Copyright (c) 2008, 2009, 2010 Fabio Proietti

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.3 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

Authors and contributors
Fabio Proietti
Fabio Ingala fabio AT ingala DOT it

Feedback

Please direct any comments or suggestions about this document to
fabio.proietti AT istruzione DOT it

Publication date and version
2008-11-15, v.0.4
2009-11-15, v.0.5
2010-04-21, v.0.6
2011-06-01, v.0.7

last modified 2013-04-17

Breve introduzione alla crittografia

Sommario

1. La comunicazione
2. La crittografia
3. La crittografia a chiave simmetrica
4. La crittografia a chiave asimmetrica
5. L'impronta di un messaggio
6. La firma digitale
7. I certificati digitali
8. La PEC o posta elettronica certificata
9. Il canale è sicuro?
10. La CEC-PAC
11. L'identificazione
12. I programmi

La comunicazione

Una comunicazione è caratterizzata da due soggetti e un messaggio che viene trasferito: l'emittente invia il messaggio e il destinatario lo riceve. Il messaggio contiene informazione e si propaga attraverso un canale (un mezzo o un supporto fisico), come ad esempio l'aria o un cavo elettrico.

Analizziamo il caso in cui due soggetti desiderino comunicare per mezzo della rete di computer "Internet": si tratta evidentemente di un mezzo di comunicazione non "sicuro" in quanto condiviso da persone che nemmeno conosciamo.
Ci sono diversi aspetti da affrontare per migliorare la sicurezza di questo sistema di comunicazione: potrebbe capitare che io riceva una e-mail da un utente che si finge di essere un'altra persona, oppure, qualcuno potrebbe leggere e/o modificare i messaggi che invio. In altre parole nello scambio di messaggi si deve garantire:

- l'autenticazione: per avere certezza che l'altro soggetto sia effettivamente colui con cui immaginiamo di comunicare.
- la riservatezza: per avere certezza che il messaggio non sia stato intercettato e letto da qualcuno.
- l'integrità: per avere certezza che il messaggio non sia stato modificato.

Si tratta di aspetti o problemi che possono sembrare marginali o improbabili, ma che sono teoricamente possibili quando il mittente e il destinatario comunicano senza potersi incontrare.

La crittografia

La parola *crittografia* significa letteralmente "scrittura nascosta" ed è una tecnica che, utilizzando un determinato insieme di regole, permette di nascondere il contenuto del messaggio scritto ad un estraneo, ad esempio, sostituendo ad ogni

lettera del messaggio una lettera diversa. La crittografia negli ultimi decenni, con lo sviluppo delle telecomunicazioni, è diventata di importanza strategica. Basta pensare alla segretezza con cui devono essere comunicati gli ordini militari durante una guerra.
Il più semplice esempio di crittografia è la crittografia a scorrimento: in un messaggio scritto in modo leggibile (messaggio in chiaro) si sostituisce ad ogni lettera, la lettera dell'alfabeto immediatamente successiva e si ottiene il *messaggio cifrato*. Se il messaggio è costituito dalla frase "Ciao Mario", il messaggio cifrato diventerà "Dkbp Nbslp".
La cifratura avviene grazie a due elementi: l'algoritmo e la chiave.

Nell'esempio della crittografia a scorrimento, l'algoritmo consiste nello scorrimento delle lettere mentre la chiave è un *numero* pari al numero delle lettere che si fanno scorrere. Per riottenere il messaggio in chiaro è necessario conoscere sia l'algoritmo che la chiave usata per effettuare la codifica.
Oggi la crittografia usa degli algoritmi ben noti a tutti, solo le chiavi sono segrete.

