Introduzione alla crittografia
Introduzione

I messaggi che passano sulla rete sono in realtà facilmente intercettabili. Esempi di attacchi che mirano all'intercettazione dei messaggi sono lo **sniffing** e lo **spoofing** dell'indirizzo IP. Oltre a ciò, l'amministratore di una macchina possiede le credenziali per intercettare tutti i dati che passano attraverso quel nodo e quindi un amministratore in malafede può intercettare facilmente messaggi destinati ad altri utenti.

L'intera **sicurezza** del sistema è fortemente compromessa dalla trasmissione di messaggi in chiaro. Un messaggio in chiaro intercettato può infatti essere letto, violando così la **confidenzialità**. Nel caso si tratti di una **password** o di una qualunque altra credenziale di identificazione, chi ha intercettato il messaggio avrà modo di sostituirsi al mittente, **abusando della sua identità elettronica** e infrangendo così anche l'**autenticazione** e il **non ripudio**. Con questa credenziale carpita maliziosamente sarà poi possibile sostituirsi all'utente nella gestione delle sue risorse, esponendo a rischio infine anche l'**integrità** e la **disponibilità** dei dati.

In realtà questo tipo di problema è percepito come critico soprattutto nel settore commerciale. In questo contesto è più che mai importante che i messaggi:

- non subiscano alterazioni (integrità): il contenuto dell'accordo non deve essere cambiato.
- Abbiano un mittente univocamente identificabile (autenticazione e non ripudio): la sottoscrizione di un messaggio è irreversibile e univoca, come una firma.
- Non vengano letti senza autorizzazione (confidenzialità): deve essere possibile inviare un numero di carta di credito o altre informazioni riservate con la garanzia che solo il destinatario le potrà leggere.

Crittografia

Il problema di inviare messaggi riservati attraverso sistemi di distribuzione non affidabili è sentito da secoli in ambito militare e sono innumerevoli le metodologie più o meno complesse messe in atto per spedire informazioni agli alleati, senza che i nemici possano decifrarle.

La **crittografia** è un procedimento di codifica e decodifica dei messaggi basata su funzioni parametriche, la cui computazione dipende da un parametro detto chiave. Un messaggio crittografato non è direttamente leggibile se non si possiedono una funzione e una chiave per decriptarlo.

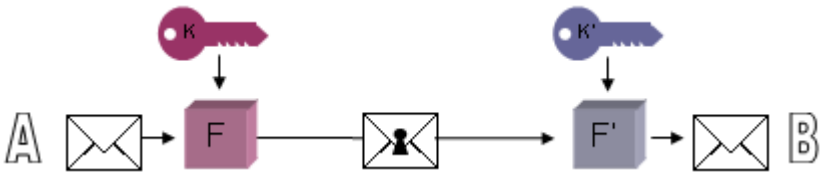
I meccanismi, anche molto evoluti, utilizzati nella crittografia classica, sono in realtà poco adatti ai sistemi basati su *computer* e reti. Una prima differenza sostanziale rispetto al passato risiede nella capacità di calcolo: molti meccanismi indecifrabili dall'uomo in tempi ragionevoli sono in realtà interpretabili velocemente da un attuale calcolatore che è in grado di compiere milioni di operazioni elementari al secondo. Occorre quindi progettare sistemi crittografici con algoritmi così complessi che un intruso, entrato in possesso anche di una grande quantità di testo criptato, non riesca a ricostruire il testo in chiaro corrispondente. Un altro problema deriva dal fatto che nella crittografia classica gli alleati nascondevano ai nemici sia il metodo per crittografare sia la chiave. Sulla rete utilizzare un algoritmo privato di crittografia può significare limitare il numero dei potenziali destinatari dei messaggi, per cui tipicamente la segretezza è riposta esclusivamente nella chiave.

