Sicurezza delle informazioni

Crittografia

Esistono due classi principali di algoritmi che si basano sull'utilizzo di chiavi:

Crittografia Simmetrica (detta anche a **chiave privata**);

Crittografia Asimmetrica (detta anche a **chiave pubblica**).

Crittografia Simmetrica

Gli algoritmi simmetrici sono quelli usati nella crittografia classica e permettono al mittente ed al destinatario di usare la stessa chiave per criptare e decriptare un messaggio.

Crittografia Asimmetrica

Gli algoritmi asimmetrici, in particolare quelli reversibili, si basano su una coppia di chiavi: l'una capace di cifrare e l'altra di decifrare l'informazione e viceversa.

Osservazione

E’ immediato concludere che più le chiavi sono lunghe e più è sicuro l’algoritmo di crittografia, anche se ciò porta a forti limitazioni prestazionali sugli algoritmi.

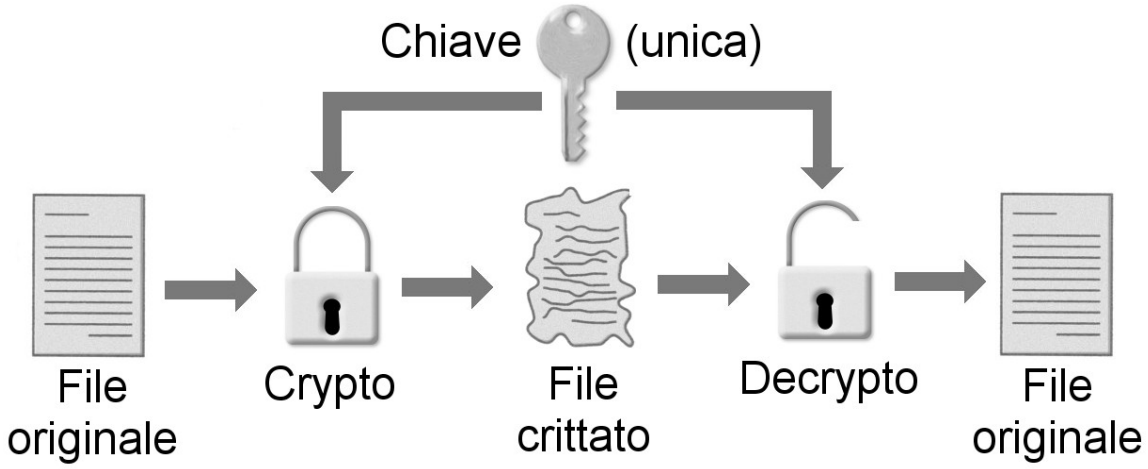
La Crittografia a chiave simmetrica

Nella crittografia a chiave simmetrica è utilizzata una sola chiave detta **segreta** o **privata** (si tratta di crittosistemi secret-key o private-key), la quale è un parametro di una funzione invertibile. Questa chiave serve sia per cifrare, che per decifrare e perciò deve essere nota al mittente ed al destinatario.

Principio di funzionamento

1. Il mittente cifra il messaggio con la chiave segreta;
2. Si trasmette il messaggio cifrato attraverso un canale (sicuro o insicuro);
3. Il destinatario riceve il messaggio cifrato e lo decifra con la chiave segreta;

Crittografia a chiave simmetrica



Vantaggi:

- *velocità di funzionamento,* quindi è possibile utilizzare chiavi molto lunghe, giacché gli algoritmi per cifrare o decifrare sono molto veloci.

- Per quanto riguarda i requisiti di *Autenticità, Integrità e Riservatezza,* non possiamo affermare che essi siano strettamente soddisfatti poiché tutto è legato al "gruppo" di persone che possiedono la chiave e non a un singolo soggetto

Svantaggi (1):

- *L'aumento dei tassi di velocità dei processori degli elaboratori*: ciò rende meno sicuro questo sistema crittografico, visto che gli algoritmi simmetrici sfruttano operazioni molto semplici come trasposizione o sostituzione di bit e le ricerche esaustive diventano possibili in tempi sempre minori.
- *L'uso ripetuto della stessa chiave*: rappresenta un potenziale problema; più volte la chiave viene utilizzata, più è facile riuscire a carpirla.

