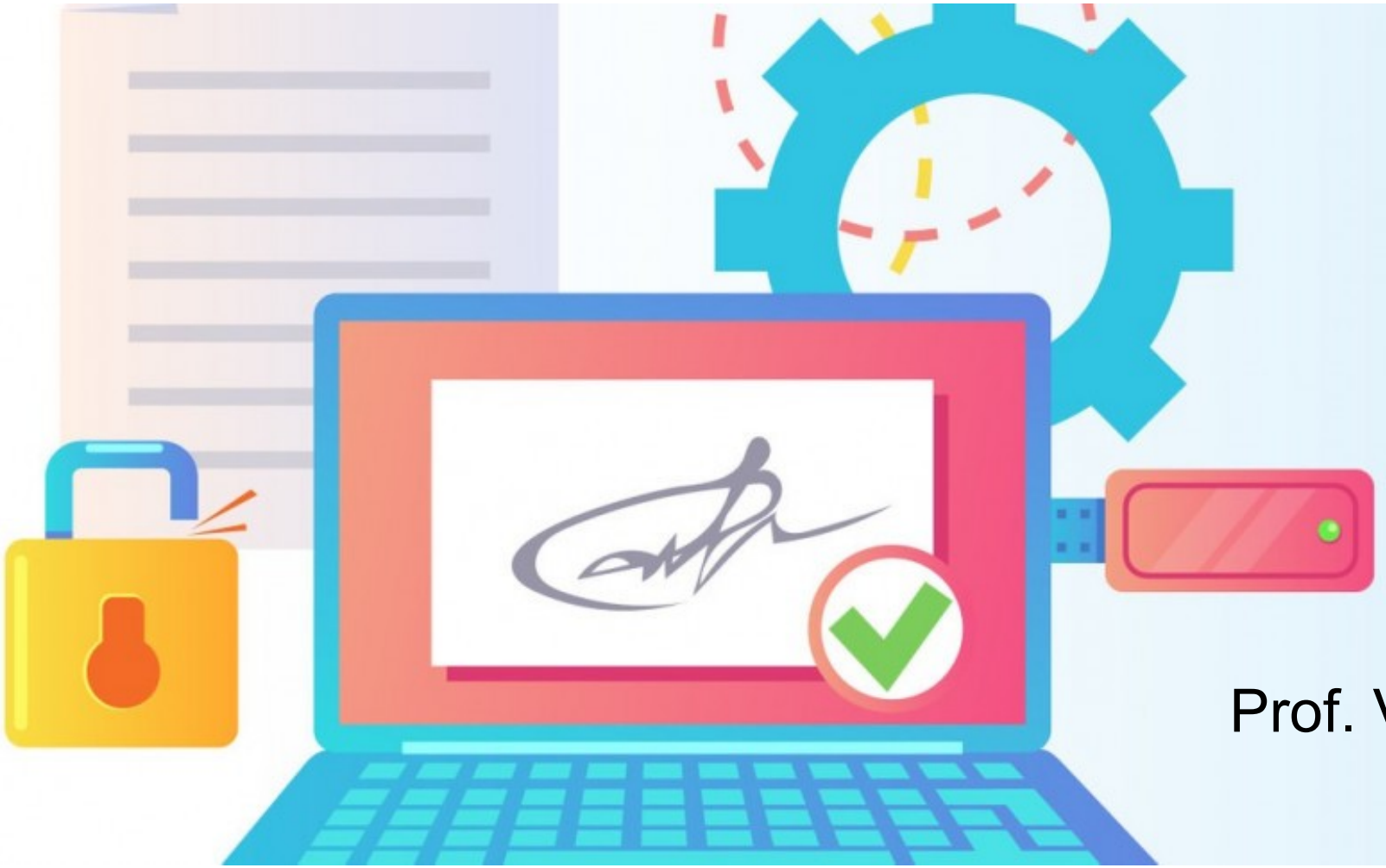
La firma digitale: cos’è e come funziona



SISTEMI E RETI

Prof. Verga - Prof.ssa Dalbesio

A.S. 2023/24

LA FIRMA DIGITALE E GLI ENTI CERTIFICATORI

La **firma digitale**, equivalente elettronico della firma autografa su carta, è associata stabilmente al documento elettronico sulla quale è apposta e ne attesta con certezza l'**integrità**, l'**autenticità** e la **non ripudiabilità**.