Modello

Il modello su cui è basato un sistema crittografico è il seguente:

- un mittente A vuole inviare un messaggio M a un destinatario B.
- A cripta il messaggio, ovvero applica al messaggio un metodo di cifratura F con chiave di

cifratura K.
- Il messaggio così modificato viene poi spedito via rete a B.
- B riceve un messaggio apparentemente illeggibile, ma possiede un metodo di decifratura F' e una chiave K' che consentono di riportare il messaggio in chiaro.

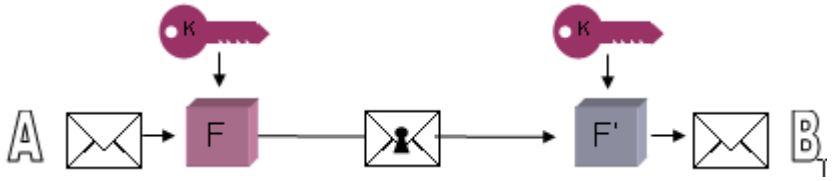


Se un intruso dovesse intercettare il messaggio cifrato non sarebbe in grado di leggerlo a meno di possedere F' e K'.

Le chiavi di cifratura e decifratura possono coincidere e in questo caso si parla di **crittografia a chiave simmetrica** (o a **chiave privata**), oppure possono essere diverse e in questo caso si parla di **crittografia a chiave pubblica**.

Crittografia a chiave privata

I metodi utilizzati tradizionalmente per la crittografia classica erano tutti metodi a chiave simmetrica, basati sull'ipotesi che gli alleati condividessero una chiave nota solo a loro (e per questo detta segreta o anche privata). Quando A vuole spedire a B un messaggio cifrato con un metodo a chiave segreta deve prima di tutto fare in modo che B conosca la sua stessa chiave di crittografia, K, e poi criptare il messaggio con F e K. Quando B riceve il messaggio utilizza F' e K per decriptarlo.



Algoritmi

I moderni sistemi di crittografia a chiave privata utilizzano meccanismi cosiddetti **a blocchi**, che prevedono di scomporre il messaggio da cifrare in blocchi e dunque di operare su di esso per parti. Sui blocchi vengono effettuate operazioni di codifica e trasposizione ricorsive per cui ciascuna parte del messaggio viene rielaborata più volte. La complessità di questo tipo di algoritmi mira a rendere difficile la decodifica da parte di un intercettatore anche quando a essere intercettato è un messaggio lungo che quindi costituisce un caso di prova significativo.

Il più diffuso sistema di cifratura a chiavi segrete si chiama **DES** (*Data Encryption System*) ed è un sistema sviluppato dall'IBM, modificato dalla NSA (*National Security Agency*) e adottato nel 1977 dal governo USA per la protezione dei dati militari. DES è basato su un sistema a blocchi e utilizza chiavi di 64 bit, di cui 8 utilizzati come *checksum* e solo 56 di vera e propria chiave. DES è un algoritmo poco sicuro poiché è pensato per essere efficiente ma anche protetto, su calcolatori di 25 anni fa. La chiave di 56 bit è decisamente troppo corta e quindi, al giorno d'oggi, può essere usato un algoritmo per tentativi per identificarla.

Nonostante ciò, DES è molto utilizzato sia nella sua forma primitiva che in forme più articolate, come a esempio il *Triple DES* (3DES) che tipicamente utilizza blocchi da 64 bit con chiavi a 112 bit. È usato per esempio nella cifratura delle *password Unix* o nei sistemi di autenticazione tipo *Kerberos*.

Sono stati sviluppati molti algoritmi più moderni (e più sicuri) di DES, tra i quali IDEA

(*International Data Encription Algorithm*) del 1991 che utilizza chiavi a 128 bit e AES (*Advanced Encryption Standard*) del 2000 che utilizza chiavi lunghe fino a 256 bit.

Problemi

Anche sistemi con chiave simmetrica impossibili da individuare soffrono di alcuni problemi, dovuti al fatto che la chiave deve essere comunicata al destinatario B perché questo possa decifrare il messaggio.