Svantaggi (2):

- *La distribuzione delle chiavi*: per decifrare un messaggio è necessario conoscere la chiave, che lo ha cifrato. Questo comporta tuttavia un problema, cioè bisogna spedire la chiave a tutti i destinatari del messaggio cifrato. Una soluzione è l'utilizzo di un canale sicuro, attraverso il quale si possa trasmettere senza timore che qualcuno stia ascoltando ed abbia la possibilità di impossessarsi della chiave, d'altro lato se si disponesse di un canale sicuro non sarebbe necessaria la crittografia. Il problema si amplifica al crescere del numero delle persone a cui si vuole spedire il messaggio.
- *L'affidabilità del destinatario*: questi potrebbe perdere o dare ad altri non autorizzati la propria chiave. In tal caso occorre generare una nuova chiave, ridistribuirla e crittare tutti i messaggi che potrebbero essere stati compromessi.

Algoritmi a chiave privata

Tra i vari algoritmi a chiave privata o segreta (o simmetrica), quello che ha ottenuto maggiore sviluppo e successo è stato il DES (Data Encryption Standard).

Si tratta di un cifratore sviluppato dall'IBM e definito dal Governo degli Stati Uniti come standard ufficiale nel 1997.

Crittografia a chiave asimmetrica

L'idea che è alla base dei crittosistemi a chiave asimmetrica è che la chiave di crittazione sia diversa da quella di decrittazione: così facendo è possibile distribuire la propria chiave di decrittazione (che prende quindi il nome di *chiave pubblica*) e mantenere segreta la chiave di crittazione (la *chiave privata*),

Risolve i problemi tipici della crittografia a chiave simmetrica:

- lo *scambio delle chiavi* non è più critico, anzi nella maggior parte dei casi le chiavi sono da considerarsi pubbliche e quindi non esiste più alcun problema in merito;
- il problema dell'*autenticità* del mittente viene immediatamente risolto, in quanto solo il titolare di quella chiave privata potrà aver generato il messaggio corrispondente alla relativa chiave pubblica;

Risolve i problemi tipici della crittografia a chiave simmetrica:

- si risolve il problema della *riservatezza*: infatti, poiché l'algoritmo è simmetrico dal punto di vista delle chiavi (ciò che viene crittato con la chiave privata va decrittato con quella pubblica, ma anche viceversa) è sufficiente crittare un messaggio con la chiave pubblica affinché solo il titolare della corrispondente chiave privata possa leggerlo;
- infine ogni soggetto dovrà detenere una sola coppia di chiavi (la propria): le chiavi pubbliche verranno iscritte in appositi registri, pubblicamente consultabili, dai quali potranno essere scaricate al momento opportuno .

Concetti su cui si basa il metodo

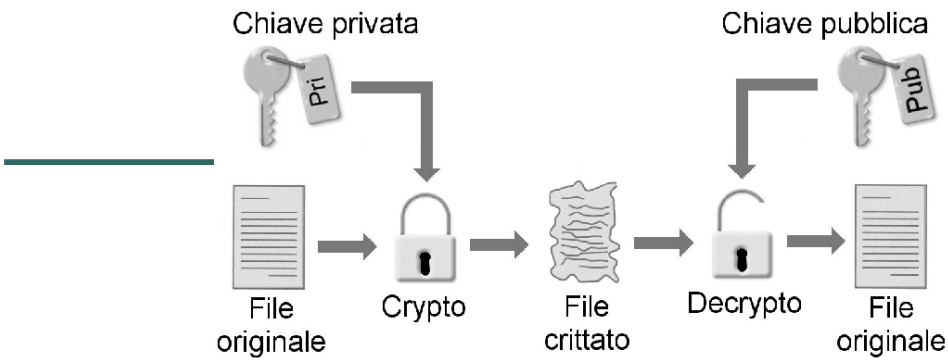
1. Un messaggio crittato con una chiave può essere decrittato solo con l'altra chiave.
2. È matematicamente improbabile ricavare una chiave dall'altra, ovvero le chiavi devono essere indipendenti; la conoscenza di una non deve concedere nessuna informazione utile alla ricostruzione dell'altra.