LA FIRMA DIGITALE E GLI ENTI CERTIFICATORI

Dal punto di vista tecnico e realizzativo, la **firma digitale** è basata su un sistema a chiavi crittografiche **asimmetriche**, utilizza un certificato digitale rilasciato da un **ente certificatore** (Certification Authority) con specifiche capacità professionali garantite dallo Stato e viene creata mediante un dispositivo con elevate caratteristiche di sicurezza, generalmente una **smart card**.

LA FIRMA DIGITALE E GLI ENTI CERTIFICATORI

I **certificatori** verificano:

- l'identità di un soggetto e la corrispondenza con la titolarità della chiave pubblica di cifratura;
- Attestano tali informazioni mediante l'emissione del certificato digitale;
- Pubblicano tempestivamente la sospensione del certificato in apposite liste.

LA FIRMA DIGITALE E GLI ENTI CERTIFICATORI

Il file firmato digitalmente deve essere certificato dall'**ente certificatore** prima dell'invio.

Con il certificato il destinatario ottiene la **chiave pubblica** sicura per verificare **identità** del mittente e **integrità** del documento.

LA FIRMA DIGITALE E GLI ENTI CERTIFICATORI

Attualmente esistono tre formati per produrre file firmati digitalmente:

1) **Pkcs#7** (meglio noto come p7m): primo formato in uso sin dal 1999. Le Amministrazioni Pubbliche sono obbligate ad accettarlo;

2) **PDF**

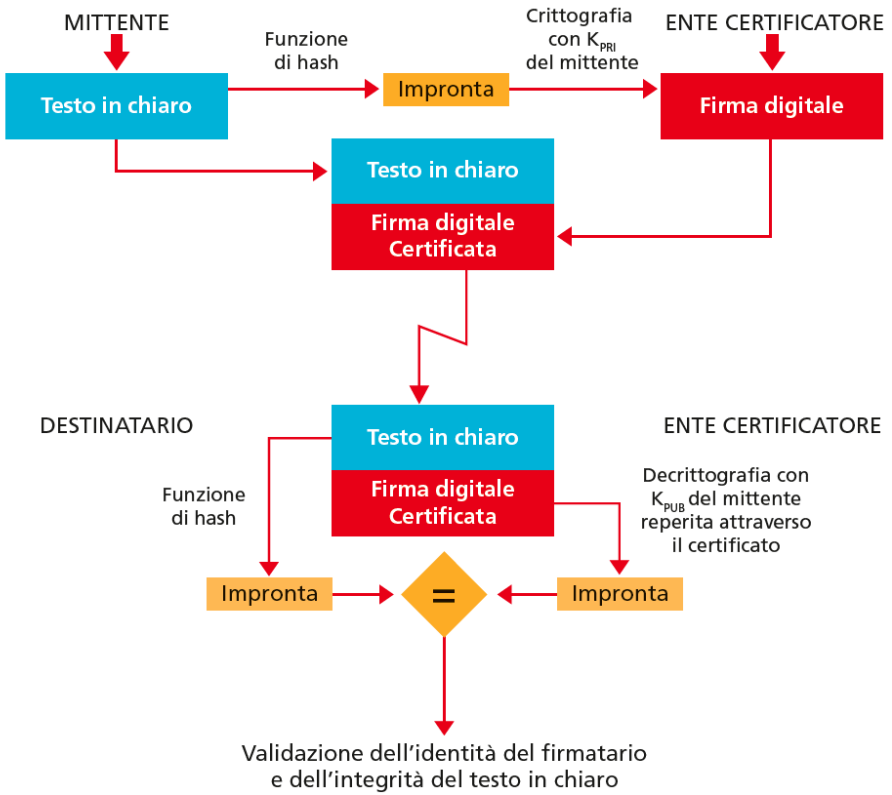
3) **XML**: il più diffuso nei settori bancari e sanitari per la gestione elettronica del flusso dei dati.