Un primo problema è insito nella trasmissione della chiave che deve quindi a sua volta essere sicura. Se la chiave passa sulla rete in chiaro, allora può essere intercettata e si può compromettere la **riservatezza**del resto della comunicazione. Un altro problema deriva dalla fiducia che B ripone in A: se A comunica dolosamente la *password* all'intercettatore, B utilizza il canale credendolo sicuro quando sicuro non è. Questa eventualità è in realtà molto peggiore del semplice uso di un canale insicuro perché abbassa i livelli di prudenza dell'utente.

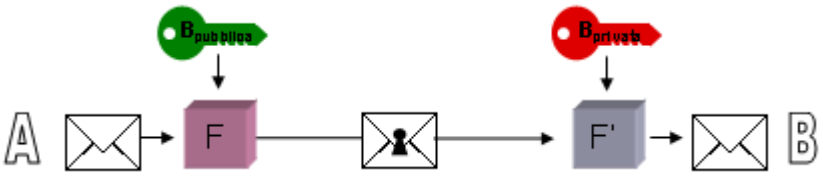
Se l'intercettatore ottiene la *password* può inserirsi nella comunicazione fingendo di essere A con B e/o B con A. In questo caso è dunque compromessa anche l'**integrità** dei messaggi, ovvero non vi è garanzia che un messaggio ricevuto sia esattamente quello spedito dal mittente.

Una soluzione a questo tipo di problema è costituita dalla **crittografia a chiave pubblica**.

Crittografia a chiave pubblica

La **crittografia a chiave pubblica** è un metodo asimmetrico basato sull'esistenza di due diverse chiavi, una utilizzata per criptare e una utilizzata per decriptare. Ciascun utente deve quindi possedere due chiavi, una privata che conosce solo lui e una pubblica che rende nota a tutti. Ovviamente esiste una relazione matematica tra **chiave pubblica** e **chiave privata** che deve rendere semplice calcolare la chiave pubblica a partire da quella privata è difficilissimo (o meglio computazionalmente molto oneroso) calcolare la chiave privata a partire da quella pubblica. La sicurezza di un algoritmo asimmetrico risiede proprio nella difficoltà a individuare la chiave privata, quando si è in possesso di quella pubblica.

Se A vuole inviare un messaggio riservato a B deve dunque procurarsi la chiave pubblica di B (che è disponibile a tutti) e utilizzarla per criptare il messaggio. B sarà l'unico a riuscire a decriptare il messaggio poiché è l'unico in possesso della chiave privata.

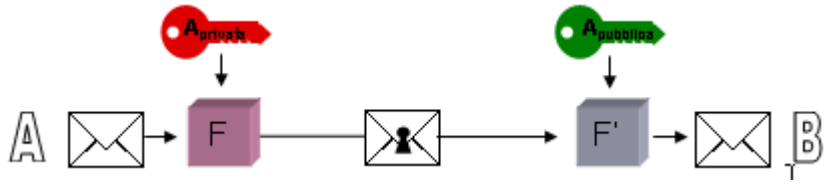


Autenticazione con sistemi a chiave pubblica

I sistemi crittografici a chiave pubblica possono essere utilizzati anche per risolvere problemi inerenti l'autenticazione degli utenti, ovvero per garantire che chi trasmette e chi riceve siano esattamente chi dichiarano di essere. Questo tipo di metodica è alla base della firma digitale e dei certificati.

Se A vuole inviare un messaggio a B e vuole provare a B che il messaggio è effettivamente suo (di A), allora A può criptarlo con la sua chiave privata. B riceverà il messaggio e tenterà di decriptarlo con la chiave pubblica di A. Se l'operazione riesce, allora il messaggio è effettivamente di A, altrimenti B si accorge dell'abuso di identità e può segnalarlo ad A.

Un algoritmo molto diffuso di codifica a chiave pubblica, basato sulla scomposizione in fattori primi di un numero intero, è **RSA** (dal nome dei suoi creatori *Rivest*, *Shamir* e *Adleman*) reso noto nel 1978.