La crittografia a chiave simmetrica

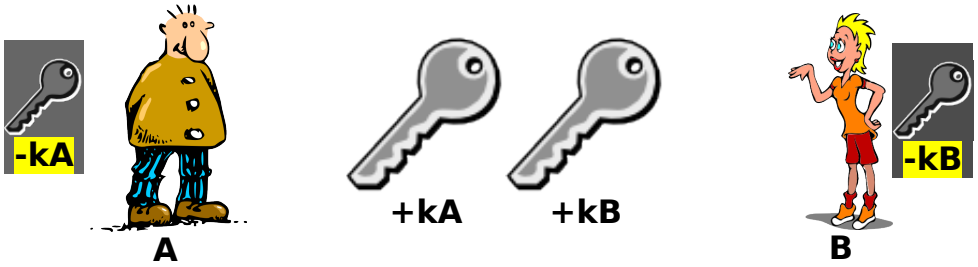
Tecniche così semplici, come la crittografia a scorrimento, sono altrettanto semplici da aggirare. Poiché l'elaboratore utilizza i numeri per rappresentare qualsiasi tipo di messaggio (un testo, un immagine, un video sono sempre costituiti da una sequenza di numeri), per scoraggiare i malintenzionati, si possono eseguire sui messaggi complesse operazioni matematiche usando chiavi di codifica numeriche molto lunghe. Ad esempio, una chiave può essere un numero di 2048 bit.
Se il messaggio in chiaro viene chiamato x, la chiave k e il messaggio cifrato y: $y=f_k(x)$ e viceversa $x=f_k^{-1}(y)$. Nella prima formula si usa la funzione di codifica e nella seconda la funzione inversa.

Tra gli algoritmi standard internazionali più diffusi vanno citati:
- il sistema DES (Data Encryption Standard), usato dal 1976 al 1998;
- il sistema AES (Advanced Encryption Standard), attualmente in uso.

Questi sistemi sono detti a <u>chiave simmetrica</u> perché utilizzano, sia per la codifica che per la decodifica, la stessa chiave segreta.
Per questo motivo i due soggetti potrebbero essere costretti ad incontrarsi fisicamente per scambiarsela in sicurezza e a ripetere questo incontro periodicamente ogni volta che è necessario modificare la chiave.
Un altro sistema di crittografia che non richiede necessariamente l'incontro tra due persone è il sistema a <u>chiave asimmetrica</u>.

La crittografia a chiave asimmetrica (pubblica e privata)

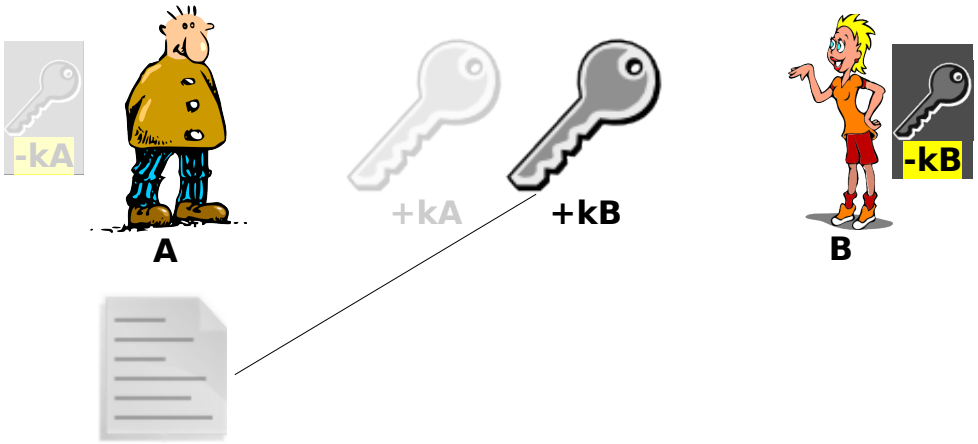
Nel 1978 Rivest, Shamir e Adleman idearono l'algoritomo per la crittografia asimmetrica RSA, utilizzando due chiavi: una segreta e l'altra pubblica.
Il meccanismo di funzionamento di base è il seguente: se la cifratura del messaggio viene fatta usando la chiave pubblica (+k), la decifratura può essere ottenuta usando quella privata(-k), e viceversa.
Se il messaggio in chiaro viene chiamato x e la prima chiave +k, la cifratura è una funzione matematica: $y=f_{+k}(x)$
Il messaggio originale x si riottiene usando l'altra chiave (-k): $x=f_{-k}(f_{+k}(x))$
Le due chiavi sono realizzate in modo che, pur conoscendo una delle due, è molto difficile scoprire l'altra; anche in questo caso, per ragioni di sicurezza, le chiavi hanno una data di "scadenza".
Supponiamo che due amici Andrea e Barbara (A e B) posseggano entrambi una chiave pubblica (+kA e +kB) e una chiave privata (-kA e -kB) e che ognuno dei



