

UNIVERSITÀ DEGLI STUDI DI TRENTO

DOCUMENTO ELETTRONICO,
FIRMA DIGITALE
E SICUREZZA IN RETE.

INTRODUZIONE ALL'ARGOMENTO.

A cura di:

Eleonora Brioni, Direzione Informatica e Telecomunicazioni – ATI NETWORK.

INDICE

INDICE.....	II
INTRODUZIONE	1
COS'È LA CRITTOGRAFIA.....	3
GLI ALGORITMI A CHIAVE SIMMETRICA	5
GLI ALGORITMI A CHIAVE ASIMMETRICA.....	6
RSA	8
COS'È LA FIRMA DIGITALE	10
COSA SONO I CERTIFICATI A CHIAVE PUBBLICA.....	15
COSA SI PUÒ FARE CON LA FIRMA DIGITALE	17
INDICE DELLE FIGURE.....	18

INTRODUZIONE

La sempre maggiore diffusione delle reti di calcolatori, grazie soprattutto all'espansione di Internet, offre l'opportunità di realizzare su rete servizi anche di tipo amministrativo. Indubbiamente l'utilizzo della rete comporta innumerevoli vantaggi dalla possibilità di scambiare informazioni in tempi rapidissimi e senza vincoli geografici, alla praticità di trattamento e di archiviazione delle informazioni.

Però lo sviluppo delle reti di comunicazione e dei servizi offerti mediante la tecnologia dell'informazione riserva alcuni svantaggi. Le reti digitali sono intrinsecamente insicure: esse non sono state progettate in modo da garantire autoprotezione e difesa contro eventuali abusi. Esse sono particolarmente sensibili all'intercettazione ed all'alterazione dei dati trasmessi nonché alla violazione dei supporti informatici ad essa connessi.

È necessaria dunque una tecnologia che possa garantire un certo livello di sicurezza per i dati che vengono trasmessi e archiviati. Al fine di proteggere i dati diffusi in rete dai pericoli derivanti da un uso illecito delle informazioni, è quindi indispensabile fornire contromisure di sicurezza mirate a garantire integrità, autenticità, riservatezza e non ripudio.

La tecnologia della crittografia a chiave pubblica sembra fornire la risposta più adeguata a queste esigenze. In particolare permette l'autenticazione dell'origine dei dati, l'integrità e il supporto per il non ripudio attraverso la firma digitale, e garantisce la riservatezza tramite operazioni di cifratura dei dati.

La firma digitale basata sulla crittografia a chiave pubblica si è ormai affermata come principale strumento in grado, allo stato attuale della tecnologia, di assicurare l'integrità e la provenienza dei documenti informatici, e quindi di svolgere per questi la funzione che nei documenti tradizionali è assolta dalla firma autografa.

Affinché tale tecnica sia utilizzabile su larga scala, si richiede la realizzazione di infrastrutture a chiave pubblica, con il compito specifico di gestire il ciclo di vita delle chiavi crittografiche.

La PKI (Public Key Infrastructure) è un'infrastruttura di sicurezza costituita da protocolli e servizi, per il supporto di applicazioni basate su crittografia a chiave pubblica. La PKI tramite l'utilizzo dei certificati digitali, consente di soddisfare i seguenti requisiti:

- Autenticazione: garantisce l'identità di un titolare.
- Confidenzialità: garantisce che solo il destinatario di un messaggio o di un documento possa leggerne il contenuto.
- Integrità: garantisce che l'informazione non sia stata alterata nella trasmissione o nell'archiviazione.

- Non ripudio: garantisce che i partecipanti ad una transazione non possano negare di averla eseguita: il mittente di un messaggio non può negare di averlo spedito e chi lo riceve non può negare di averlo ricevuto.

COS'È LA CRITTOGRAFIA

La crittografia è lo studio della codifica e della decodifica dei dati. Il termine crittografia viene dalle parole greche kryptos che significa nascosto, e graphia, che significa scrittura.

Tale scienza che studia i sistemi per rendere certe informazioni segrete e leggibili solo a chi possiede la chiave per decifrarle, oggi è fondata quasi esclusivamente sull'impiego di sistemi informatici e di programmi che svolgono complesse operazioni matematiche.

La crittografia riveste un ruolo fondamentale nell'ambito dei sistemi di sicurezza, essendo in grado di fornire la maggior parte dei servizi contemplati nell'architettura di sicurezza stabilita dall'ISO (International Organization for Standardization), pertanto i sistemi crittografici rivestono un'importanza fondamentale nella soluzione di molte problematiche di sicurezza connesse con la protezione di informazioni.

Garantire che i messaggi vengano letti solo dalle persone autorizzate, che non vengano modificati e che si possa stabilire con assoluta certezza il loro vero autore sono le principali necessità della comunicazione sicura.