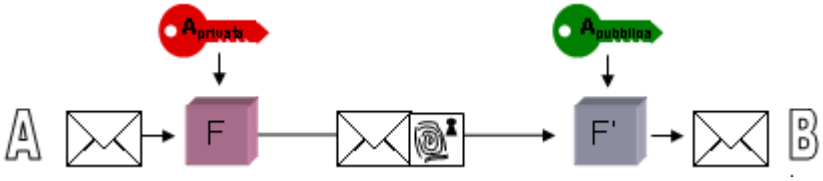
Fingerprint

I sistemi di crittografia a chiave pubblica, incluso RSA, sono piuttosto lenti e la necessità di autenticare un'intera comunicazione può a volte scontrarsi con il ritardo inserito dal criptare l'intero messaggio alla sorgente e dal decriptarlo alla destinazione.

Per rendere più efficiente il meccanismo si utilizza una funzione di **hash** attraverso la quale si calcola una stringa identificativa del messaggio, detta **fingerprint** (impronta digitale) o **message digest** composta da un numero limitato di caratteri (solitamente 128 bit). Questa stringa rappresenta una sintesi del messaggio che è ottenuta attraverso una funzione non invertibile (dato l'*hash* non si risale al messaggio) e che ha una probabilità di generare la stessa *fingerprint* per due messaggi diversi molto bassa. La funzione di *hash* deve inoltre essere molto veloce da calcolare, in modo da rendere significativamente vantaggioso creare il *fingerprint* del messaggio e criptare quello, piuttosto che criptare tutto il messaggio.

A questo punto è possibile autenticare il messaggio limitando l'uso dell'algoritmo di crittografia a chiave pubblica al solo *fingerprint*. Quando A vuole mandare a B un messaggio autenticato e integro, calcola il *fingerprint*, lo cripta con la sua chiave privata e lo aggancia in fondo al messaggio in chiaro. Quando B riceve il messaggio può decriptare con la chiave pubblica di A il *fingerprint* e verificare che esso corrisponde applicando la funzione di *hash* al messaggio ricevuto. Se non c'è conformità tra il *fingerprint* calcolato e quello autenticato, il messaggio non è integro.

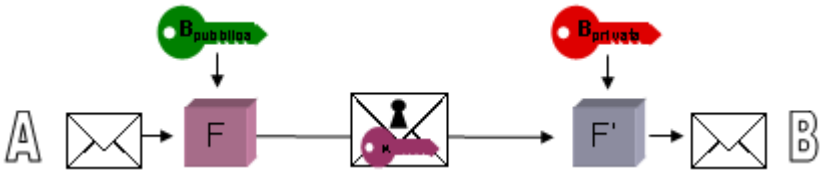
Un algoritmo di *hash* molto utilizzato in crittografia è **MD5** (*Message Digest* 5, 1992) che produce *fingerprint* di 128 bit.



PGP

I sistemi di crittografia propongono spesso soluzioni ibride che utilizzano contemporaneamente più tecniche. Una motivazione a questa scelta è dettata dalla lentezza degli algoritmi a chiave pubblica che impedisce il loro utilizzo in contesti in cui la comunicazione deve essere sollecita. D'altro canto i sistemi a chiave privata hanno il problema della trasmissione sicura della chiave. Una soluzione ibrida di grande successo è PGP (*Pretty Good Privacy*) del 1991 che utilizza come base la cifratura simmetrica di IDEA, la crittografia asimmetrica di RSA e il l'*hashing* di MD5 per le *fingerprint*.

Quando A vuole mandare un messaggio riservato a B, genera casualmente una chiave K e la invia a B criptandola con la chiave pubblica di B. B riceve il messaggio criptato e decriptandolo con la sua chiave privata ottiene K. K è detta **chiave di sessione** poiché la prossima sessione di comunicazione tra A e B avverrà utilizzando K come chiave. A può a questo punto codificare con IDEA il messaggio utilizzando K come chiave. B conosce K e comprende il resto della comunicazione.