due conosca solo la chiave pubblica dell'altro (ovviamente le quattro chiavi sono tutte diverse tra loro).

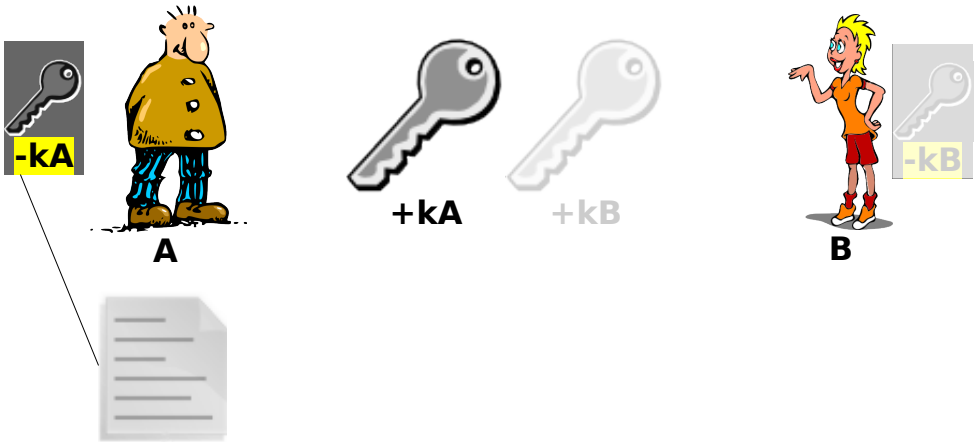
Garanzia della riservatezza

Se A codifica il suo messaggio usando la chiave pubblica di B (+kB), sarà sicuro che solo B sarà in grado di decodificarlo con la propria chiave privata (-kB). Per tutti gli altri il messaggio criptato sarebbe incomprensibile.



Garanzia dell'autenticazione (del mittente) e dell'integrità

Se A codifica il suo messaggio con la sua chiave privata (-kA), B sarà certa che il mittente è proprio A, in quanto potrà decodificarlo usando la chiave pubblica di A (+kA). Inoltre ogni eventuale alterazione del messaggio è impossibile senza usare la chiave privata di A.

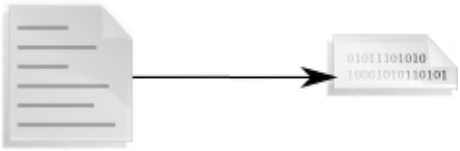


Riassumendo: per ottenere la riservatezza, l'autenticazione e l'integrità del messaggio, si deve usare sia la chiave privata del mittente che la chiave pubblica del destinatario.

La garanzia dell'autenticazione del mittente e dell'integrità possono essere leggermente semplificate, applicando la crittografia solo su una parte del messaggio. Vediamo come.

L'impronta del messaggio (o riassunto)

Partendo da un messaggio (di qualsiasi lunghezza esso sia), usando opportune formule matematiche, chiamate *funzioni hash* (che in inglese significa "fare a pezzettini"), è possibile ottenere un numero (di lunghezza fissa) che cambia completamente cambiando anche una sola lettera del messaggio originale. Questo numero è chiamato riassunto, o impronta, del messaggio.