LA FIRMA DIGITALE E GLI ENTI CERTIFICATORI

Generalmente la firma digitale richiede un kit di firma digitale, composto dal dispositivo sicuro (smart card o otken USB) e dal software di firma capace di usare il dispositivo associato.

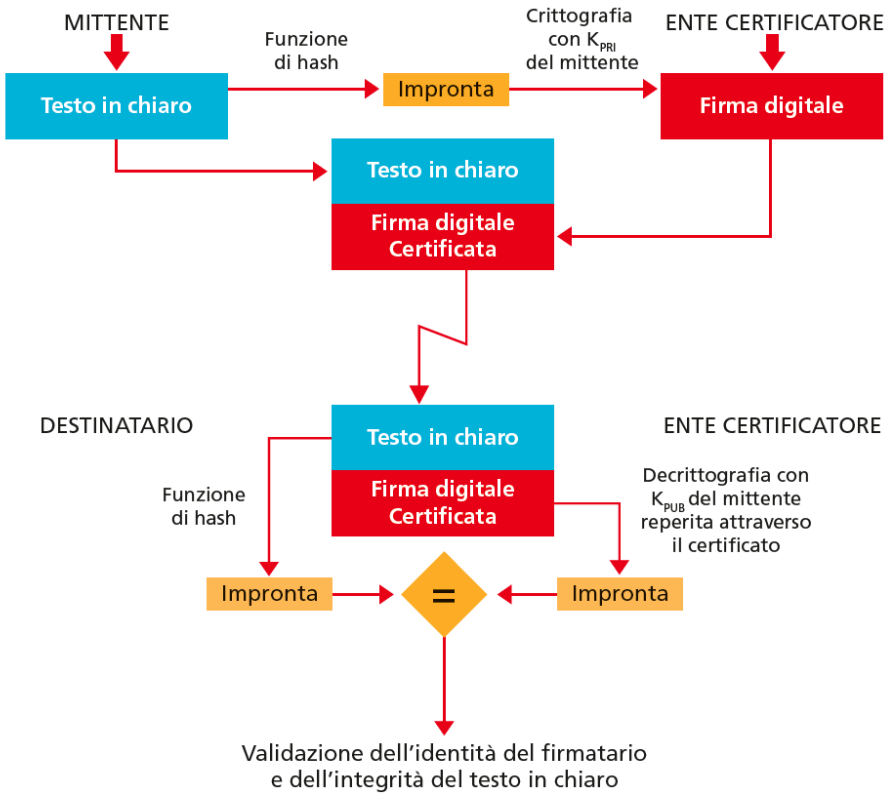
LA FIRMA DIGITALE E GLI ENTI CERTIFICATORI

L'algoritmo di apposizione della firma digitale prevede la creazione di un'**impronta** (message digest) attraverso la **funzione di hash**.