Secondo l'ISO le caratteristiche che devono essere garantite in un documento qualsiasi perché quest'ultimo possa essere considerato affidabile sono:

- Confidenzialità: con tale funzionalità si vuole impedire di rilevare informazioni riservate ad entità non autorizzate; la confidenzialità è ottenuta tramite tecniche crittografiche di cifratura dei dati.
- Integrità dei dati: i servizi di integrità dei dati proteggono contro gli attacchi attivi finalizzati ad alterare illegittimamente il valore di un dato; l'alterazione di un messaggio può comprendere la cancellazione, la modifica, o il cambiamento dell'ordine dei dati.
- Autenticazione: i servizi di autenticazione garantiscono l'accertamento dell'identità; quando a qualcuno (o a qualcosa) si attribuisce una certa identità, i servizi di autenticazione forniscono lo strumento con cui verificare la correttezza di tale affermazione. I servizi di autenticazione si suddividono in:
 - servizi di autenticazione dell'entità: in questo caso si autentica l'identità presentata ad un'entità remota che partecipa ad una sessione di comunicazione (le password sono un esempio tipico di strumenti atti ad ottenere autenticazione dell'entità);
 - servizi di autenticazione dell'origine dei dati: in questo caso si autentica l'identità di chi invia un messaggio o crea un documento.

- Controllo degli accessi: una volta che l'autenticazione è avvenuta, è possibile eseguire un controllo degli accessi in modo tale da verificare che vengano utilizzate solo quelle risorse o servizi ai quali si è autorizzati.
- Non ripudio: tali servizi devono garantire che le entità coinvolte in una comunicazione o transazione non possano rinnegare la partecipazione. I servizi di non ripudio non prevencono il ripudio di una comunicazione o di una transazione, forniscono, invece, gli strumenti per dimostrare in caso di contenzioso l'evidenza dei fatti. Il non ripudio, va oltre le problematiche di autenticazione ed integrità: è, infatti, lo strumento con cui dimostrare ad una terza parte che una comunicazione o transazione è stata originata o avviata da un'entità. Si pensi ad esempio al caso di una persona, Alice, che invia un ordine di acquisto di beni a Bob; la paternità dell'ordine di acquisto viene attribuita con assoluta certezza ad Alice se si adotta un servizio corretto di non ripudio; in caso di contenzioso Bob può dimostrare con assoluta certezza che l'ordine di acquisto è stato effettuato da Alice. Nei documenti cartacei, quali contratti, ordini, bonifici, è la firma autografa ad essere utilizzata per garantire il servizio di non ripudio, nei documenti elettronici è, invece, la tecnica crittografica di firma digitale.

Le principali tecniche crittografiche costituiscono i componenti basilari nell'implementazione di tutti i servizi di sicurezza sopra descritti.

La crittografia rende non intelligibile il messaggio pur rimanendo pubblicamente leggibile, trasformando il contenuto del messaggio in modo da renderlo incomprensibile a chi non può eseguire la trasformazione inversa. Trasforma quindi un testo in chiaro in uno cifrato. Con la crittografia si può quindi:

- Proteggere le informazioni depositate sul proprio computer da eventuali accessi non autorizzati.
- Proteggere le informazioni durante il loro viaggio attraverso le reti, locali o planetarie che siano.
- Verificare l'integrità del documento ricevuto;

La forza degli algoritmi di crittografia si basa e si deve basare solo ed esclusivamente sulla segretezza delle chiavi utilizzate e non sulla segretezza dell'algoritmo stesso, in quanto se un algoritmo è segreto, non si può vedere se funziona bene o se ha qualche pericoloso difetto.

I tipi di algoritmi di crittografia oggi disponibili sono tre:

- crittografia simmetrica (detta anche a Chiave Privata);
- crittografia Asimmetrica (detta anche a Chiave Pubblica);
- crittografia Ibrida (combinazione delle precedenti).

GLI ALGORITMI A CHIAVE SIMMETRICA



Fig. 1.1 Cifrario simmetrico

In questo caso la stessa chiave serve per cifrare e decifrare il testo

I cifrari a chiave segreta (o simmetrici) usano la stessa chiave per cifrare e decifrare il messaggio, tale chiave ovviamente non deve essere resa nota.

Mittente e destinatario devono scambiarsi la chiave in modo sicuro altrimenti tutto il cifrario crollerebbe.

Questo tipo di cifrario ha un grave difetto: se la chiave viene a conoscenza di chi è interessato a conoscere abusivamente il contenuto del testo, la segretezza viene meno. Occorre un canale sicuro per trasmettere preventivamente la chiave al destinatario. Ma se si dispone di un canale veramente sicuro, tanto vale usarlo per trasmettere direttamente il testo!