Usare PGP

PGP è un *tool* (o meglio un insieme di *tool*) distribuito gratuitamente e disponibile su diverse piattaforme, basato principalmente sulla crittografia a chiave privata di IDEA e sulla crittografia a chiave pubblica di RSA. Il sistema offre supporto a numerose funzionalità tra le quali:

- la **generazione delle chiavi**, pubblica e privata, che vengono prodotte su base casuale a partire da alcuni *input* forniti dall'utente. Ovviamente la chiave privata va mantenuta segreta mentre la chiave pubblica deve essere diffusa il più possibile. La gestione delle chiavi avviene attraverso due *file*: il ***secret ring***, che contiene la chiave privata e va mantenuto segreto, e il ***public ring***, che contiene tutte le chiavi pubbliche note, compresa la propria, e costituisce una specie di rubrica degli utenti riconosciuti.
- La **gestione delle chiavi**, che avviene appunto modificando il *public ring*.
- La **codifica** dei messaggi, attraverso funzioni che consentono di codificare un messaggio, di firmare in chiaro un messaggio e di codificare e firmare un messaggio.
- La **decodifica** dei messaggi, attraverso funzioni che consentono di decodificare messaggi codificati con la propria chiave pubblica, oppure firmati da un mittente di cui si possiede la chiave pubblica oppure codificati e firmati.

Il *download* di PGP può essere fatto a partire dal sito [**The International PGP Home Page**].

Sicurezza del PGP

La crittografia a chiave pubblica riduce di fatto drasticamente la possibilità che un intercettatore si impadronisca della chiave segreta. A fronte di questo vantaggio, la crittografia asimmetrica soffre di un problema correlato con la gestione delle chiavi pubbliche. Non vi è, infatti, alcuna prova che una certa chiave pubblica corrisponda ad una certa persona poiché di per sé non costituisce una prova di identità.

Quando B riceve la chiave pubblica di A:

- non può essere certo che sia realmente di A e non di qualcuno che si spaccia per A. B non ha cioé modo di sapere se è realmente A che utilizza quella chiave.
- Non può sapere se la chiave, che è realmente di A, è stata manipolata e quindi viene usata da terze parti in modo doloso.

Anche in questo caso sono i comportamenti prudenti a difendere gli utenti e i dati:

- le chiavi pubbliche sono gestite automaticamente dai *Keyserver*, che sono archivi di chiavi pubbliche accedibili da tutti. I *Keyserver* si aggiornano l'un l'altro automaticamente per rendere consistente l'insieme di informazioni che gestiscono in modo distribuito.
- Il PGP prevede la possibilità di firmare reciprocamente le proprie chiavi. Questo significa che B può sottoscrivere il fatto che la chiave pubblica di A è una certa chiave K. Se io mi fido della chiave pubblica di B, allora questa controfirma mi fa essere fiducioso, in modo transitivo, anche riguardo alla chiave pubblica di A.

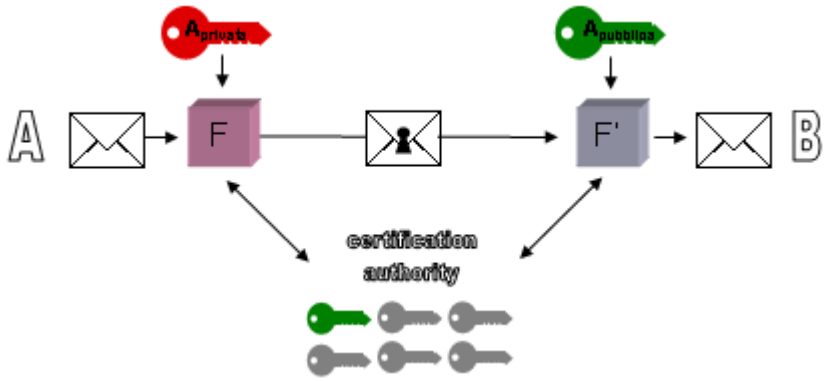
Per contro si deve diffidare di chiavi pubbliche poco pubblicizzate o ottenute in modo poco sicuro, per cui è inopportuno controfirmare una chiave e attribuirle credibilità se non si hanno credenziali opportune. Contemporaneamente è importante dare massima diffusione alla propria chiave in modo

che sia difficile contraffarla.