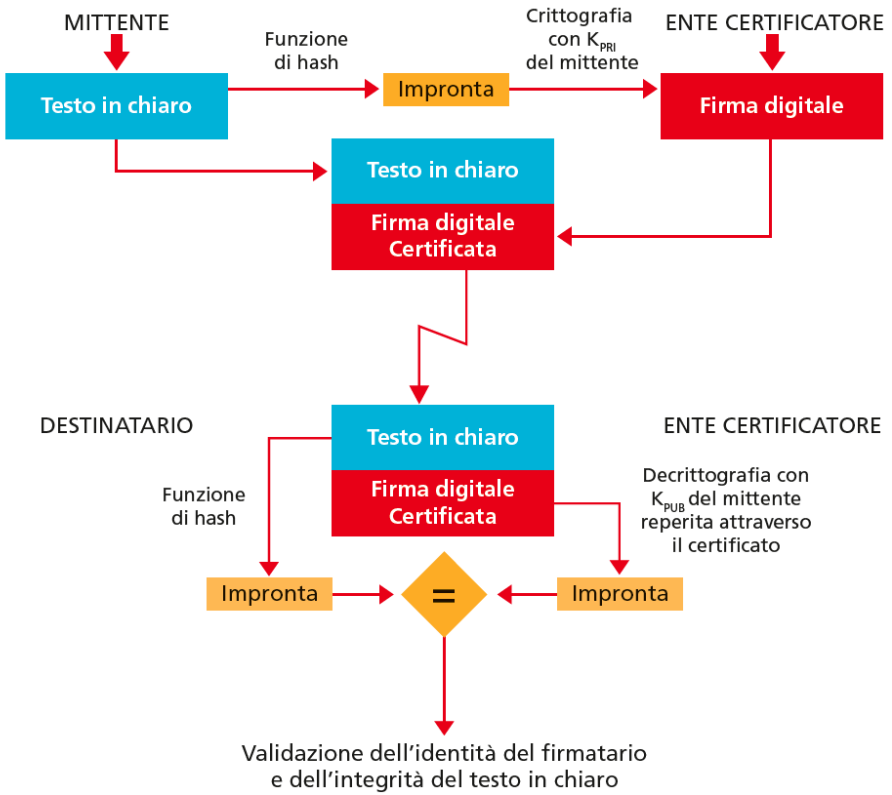
LA FIRMA DIGITALE E GLI ENTI CERTIFICATORI

Un funzione crittografica hash è un algoritmo matematico che trasforma dei dati di lunghezza arbitraria (messaggio) in una stringa binaria di dimensione fissa (128 o 160 bit).



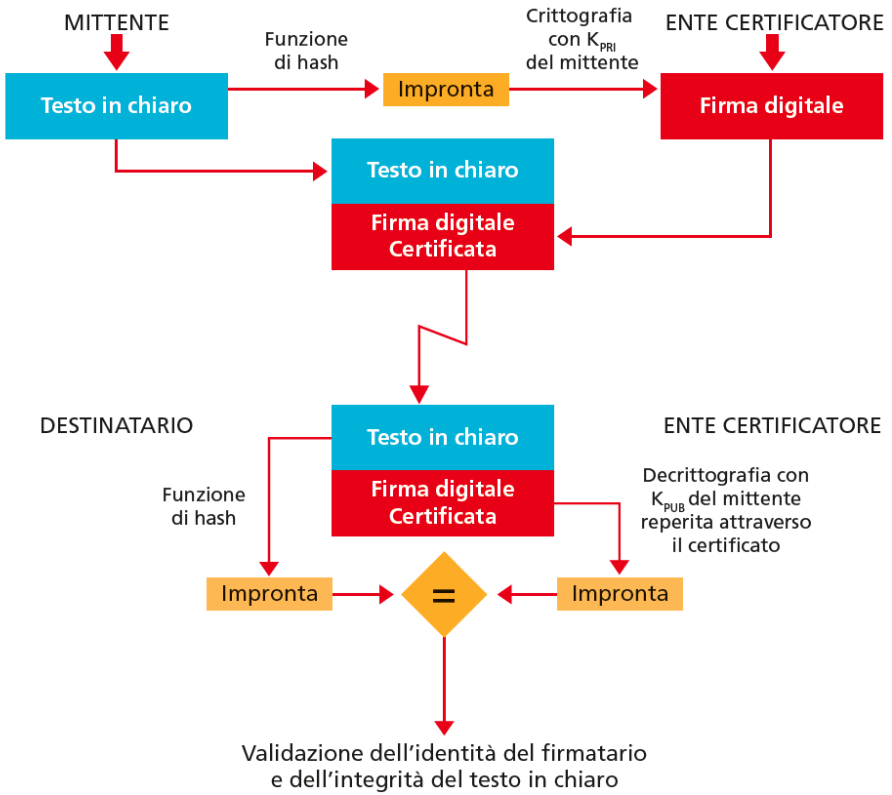
LA FIRMA DIGITALE E GLI ENTI CERTIFICATORI