Poiché la robustezza dipende solo dalla chiave essa deve essere scelta in uno spazio sufficientemente grande altrimenti tramite un attacco esaustivo si individuerebbe facilmente la chiave usata. La segretezza della chiave garantisce riservatezza ed integrità.

Se N persone volessero poter comunicare tra loro in modo segreto avrebbero bisogno di $(N(N-1))/2$ chiavi segrete, una per ogni coppia di persone

Tale numero aumenta notevolmente all'aumentare di N e questo rappresenta un grosso limite se la comunicazione coinvolge tanti utenti.

Gli algoritmi a chiave simmetrica servono solo per cifrare i dati.

GLI ALGORITMI A CHIAVE ASIMMETRICA

Nella crittografia a chiave pubblica o asimmetrica, si impiegano cifrari che fanno uso di due chiavi diverse, univocamente correlate: una serve per cifrare il testo chiaro, una per decifrare il testo cifrato con la prima (non importa quale delle due chiavi della coppia venga usata per la prima operazione). I punti fondamentali sono tre:

- non si può decifrare il testo con la stessa chiave usata per cifrarlo
- le due chiavi sono generate con la stessa procedura e correlate univocamente;
- conoscendo una delle due chiavi, non c'è nessun modo di ricostruire l'altra.



Fig. 1.2. Cifrario asimmetrico

Cifratura e decifratura di un documento con un cifrario a chiave asimmetrica

Questo sistema schematizzato in figura 1.2, offre una straordinaria possibilità: chiunque può inviare un messaggio segreto a chi renda pubblica una delle due chiavi.

Bisogna quindi rendere disponibile a qualunque persona una delle due chiavi (chiave pubblica), mentre si deve custodire gelosamente l'altra (chiave privata).

Per mandare a qualcuno un messaggio segreto, si deve cifrarlo con la chiave pubblica del destinatario; solo il destinatario può decifrare il messaggio, perché solo lui dispone della chiave privata correlata alla chiave pubblica usata dal mittente(Fig 1.3).

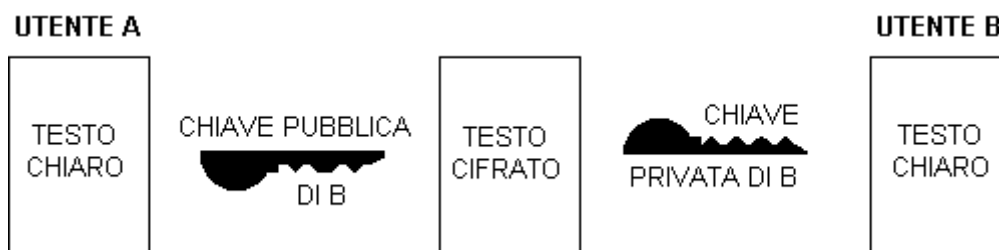


Fig. 1.3. Invio di un messaggio cifrato con un sistema asimmetrico

Il mittente cifra il testo con la chiave pubblica del destinatario, questi lo decifra con la propria chiave privata

I cifrari a chiave pubblica possono essere usati anche al contrario, cioè cifrando il testo chiaro con la chiave privata del mittente. A prima vista questa operazione non serve a nulla, perché chiunque può decifrare il testo con la chiave pubblica dello stesso mittente. Invece è una funzione

importantissima, perché, se l'operazione riesce, significa che il messaggio è stato inviato proprio dal titolare della chiave pubblica usata per la decifratura, perché solo lui dispone della chiave privata con la quale il testo è stato cifrato(Fig. 1.4).



Fig. 1.4. Testo cifrato con la chiave privata del mittente

Se B riesce a decifrare il messaggio con la chiave pubblica di A, questi è certamente l'autore del testo

Quindi con tali algoritmi, a differenza di quelli simmetrici, non è più necessario prevedere un canale sicuro per la trasmissione della chiave, in quanto, essendo la chiave di decifratura distinta da quella di cifratura, è possibile distribuire quest'ultima in maniera non riservata tramite dei server pubblici. Se, poi, n sono gli utenti coinvolti, n è anche il numero di chiavi da distribuire e non $n*(n-1)/2$ come nel caso degli algoritmi simmetrici.

Gli algoritmi asimmetrici garantiscono la confidenzialità nella comunicazione. Infatti, un messaggio cifrato con la chiave pubblica del destinatario fa sì che solo quest'ultimo sia in grado di decifrare tale messaggio, in quanto è l'unico che possiede la corrispondente chiave privata.

Inoltre invertendo l'utilizzo delle chiavi, ossia cifrando con la chiave privata del mittente e decifrando con la chiave pubblica del mittente, è possibile garantire l'autenticazione. È su tale principio che si basa la firma digitale.