Due modalità di funzionamento:

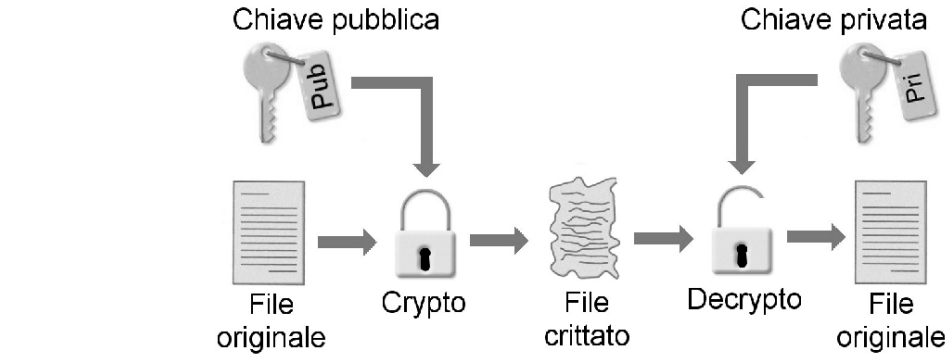
- “modalità autenticazione” infatti solo il possessore della chiave privata può aver cifrato il file. Ciò garantisce anche l’*integrità* del documento (una volta decifrato e modificato, solo il possessore della chiave privata può cifrato di nuovo) e il *non ripudio* da parte del firmatario, tuttavia non è garantita la riservatezza (o confidenzialità) per il destinatario dato che chiunque sia in possesso della chiave pubblica può decrittare il file.

Due modalità di funzionamento:

1. “modalità confidenziale”, in cui la confidenzialità e l’integrità del file sono garantite dal fatto che solo il possessore della chiave privata può decrittare il file.



LE CHIAVI SONO INVERTIBILI



Svantaggi:

Uno dei grossi limiti nell'utilizzo degli algoritmi a crittografia asimmetrica consiste nel fatto che i numerosi e complessi calcoli rendono la loro implementazione poco efficiente soprattutto quando occorre garantire una lunghezza minima della chiave superiore ai 1024 bit (AIPA).

Le funzioni di hash

A questo punto la soluzione più semplice che si possa pensare per pervenire ad un sistema di Firma Digitale è quella di prendere il messaggio in blocco e di crittografarlo con la chiave privata del mittente. Purtroppo tale tecnica non sempre è utilizzabile, in quanto il crittosistema può diventare troppo lento per poterlo utilizzare in maniera efficiente anche con file di pochi Kbyte, soprattutto se le chiavi sono lunghe.

Le funzioni di hash

necessaria una tecnica che, a partire da un messaggio, generi una sequenza di numeri (impronta o *fingerprint* o *digest*) molto più corta del messaggio stesso e che possa essere considerata *relativamente univoca*, nel senso che dovrà essere estremamente difficile trovare un altro messaggio, specie se sensato, che generi la medesima sequenza. Le funzioni di *hash*

Una funzione di *hash* deve godere delle seguenti proprietà:

1) deve essere coerente: a messaggio uguale deve corrispondere uguale hash;
2) deve essere (o quanto meno apparire) casuale, per impedire l'interpretazione accidentale del messaggio originale;
3) deve essere (relativamente) univoca, ossia la probabilità che due messaggi generino il medesimo hash deve essere virtualmente nulla;
4) deve essere non invertibile: non deve essere possibile risalire al messaggio originale dalla sua fingerprint;
5) deve infine essere equiprobabile: ognuna delle possibili sequenze binarie che costituiscono l'hash deve avere la stessa probabilità di essere generata delle altre.

Algoritmi di hash utilizzati

- quelli della serie "Message Digest": gli ormai obsoleti MD2 e MD4 e il più recente MD5; quest'ultimo in particolare elabora il messaggio a blocchi di 512 bit per generare una fingerprint di 128 bit ;
- il "Secure Hash Algorythm 1" (o SHA-1): derivato da MD4, elabora il messaggio a blocchi di 512 bit e genera una fingerprint di 160 bit ;
- il RIPEMD-160: elaborato da un gruppo di lavoro finanziato dall'Unione Europea (il RIPE – Race Integrity Primitives Evaluation), nasce come ideale sostituto di MD5 e SHA-1, rispetto ai quali promette maggiore sicurezza; elabora il messaggio a blocchi di 256 bit e genera una fingerprint di 160 bit (ne esistono anche versioni a 128, 256 e 320 bit, ma in questi casi viene chiaramente specificato che all'aumentare della lunghezza dell'hash non aumenta il livello di sicurezza ottenuto.

Combinazione di tecniche

- Firma digitale + crittografia
  - Per assicurare non ripudibilità, non modificabilità e segretezza dei messaggi
  - Si crittografa testo in chiaro e firma digitale
- Crittografia mista
  - L'uso della crittografia asimmetrica è poco pratica a causa della lentezza degli algoritmi
  - Si usa la crittografia a chiave pubblica per scambiare in modo sicuro chiavi simmetriche
  - Le chiavi simmetriche sono usate per crittografare il flusso di dati (vengono frequentemente cambiate)

Firma digitale