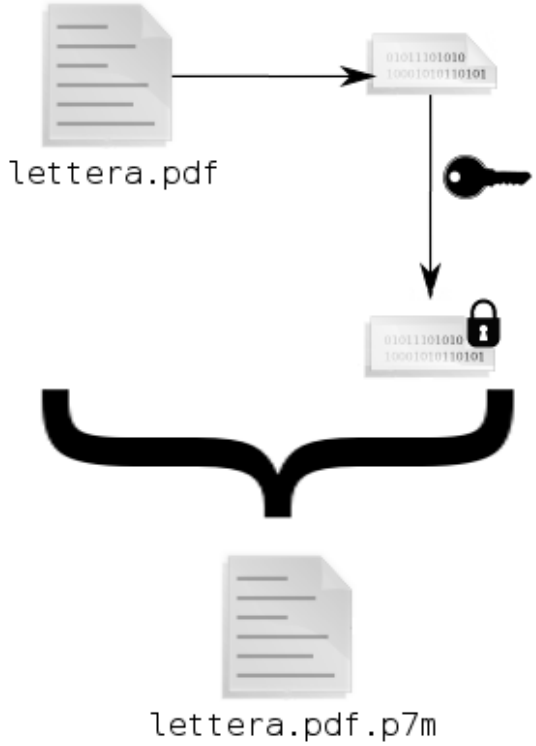
Confronto delle differenti impronte numeriche (espresse in base 16) di due messaggi molto simili tra loro:

```
"Caro Mario"   2d08c492dd2a944dc2b9710b106a2b75(md5)
"Cari Mario"   8f90dbcbe8c0cbae40f77e914417fa6c(md5)
```

La modifica di un messaggio causerebbe quindi un cambiamento anche del suo riassunto, che può essere quindi usato come un rivelatore di eventuali alterazioni del messaggio originale.

La Firma Digitale

Un documento cartaceo ha validità legale quando vi viene apposta la data e una firma con la penna.
Siccome un documento elettronico non può essere firmato (perché si trova "dentro" al computer), allora si aggiunge al documento un numero che rappresenta una firma "digitale" (che vale solo per quel documento).
La cosiddetta "firma digitale" non è altro che l'impronta (o riassunto del file) codificata con la chiave privata del mittente.



La firma digitale viene aggiunta al documento originale per garantire:

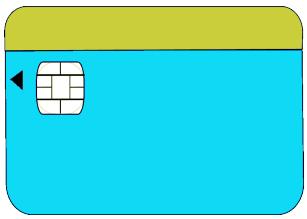
- Autenticazione: perché la firma si deve poter decodificare con la chiave pubblica del mittente.
- Integrità: perché dalla decodifica della firma si deve ottenere un'impronta che deve corrispondere all'impronta del messaggio ricevuto (o del file allegato).

Il documento originale, dopo essere stato firmato, viene modificato da un programma che vi aggiunge la firma.

La firma digitale può avere tre formati xml, pdf, pkcs#7 (.p7m).
Esempio di file prima della firma digitale:
`lettera.txt`
Esempio di file dopo la firma digitale:
`lettera.txt.p7m`
Il file con estensione .p7m contiene sia il documento, la sua firma e la chiave pubblica del mittente per consentire al destinatario di verificare eventuali manomissioni. Per aprire file con estensione .p7m esistono dei plugin per i client di posta elettronica oppure dei software a pagamento (vedere l'ultima pagina di questo documento)

I Certificati Digitali

L'autenticazione però, non garantisce che chi utilizza una chiave (pubblica o privata) sia proprio la persona che dichiara di essere, cioè non identifica una persona con nome e cognome.
Il compito di identificare la persona fisica (o giuridica) con i suoi dati anagrafici viene affidato a soggetti autorevoli, detti *enti certificatori*, che conservano una copia dei documenti per 20 anni (escluse le chiavi private) e che rilasciano un certificato digitale (disponibile al pubblico) che attesta la proprietà della chiave pubblica a lui intestata e il tempo di validità di tale documento e delle chiavi.
I soggetti certificatori sono *accreditati* dal CNIPA in un elenco pubblico.
La chiave privata viene consegnata all'utente in un dispositivo di memoria mobile (ad esempio una memoria USB o una smart card (simile ad una carta di credito).