RSA

L'algoritmo RSA, proposto nel 1978 da Rivest, Shamir e Adleman, da cui il nome, è il primo sistema di crittografia a chiavi pubbliche che sfrutta l'approccio di Diffie ed Hellman ed è anche quello attualmente più diffuso ed utilizzato.

Può essere usato sia per cifrare sia per firmare digitalmente documenti. È considerato sicuro se sono usate chiavi abbastanza lunghe (almeno 1024 bit). La sua sicurezza si basa infatti sulla difficoltà di fattorizzare numeri interi molto grandi.

Il metodo si basa sulla fattorizzazione di interi di grandi dimensioni e per la sua implementazione si devono seguire i seguenti passi:

1. Scegliere due numeri primi molto grandi p e q .
2. Calcolare il prodotto $p * q = N$, chiamato modulo, in quanto verrà utilizzato nel calcolo del modulo nelle operazioni di codifica e decodifica.
3. Calcolare la funzione di Eulero $E = (p - 1) * (q - 1)$
4. Scegliere un intero e tale che $0 < e < E$ e che sia primo rispetto a E , ossia tale che tra E ed e non ci siano fattori comuni eccetto 1. Si ottiene così la chiave pubblica di codifica $K_p = e$.
5. Calcolare l'intero d per il quale risulta $e * d \bmod E = 1$, ossia trovare l'intero d per cui $[(e*d)-1]$ sia divisibile per E . Si ottiene così la chiave segreta di decodifica $K_s = d$.
6. Rendere pubblici N e $K_p = e$.

Il messaggio cifrato X corrispondente al messaggio M secondo la relazione:

$$X = M^e \bmod N$$

Invece la decodifica avviene secondo la relazione:

$$X^d \bmod N = (M^e \bmod N)^d \bmod N = M^{ed} \bmod N = M$$

La sicurezza dello RSA è affidata alla difficoltà di determinare i fattori primi di un intero quando questo è molto grande, difficoltà che aumenta in modo esponenziale al crescere del numero di bit usati per la chiave. Infatti se un intrusore riuscisse a sapere che N è fattorizzato in p e q , allora potrebbe calcolare E , e conoscendo d risalire a e tramite l'equazione

$$e * d \bmod E = 1.$$

Va osservato che tale algoritmo può essere utilizzato sia per cifrare un documento sia per firmarlo digitalmente. Per far ciò è sufficiente invertire la sequenza di utilizzo delle chiavi: il mittente firma il documento con la propria chiave privata e poi il destinatario verifica la tale firma con la chiave pubblica del mittente. Ciò è possibile in virtù della seguente proprietà dell'aritmetica modulare:

$$(M^e \bmod N)^d \bmod N = (M^d \bmod N)^e \bmod N = M^{ed} \bmod N = M$$

Esempio:

Si scelgono due numeri primi. Per facilità di calcolo non si scelgono due numeri primi grandi.

$$p=3$$

$$q=11 \rightarrow N=p*q=33$$

$$E = (p-1)*(q-1) = 2*10=20$$

$$e=7$$

Chiave Pubblica $K_p = 7$

Si calcola l'intero d per cui $[(e*d)-1]$ sia divisibile per E

$$e * d \bmod E = 1$$

$$d=3$$

Chiave Privata $K_s = 3$

Si cifra il messaggio nel seguente modo:

$$M = 15 \rightarrow X = M^e \bmod N$$

$$X = 15^7 \bmod 33 = 27$$

Si decifra il messaggio criptato nel seguente modo:

$$X^d \bmod N = (M^e \bmod N)^d \bmod N = M^{ed} \bmod N = M$$

$$27^3 \bmod 33 = 15$$

COS'È LA FIRMA DIGITALE

La firma digitale è la tecnologia con cui possono essere effettivamente soddisfatti tutti i requisiti richiesti per dare validità legale ad un documento elettronico firmato digitalmente; garantisce i servizi di integrità, autenticazione e non ripudio.

In particolare le proprietà che deve avere una firma digitale per essere ritenuta valida sono:

- Autenticità della firma: la firma deve assicurare il destinatario che il mittente ha deliberatamente sottoscritto il contenuto del documento.
- Non falsificabilità: la firma è la prova che solo il firmatario e nessun altro ha apposto la firma sul documento.
- Non riusabilità: la firma fa parte integrante del documento e non deve essere utilizzabile su un altro documento.
- Non alterabilità: una volta firmato, il documento non deve poter essere alterato.
- Non contestabilità: il firmatario non può rinnegare la paternità dei documenti firmati; la firma attesta la volontà del firmatario di sottoscrivere quanto contenuto nel documento.