Certification authority

Per garantire effettivamente che una chiave pubblica corrisponda a una e una sola persona, e ottenere così quella caratteristica di non ripudio che è indispensabile a condurre a termine attività che abbiano effetti legali (dalla sottoscrizione di un contratto al verbale di un esame universitario) occorre un'istituzione che certifichi le chiavi.

Occorre cioé che la chiave pubblica sia in qualche modo garantita da una terza parte che ne ratifichi la validità. Questa terza parte viene chiamata **Certification Authority**.



Certificati digitali

Un **certificato** è un documento elettronico che associa una **chiave pubblica**, e di conseguenza la chiave privata corrispondente, a una particolare identità. Il certificato viene emesso dalla **Certification Authority**, che è il garante dell'identità del proprietario del certificato. La *Certification Authority*, per convalidare il certificato emesso, lo firma con la sua chiave pubblica.

Dunque un certificato tipicamente contiene:

- i dati relativi al proprietario, tra cui il nome e la chiave pubblica;
- i dati relativi al certificato, tra cui la data di scadenza e il numero di serie del certificato;
- i dati relativi alla *Certification Authority*, ovvero il nome e la firma digitale.

È la **Registration Authority** che si incarica delle pratiche di identificazione prima dell'emissione dei certificati, che possono essere differenziati in base al livello di affidabilità che offrono, ovvero al tipo di procedura utilizzata dalla *Registration Authority* per identificare l'utente. La *Certification Authority*, invece, emette il certificato e ne segue il ciclo vitale, rendendolo pubblico con un sistema *on line* sempre disponibile. Sia le *Registration* che le *Certification Authority* svolgono dunque un ruolo fondamentale e particolarmente delicato, per cui sono scelte tra soggetti altamente affidabili e sopra le parti.

L'insieme costituito da tutte le parti, utenti e *Authority*, nonché dalle tecnologie che queste utilizzano, dai servizi che offrono e dalle politiche di gestione che attuano, è detto PKI (**Public Key Infrastructure**).

Certificati e Web

I certificati digitali sono la tecnologia di base utilizzata nella realizzazione di siti *Web* sicuri. Un sito *Web* può offrire all'utente due funzionalità correlate alla sicurezza della comunicazione e strettamente interdipendenti. La prima consiste nel consentire all'utente di identificare in modo univoco il *server Web*, per garantire che eventuali dati personali o codici di accesso siano inviati a

una controparte che è proprio quella che l'utente voleva contattare. La seconda è relativa all'invio sulla rete di dati riservati: supposto che il *server* sia proprio il *server* di riferimento, occorre comunque proteggere da terze parti indiscrete le informazioni che i *client* e *server Web* si vogliono scambiare.

Il *browser* che si collega a un sito *Web* sicuro, utilizza come protocollo **SSL** (*Secure Sockets Layer*) e inizia una sessione sicura chiedendo al *server Web* il suo certificato. Il *server* invia il certificato e il *browser* ne verifica la validità. Solo a questo punto le due parti concordano una chiave di sessione che utilizzeranno per la codifica dei messaggi successivi. È il *client* che genera la chiave di sessione e la cripta con la chiave pubblica del *server Web* (la stessa indicata sul certificato). Solo il *server Web* può quindi leggere il messaggio ed entrare in possesso della chiave di sessione. Questa chiave verrà usate per criptare i messaggi successivi, utilizzando l'algoritmo a chiave privata **DES**.

Il protocollo SSL utilizza url di tipo https:// al posto dell'URL http:// utilizzato dal protocollo HTTP.