L'utente ha l'obbligo di utilizzare personalmente il dispositivo di firma. Usando la firma digitale si impedisce di modificare il documento o il nome del suo autore; la firma digitale ha lo stesso valore legale della firma autografa. I certificati possono essere sospesi o revocati.

La firma elettronica

La firma elettronica (detta anche *non* qualificata) è tecnicamente molto simile alla firma digitale (detta anche qualificata).
La differenza è che le chiavi usate per ottenere una firma digitale sono rilasciate su hardware sicuro (come una smart card) e garantite da un Certificato digitale rilasciato da un Ente Certificatore autorizzato, mentre le chiavi usate nella firma elettronica sono state realizzata in proprio oppure da enti non certificati.
I software utilizzati per generare le chiavi pubbliche e private indispensabili sia per la firma digitale (qualificata) che per quella elettronica (non qualificata), sono sostanzialmente gli stessi o comunque molto simili.
Per approfondire questo argomento si rimanda all'ultimo paragrafo.

La PEC o Posta Elettronica Certificata

La firma digitale e i certificati digitali garantiscono il contenuto del messaggio, ma chi garantisce che sia avvenuto l'invio (e la ricezione)? Cioè la non ripudiabilità?
In Italia si è affidato il compito di registrare le spedizioni (e le ricezioni) ai gestori di posta elettronica e solo in Italia queste spedizioni sono legalmente equiparate alle raccomandate. Alcuni dei gestori offrono ai loro utenti la possibilità di aprire una speciale casella di posta elettronica (denominata PEC) che registra il momento in cui un messaggio viene preso in consegna, per essere spedito, o per essere ricevuto da un'altra casella PEC. Per questo motivo è possibile ricevere (o inviare) un messaggio di tipo PEC solo da (o verso) un'altra casella di tipo PEC.
La data dell'invio e della ricezione è quella indicata dal gestore di posta e non quella del computer dove l'e-mail viene ricevuta, ed ha lo stesso valore legale di una lettera raccomandata. Il messaggio si ritiene "spedito" se è stato ricevuto dal primo gestore e "consegnato" se ricevuto dal secondo gestore.
Per garantire il contenuto e l'identità dell'autore di un documento informatico,

come visto prima, si deve usare la firma digitale.
Per legge tutte le società, tutti i liberi professionisti (iscritti ad un ordine o un albo)e tutte le Pubbliche Amministrazioni devono dotarsi di una casella PEC e avere un indirizzo e-mail "istituzionale" e un indirizzo per ogni dipendente.

Il canale è sicuro?

Quando l'utente utilizza la propria web mail o quando gestisce il proprio conto corrente, comunica con il browser tramite un protocollo, che può essere **http** oppure **https**. Quest'ultimo vuol dire "http over Secure Socket Layer" e permette di stabilire una connessione sicura. Di solito per usare una casella PEC si richiede una connessione sicura come quella per comunicare con la propria banca perché deve essere garantita l'inviolabilità del canale di comunicazione tra client e server. Il protocollo https si basa sempre sullo scambio di una chiave pubblica (tra web client e web server) però non garantisce l'identificazione del computer o dell'utente, ma solo la sicurezza del canale di comunicazione.

La CEC-PAC

Il governo ha promesso di fornire gratuitamente ai cittadini una casella di posta certificata, ma queste caselle consentono di inviare messaggi solo alle caselle PEC della Pubblica Amministrazione. Questo tipo di caselle gratuite sono chiamate anche CEC-PAC (Comunicazione Elettronica Certificata tra Pubblica Amministrazione e Cittadino).