I metodi crittografici a chiave pubblica possono essere utilizzati per la costruzione di strumenti per la firma digitale, variamente concepiti. Mentre nella crittografia la chiave pubblica viene usata per la cifratura, ed il destinatario usa quella privata per leggere in chiaro il messaggio, nel sistema della firma digitale il mittente utilizza la funzione di cifratura e la sua chiave privata per generare un'informazione che (associata al messaggio) ne verifica la provenienza, grazie alla segretezza della chiave privata. Chiunque può accertare la provenienza del messaggio utilizzando la chiave pubblica. La firma digitale viene realizzata tramite tecniche crittografiche a chiave pubblica insieme all'utilizzo di particolari funzioni matematiche, chiamate funzioni hash unidirezionali. Il processo di firma digitale passa attraverso tre fasi:

1. Generazione dell'impronta digitale.
2. Generazione della firma.
3. Apposizione della firma.

Nella prima fase viene applicata al documento in chiaro una funzione di hash appositamente studiata che produce una stringa binaria di lunghezza costante e piccola, normalmente 128 o 160 bit, chiamata *digest message*, ossia impronta digitale. Queste funzioni devono avere due proprietà:

- unidirezionalità, ossia dato x è facile calcolare $f(x)$, ma data $f(x)$ è computazionalmente difficile risalire a x .
- prive di collisioni (collision-free), ossia a due testi diversi deve essere computazionalmente impossibile che corrisponda la medesima impronta.

$$(x \neq y \rightarrow f(x) \neq f(y))$$

Poiché la dimensione del *digest message* è fissa, e molto più piccola di quella del messaggio originale; la generazione della firma risulta estremamente rapida.

L'utilità dell'uso delle funzioni hash consente di evitare che per la generazione della firma sia necessario applicare l'algoritmo di cifratura, che è intrinsecamente inefficiente, all'intero testo che può essere molto lungo.

Mediante un software adatto, nel nostro caso quello di Entrsut, al sistema crittografico adottato, si genera una coppia di chiavi da utilizzare: una, che verrà mantenuta segreta, per l'apposizione della firma; l'altra, destinata alla verifica, che verrà resa pubblica.

Quindi la seconda fase, la generazione della firma, consiste semplicemente nella cifratura con la propria chiave privata dell'impronta digitale generata il precedenza.

In questo modo la firma risulta legata, da un lato (attraverso la chiave privata usata per la generazione) al soggetto sottoscrittore, e dall'altro (per il tramite dell'impronta) al testo sottoscritto.

In realtà l'operazione di cifratura viene effettuata, anziché sulla sola impronta, su una struttura di dati che la contiene insieme con altre informazioni utili, quali ad esempio l'indicazione della funzione hash usata per la sua generazione. Sebbene tali informazioni possano essere fornite separatamente rispetto alla firma, la loro inclusione nell'operazione di codifica ne garantisce l'autenticità.

Nell'ultima fase, la firma digitale generata precedentemente viene aggiunta in una posizione predefinita, normalmente alla fine del testo del documento.

A questo punto possiamo capire come funziona la firma digitale, cioè come si può dare a un testo chiaro la certezza dell'identità del mittente e dell'integrità del contenuto, cioè avere la sicurezza che il documento non è stato modificato da nessuno dopo che il firmatario ha posto la propria firma.

Nel caso dell'utilizzo della forma scritta, l'imputazione del contenuto di un documento a un determinato soggetto è assicurata dalla firma: chi sottoscrive un documento ne assume la paternità.

La diffusione del documento informatico ha consentito di distinguere il suo contenuto dal supporto sul quale esso è stato conservato. In questo modo le correzioni apportate non sono riconoscibili, chi legge il documento finale non è in grado di capire quante e quali modifiche sono state effettuate. Per fare questo è necessaria la "firma digitale" o più precisamente un processo di crittografia a chiavi asimmetriche.

Nel caso in cui Bob debba trasmettere ad Alice un documento informatico assicurandone l'integrità e l'autenticità, lo cripterà con la propria chiave privata e lo invierà ad Alice che, procuratasi la chiave pubblica di Bob, lo decifrerà (Fig. 1.5).

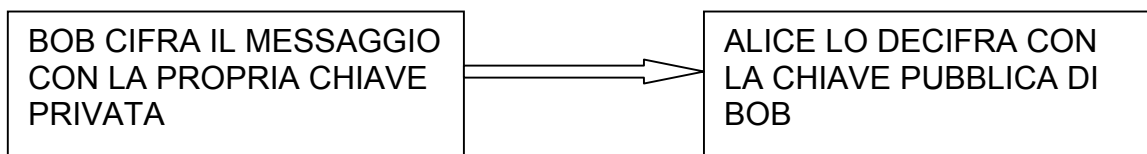


Fig. 1.5. Invio messaggio cifrato da Bob ad Alice con chiave privata

Un documento decifrato con una determinata chiave privata potrà essere decifrato solo con la corrispondente chiave pubblica e viceversa. Rimane il problema della segretezza. Infatti, se per la decifrazione di un messaggio crittografato con una chiave privata è necessaria e sufficiente la chiave pubblica, accessibile a chiunque, il documento cifrato è, per definizione, pubblico o, quantomeno, può essere reso intelleggibile da tutti. Il sistema a chiavi asimmetriche offre la soluzione anche a questo problema, essendo sufficiente invertire l'uso delle chiavi sopra indicato, di modo che il mittente Bob cifrerà il messaggio utilizzando la chiave pubblica del destinatario, che, quindi sarà l'unico in grado di leggerlo perché titolare della corrispondente chiave privata (Fig. 1.6).