Gli algoritmi per la firma digitale sono unidirezionali (***one way***), quindi difficili da invertire (conoscendo l'impronta non si può ricostruire il testo che l'ha generata). Una funzione hash deve avere un **ottimo effetto valanga**.



LA FIRMA DIGITALE E GLI ENTI CERTIFICATORI

La firma digitale è l'impronta crittografata con la chiave privata del mittente validata dall'ente di certificazione. Il destinatario, ricevuto il documento firmato, calcolerà a sua volta l'impronta partendo dal testo in chiaro ed usando la stessa funzione hash. Infine la ricalcolerà usando la chiave pubblica reperita con il certificato. Se le due impronte sono uguali, il documento è stato firmato dalla persona giusta e non è stato modificato.

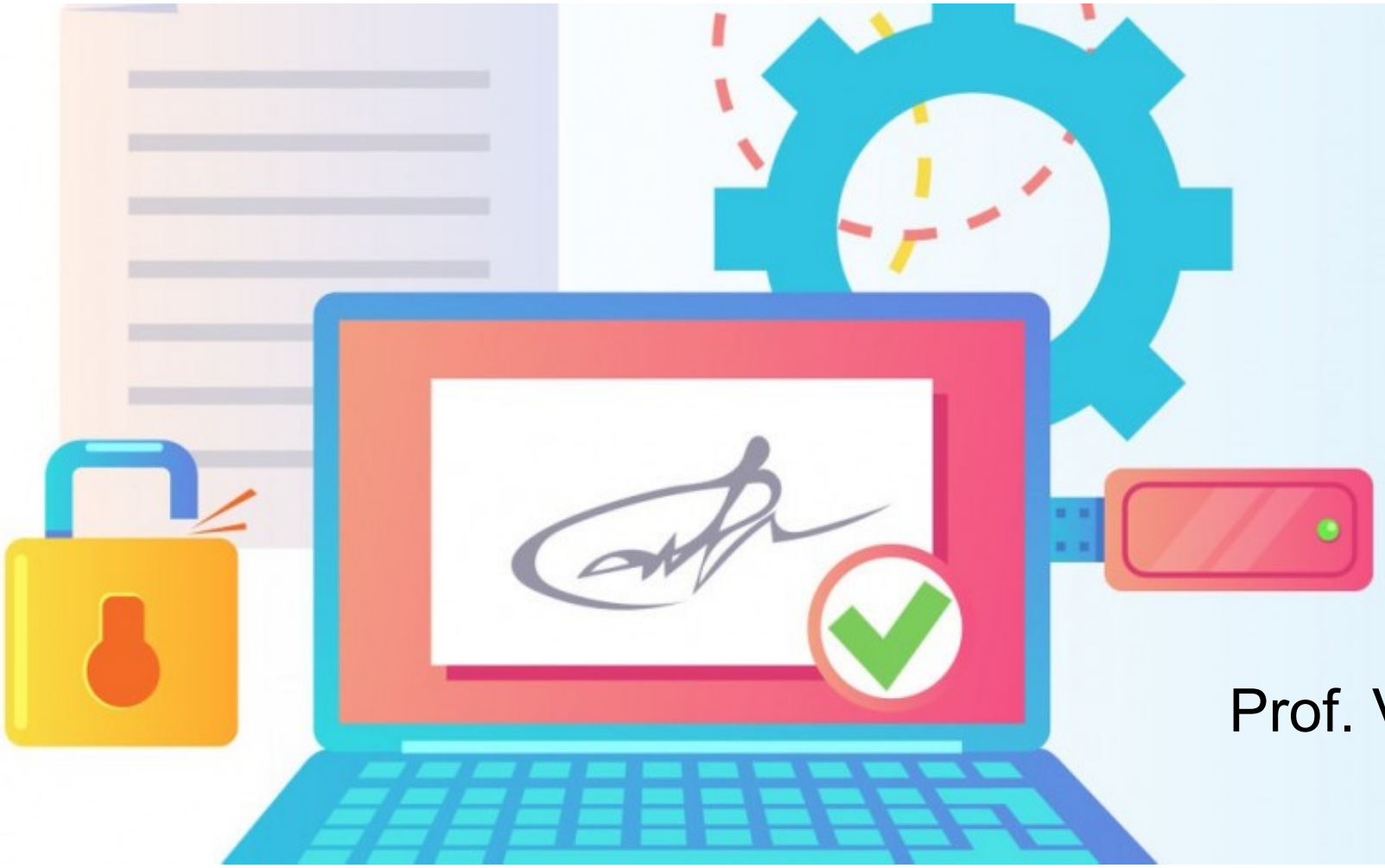


LA FIRMA DIGITALE E GLI ENTI CERTIFICATORI

Oltre alla firma digitale esistono altri servizi che si basano sugli enti certificatori:

- **PEC** (Posta Elettronica Certificata)
- **SPID** (Sistema Pubblico di Identità Digitale)
- **CNS** (Carta Nazionale dei Servizi)

La firma digitale: cos’è e come funziona



SISTEMI E RETI

Prof. Verga - Prof.ssa Dalbesio

A.S. 2023/24

LA FUNZIONE CRITTOGRAFICA DI HASH

Da Wikipedia, l'enciclopedia libera:

In informatica una **funzione crittografica di hash** è un algoritmo matematico che mappa dei dati di lunghezza arbitraria (**messaggio**) in una stringa binaria di dimensione fissa chiamata valore di **hash**, ma spesso viene indicata anche con il termine inglese **message digest** (o semplicemente digest).