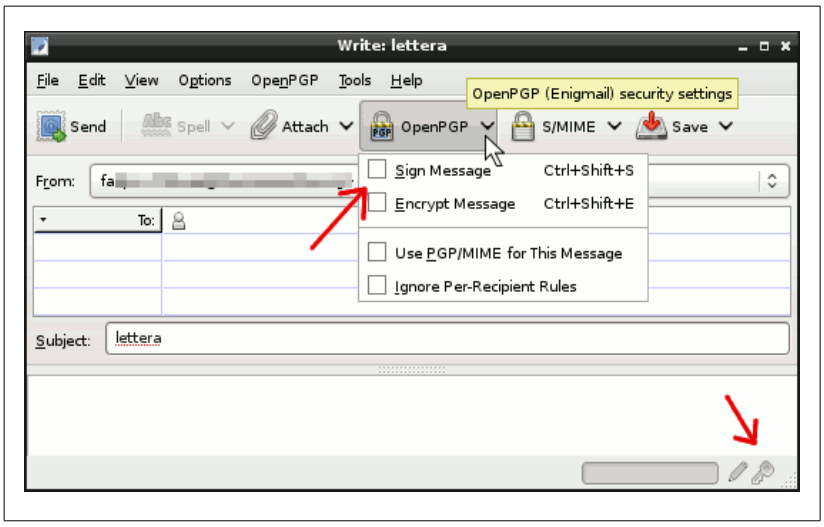
L'identificazione

Fino ad ora si è detto che:la firma digitale permette di garantire l'autenticazione del mittente e del destinatario, che i certificati digitali garantiscono l'identificazione e che la PEC garantisce la non ripudiabilità. Esiste comunque una possibile semplificazione che permette di usare la PEC senza necessiaramente aggiungere la firma digitale ai documenti. Secondo l'art. 65, comma 1, del Codice dell’Amministrazione Digitale (D.Lgs 7 marzo 2005, N. 82):
Le istanze e le dichiarazioni presentate alle pubbliche amministrazioni per via telematica [...] sono valide [...] se sottoscritte mediante la firma digitale [...], ovvero, se trasmesse dall’autore mediante la propria casella di posta elettronica certificata purché le relative credenziali di accesso siano state rilasciate previa identificazione del titolare.
La CEC PAC rilasciata presso gli uffici di poste italiane avviene infatti solo dopo una identificazione "forte".

I programmi

Per ogni file del proprio computer (testi, immagini, audio, video,..) si può generare un'impronta e aggiungere una firma digitale che garantirà la sua integrità e la sua provenienza al destinatario che lo riceverà.
Ogni Ente certificatore rilascia una smart card e un software per utilizzarla per firmare digitalmente un file (documento). Altri software liberi sono:
http://www.opensc-project.org e http://www.openscdp.org/

Un software libero che permette di apporre la firma e controllare le firme del mittenti è GPG, che significa GNU Pivacy Guard.
http://www.gnupg.org/index.it.html
Per utilizzare questo software con il mouse, esistono delle interfacce grafiche: una si chiama GPG Shell
Pper firmare i messaggi di posta elettronica scritti con Mozilla Thunderbird, si può usare un'estensione chiamata Enigmail http://enigmail.mozdev.org/ mentre per aprire i file .p7m si può usare l'estensione thunderPEC
https://addons.mozilla.org/en-us/thunderbird/addon/thunderpec/



Quando il programma di posta elettronica riceve un messaggio con una firma elettronica, può effettuare velocemente una verifica, collegandosi ad un keyserver, dove poter ottenere la chiave pubblica del mittente.
Il file di testo che contiene il codice della propria chiave privata, o è contenuto in un hardware sicuro, oppure si trova nel proprio computer come file protetto dalla lettura di altri utenti.
In pratica, quando è necessario usare la chiave privata, viene chiesto all'utente di digitare una lunga password (che per questo motivo viene chiamata anche passphrase).
Per ulteriori informazioni tecniche si rimanda ai manuali d'uso dei programmi citati.

Indirizzi utili
- enti certificatori: http://www.digitpa.gov.it/firma-digitale/certificatori-accreditati
- indice delle amministrazioni con PEC: http://www.indicepa.gov.it
- motore di ricerca: http://www.paginepecpa.gov.it
- come ottenere un indirizzo CEC-PAC: http://www.postacertificata.gov.it