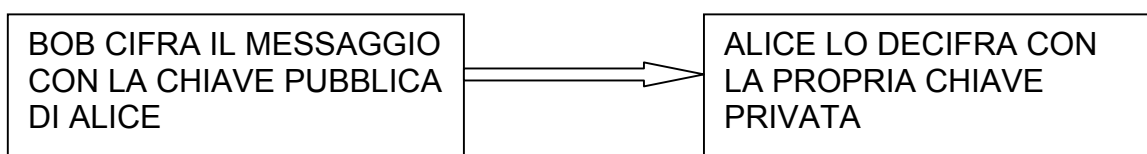


Fig. 1.6. Invio messaggio cifrato da Bob ad Alice con chiave pubblica

Le due funzioni possono poi essere combinate per assicurare l'integrità, l'autenticità del documento e la sua riservatezza. E qui interviene la firma digitale.

Poiché la cifratura di un intero documento è una procedura lunga, ad abbreviare i tempi e conseguire il risultato di assicurare al destinatario che il documento proviene da un determinato soggetto e non è stato alterato, soccorre la procedura di firma digitale che consiste in questo.

Al documento viene applicata una determinata funzione, denominata "hash function", che produce un riassunto chiamato "impronta" di lunghezza fissa (20 caratteri), indipendentemente dalle dimensioni dell'originale.

L'impronta è unica, nel senso che modificando anche un solo carattere del testo si otterrà un'impronta diversa. L'impronta, e non l'intero documento, viene quindi criptata con la chiave privata del mittente in questo modo si ottiene la generazione della "firma digitale" che verrà apposta al documento originale. Al destinatario vengono spediti: il documento con la "firma digitale" in calce e il certificato rilasciato dalla competente autorità di certificazione a garanzia della titolarità della chiave pubblica necessaria per decrittare la firma digitale. Per maggior chiarezza si veda la figura 1.7.

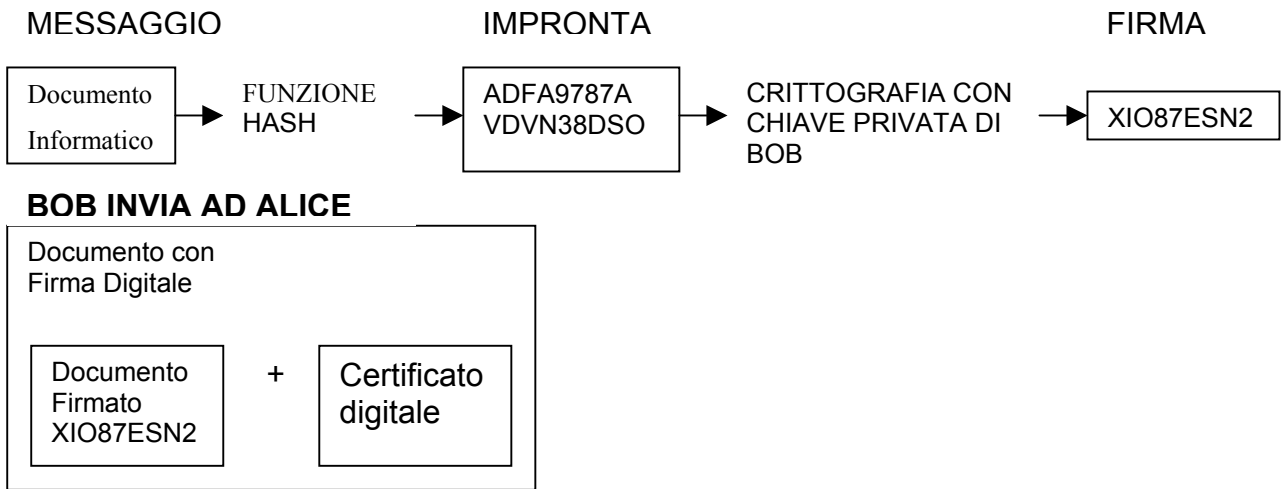


Fig. 1.7. Impronta digitale

Chi riceve il messaggio procederà all'apertura e/o verifica dello stesso mediante il proprio software per l'attività di firma. Il programma acquisirà dal certificato annesso al documento firmato, la chiave pubblica del mittente. Con tale chiave viene decifrata la stringa della "firma digitale" che darà come risultato l'"impronta" del documento. Il destinatario prenderà il documento originario, lo farà passare attraverso la funzione di "hash" e genererà l'"impronta": se coincide con quella decrittata del mittente allora sarà sicuro dell'integrità e provenienza del documento (Fig. 1.8, Fig. 1.9).