Firma digitale

I certificati digitali sono la tecnologia di supporto per dare valore legale alla firma digitale, un sistema che consente a chi sottoscrive il documento di renderne evidente l'autenticità e a chi riceve il documento di verificarne l'integrità. L'Italia ha dato validità giuridica alla firma digitale attraverso vari interventi normativi che definiscono, tra l'altro, chi può essere certificatore e come deve essere fatto il supporto per la firma digitale.
Oggi in Italia la firma digitale ha lo stesso valore giuridico della firma tradizionale.

Sono distinti tre tipi di certificatori: i certificatori di base, che offrono un relativo livello di qualità e sicurezza, i certificatori qualificati e i certificatori accreditati.
I requisiti dei certificatori accreditati e qualificati sono in corso di elaborazione.

La normativa finora vigente prevede che possano essere certificatori qualificati le società per azioni con capitale sociale non inferiore a quello necessario ai fini dell'autorizzazione all'attività bancaria e le pubbliche amministrazioni che emettono chiavi pubbliche di competenza in riferimento al proprio ordinamento. La normativa italiana definisce dunque con molto rigore le caratteristiche del certificatore, al punto che il numero dei certificatori è fortemente limitato .

La ragione di questa scelta fortemente vincolante sta nel fatto che la nomina del certificatore qualificato è particolarmente critica poiché questo emette firme digitali con validità e rilevanza a ogni effetto di legge.

Smart card

Per la legge italiana un dispositivo di firma idoneo è un apparato elettronico programmabile solo all'origine, facente parte del sistema di validazione, in grado almeno di conservare in modo protetto le chiavi private e generare al suo interno firme digitali. Il dispositivo di firma è il supporto candidato alla conservazione della chiave privata e deve dunque essere non riproducibile e, in parte, non modificabile. La chiave deve inoltre essere protetta da una procedura di identificazione del titolare (tipicamente l'inserimento di un PIN) e deve essere fatta in modo da non lasciare alcuna traccia della chiave privata sul sistema di validazione.

Il supporto più diffuso che risponde a tutti questi requisiti è la **smart card** ovvero una tessera plastificata, con dimensioni di una carta di credito, su cui è integrato un *microchip* programmabile. La *smart card* possiede tutte le caratteristiche richieste poiché è dotata di una ROM non cancellabile, di una EPROM che può contenere i dati del proprietario e di meccanismi di protezione che ne evitano la clonazione.

Il dispositivo di firma non può essere invece realizzato utilizzando un *floppy* o un qualunque altro supporto simile, perché è fondamentale che non possa essere duplicato e che contenga informazioni non modificabili ma programmabili solo all'atto dell'emissione della firma. Inoltre, una chiave pubblica memorizzata su *floppy*, dovrebbe essere trasferita sul sistema di validazione per essere controllata poiché il *floppy* in sé non ha capacità di calcolo.

Conclusioni

Questa breve trattazione ha avuto lo scopo di introdurre la crittografia, descrivendone le principali metodologie e applicazioni. La sicurezza dei dati in generale trae vantaggio dall'uso di questo tipo di tecnologie, ma particolare sostegno viene alle transazioni che devono avere validità legale e che quindi necessitano della garanzia di rispettare integrità, confidenzialità, autenticazione e non ripudio.

In particolare rispondono efficacemente a queste problematiche le tecnologie ibride, che integrano meccaniche tipiche della crittografia a chiave privata con quelle proprie della crittografia a chiave pubblica. Quest'ultima però è davvero sicura solo quando esiste un modo certo per identificare con precisione una persona attraverso la sua chiave pubblica e questa proprietà può essere garantita attraverso l'uso di certificati digitali. I certificati digitali sono utilizzati in svariati contesti, sia in quelli applicativi più diffusi, dall'accesso autenticato ai *server Web* alla posta elettronica, che nelle applicazioni proprietarie, dalla protezione dei dati alla firma digitale.

I **riferimenti bibliografici** consentono di approfondire sia l'argomento in generale e i suoi fondamenti matematici, che gli aspetti più pratici legati alle tecnologie e alle applicazioni, che i principali aspetti normativi correlati.