Tale funzione di hash è progettata per essere unidirezionale (**one-way**), ovvero una funzione difficile da invertire: l'unico modo per ricreare i dati di input dall'output di una funzione di hash ideale è quello di tentare una ricerca di forza-bruta di possibili input per vedere se vi è corrispondenza (match).

LA FUNZIONE CRITTOGRAFICA DI HASH

Proprietà fondamentali della funzione crittografica di hash ideale:

- deve **identificare univocamente il messaggio**, non è possibile che due messaggi differenti, pur essendo simili, abbiano lo stesso valore di hash;
- il **risultato deve essere deterministico**, in modo che lo stesso messaggio si traduca sempre nello stesso hash;
- deve essere **semplice e veloce** calcolare un valore hash da un qualunque tipo di dato;
- deve essere molto **difficile o quasi impossibile generare un messaggio dal suo valore hash** se non provando tutti i messaggi possibili.

LA FUNZIONE CRITTOGRAFICA DI HASH

Tali caratteristiche permettono alle funzioni crittografiche di hash di trovare **ampio utilizzo negli ambiti della sicurezza informatica**, quali **firme digitali**, **codici di autenticazione** dei messaggi (MAC) e altre forme di autenticazione.

Gli algoritmi di hash possono essere utilizzati anche come funzioni di hash ordinarie, per indicizzare i dati nelle tabelle di hash, per la rilevazione di impronte digitali, per rilevare dati duplicati o identificare in modo univoco i file e come checksum per rilevare la corruzione accidentale dei dati. Infatti, nei contesti di sicurezza informatica, i valori di hash crittografici sono talvolta chiamati «impronte digitali» o «checksum» anche se tutti questi termini hanno funzioni più generali con proprietà e scopi piuttosto diversi.

LA FUNZIONE CRITTOGRAFICA DI HASH