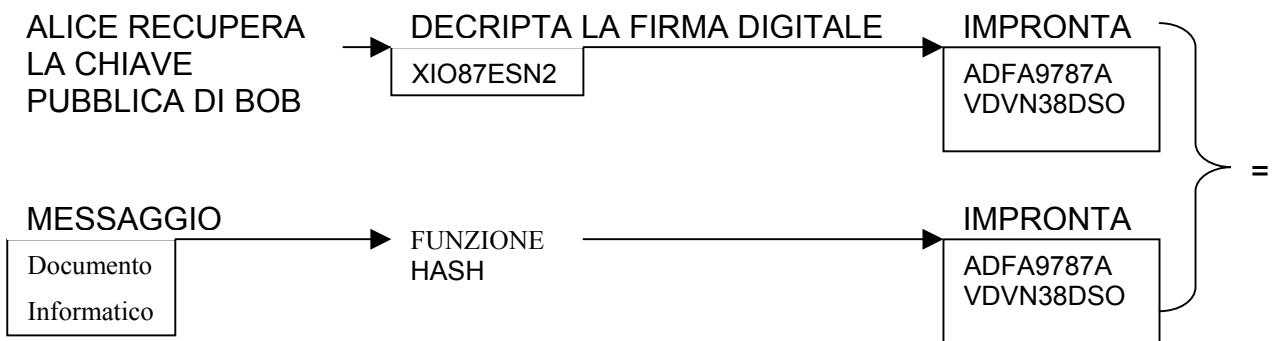


Fig. 1.8 Verifica dell'impronta digitale

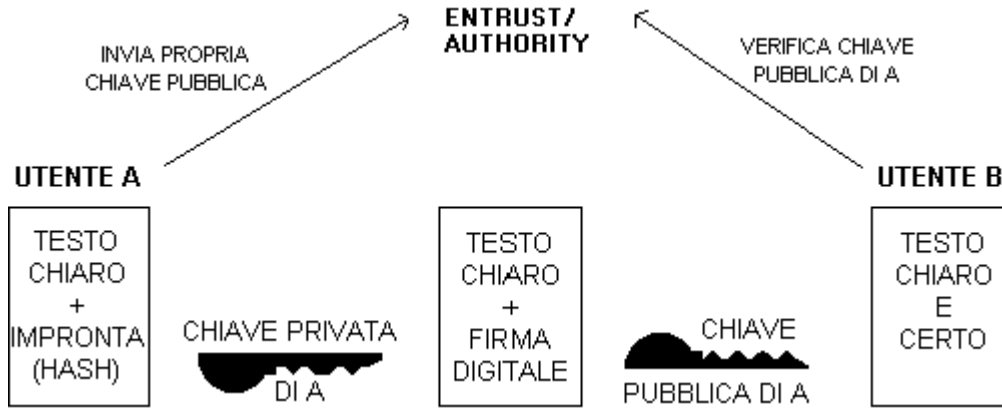


Fig. 1.9. Generazione e verifica della firma digitale

La firma digitale si genera applicando la propria chiave privata all'impronta del testo

COSA SONO I CERTIFICATI A CHIAVE PUBBLICA

Nella tecnologia di crittografia a chiave pubblica, sia in fase di cifratura che in fase di verifica di una firma digitale, occorre ritrovare la chiave pubblica o del destinatario di un messaggio o del firmatario del messaggio firmato. In entrambi i casi il valore delle chiavi pubbliche non è confidenziale e la criticità del reperimento delle chiavi sta nel garantire l'autenticità delle chiavi pubbliche. Quindi si deve essere certi che una certa chiave pubblica appartenga effettivamente all'interlocutore per cui si vuole cifrare o di cui si deve verificare la firma. Se, infatti, una terza parte prelevasse la chiave pubblica del destinatario sostituendola con la propria, il contenuto dei messaggi cifrati sarebbe svelato e non si riuscirebbe a verificare la validità di una firma digitale.

La distribuzione delle chiavi pubbliche è, pertanto, il problema cruciale della tecnologia a chiave pubblica. In un dominio con un numero limitato di utenti si potrebbe anche ricorrere ad un meccanismo manuale di distribuzione delle chiavi: due interlocutori che abbiano una relazione di conoscenza già stabilita, potrebbero, ad esempio, scambiarsi reciprocamente le chiavi attraverso floppy disk. Meccanismi di distribuzione manuale diventano, tuttavia, assolutamente inadeguati ed impraticabili in dominio scalabile dove non c'è alcuna diretta conoscenza prestabilita tra gli interlocutori.

Il problema della distribuzione delle chiavi pubbliche è risolto tramite l'impiego dei certificati elettronici. I certificati a chiave pubblica costituiscono, infatti, lo strumento affidabile e sicuro attraverso cui rispondere ad esigenze di scalabilità; attraverso i certificati elettronici, le chiavi pubbliche vengono distribuite e rese note agli utenti finali con garanzia di autenticità ed integrità.

L'utilizzo dei certificati elettronici presuppone l'esistenza di una Autorità di Certificazione (Certification Authority, CA) che li emetta e li gestisca (Entrust/Authority per il nostro caso).

Ogni certificato è una struttura dati costituita da una parte dati contenente al minimo:

- informazioni che identificano univocamente il possessore di una chiave pubblica (ad esempio nome e cognome);
- il valore della chiave pubblica;
- il periodo di validità temporale del certificato;
- la firma digitale della autorità di certificazione con cui si assicura autenticità della chiave ed integrità delle informazioni contenute nel certificato.

La semplicità del meccanismo di distribuzione delle chiavi è diretta conseguenza delle caratteristiche stesse dei certificati: i certificati, infatti, possono essere distribuiti senza dover necessariamente ricorrere ai tipici servizi di sicurezza di confidenzialità, integrità, e autenticazione delle comunicazioni. Per le proprietà della crittografia a chiave pubblica non c'è infatti alcun

bisogno di garantire la riservatezza del valore della chiave pubblica; durante il processo di distribuzione, poi, non ci sono requisiti di autenticazione ed integrità dal momento che il certificato è per sua costituzione una struttura già protetta (la firma digitale dell'autorità di certificazione sul certificato fornisce, infatti, sia autenticazione sia integrità).

Quindi se una terza parte tentasse di alterare il contenuto di un certificato, la manomissione sarebbe immediatamente rilevata in fase di verifica della firma sul certificato; il processo di verifica fallirebbe e l'utente finale sarebbe avvertito della non integrità della chiave pubblica contenuta nel certificato. Le caratteristiche stesse, del certificato permettono di distribuire i certificati a chiave pubblica anche mediante canali non sicuri (file server insicuri o sistemi di directory o protocolli di comunicazione intrinsecamente insicuri.)

I certificati vengono salvati nella directory a cui gli utenti hanno accesso per

- cifrare mail con la chiave pubblica del destinatario;
- per verificare la firma del mittente tramite la sua chiave pubblica.

COSA SI PUÒ FARE CON LA FIRMA DIGITALE

Essendo una firma, essa ha, in primo luogo, tante applicazioni quante sono quelle della tradizionale firma autografa. La legge consente, mediante l'utilizzo della firma digitale di:

- di sottoscrivere un documento informatico;
- di verificare (quale destinatario) l'identità del firmatario;
- di avere la certezza circa la provenienza, l'integrità e la segretezza del documento;
- di archiviare qualsiasi tipo di documento su supporto informatico con pieno valore legale;
- di tenere in forma informatica con pieno valore legale i libri sociali e le scritture contabili obbligatorie per legge;
- di rendere impossibile il ripudio della paternità di un documento.

Le possibili applicazioni della firma digitale sono:

- comunicazioni ufficiali con le amministrazioni pubbliche;
- risposte a bandi/gare pubbliche;
- moduli di richiesta di vario tipo;
- dichiarazioni fiscali e d'altro tipo;
- trasmissioni di documenti legali;
- rapporti contrattuali su reti aperte (Internet);
- fornitura elettronica di beni e servizi;
- transazioni finanziarie;
- identificazione e autorizzazione;
- gestione di attività in gruppi e sistemi chiusi o a partecipazione controllata;
- gruppi di lavoro e di ricerca;
- transazioni personali.

INDICE DELLE FIGURE.

Fig. 1.1 Cifrario simmetrico	5
Fig. 1.2. Cifrario asimmetrico	6
Fig. 1.3. Invio di un messaggio cifrato con un sistema asimmetrico.....	6
Fig. 1.4. Testo cifrato con la chiave privata del mittente.....	7
Fig. 1.5. Invio messaggio cifrato da Bob ad Alice con chiave privata	12
Fig. 1.6. Invio messaggio cifrato da Bob ad Alice con chiave pubblica.....	12
Fig. 1.7. Impronta digitale	13
Fig. 1.8 Verifica dell'impronta digitale	13
Fig. 1.9. Generazione e verifica della firma digitale	14