CRITTOGRAFIA

E

FIRMA DIGITALE

Relazione a cura di:

MORDENTI Marilena

Anno 2002

CRITTOGRAFIA

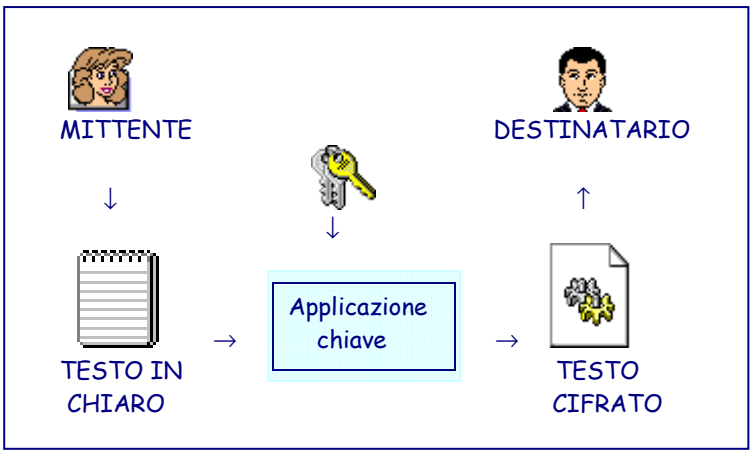
La parola crittografia (dal greco kryptós, nascosto e grápho cioè scrivere) è usata per indicare una grande varietà di tecniche il cui obiettivo è quello di scrivere dei messaggi che nessuno al di là del vero destinatario potrà leggere. Per migliaia di anni regnanti e generali hanno avuto il bisogno di comunicazioni efficienti per governare i loro paesi e comandare i loro eserciti. Essi compresero quali conseguenze avrebbe avuto la caduta dei loro messaggi in mano ostili: informazioni preziose sarebbero state a disposizione delle nazioni rivali e degli eserciti nemici. Fu il pericolo dell'intercettazione da parte degli avversari a promuovere lo sviluppo di codici, tecniche di alterazione del messaggio destinate a renderlo comprensibile solo alle persone autorizzate. Uno dei metodi più bizzarri per trasmettere le informazioni segrete era utilizzato nell'antica Persia e viene raccontato da Erodoto: consisteva nel rapare i capelli di uno schiavo e nel scrivergli il messaggio sulla testa. Lo schiavo si recava poi dal destinatario del messaggio dopo che gli erano ricresciuti i capelli e il messaggio era recuperato rapandoglieli nuovamente… naturalmente il messaggio non doveva essere urgente!
A parte questa piccolo aneddoto, la crittografia non mira a nascondere il messaggio in sé, ma il suo significato. Per rendere incomprensibile un testo, lo si altera per mezzo di un procedimento concordato dal mittente e dal destinatario. Questi può quindi invertire il procedimento, e ricavare il messaggio originale. Il vantaggio è che anche se un estraneo intercettasse il messaggio, quest'ultimo risulterebbe incomprensibile e quindi inutilizzabile perché sarebbe difficile, non conoscendo il procedimento di alterazione, ricostruirne il significato. Oggi la crittografia ha come obbiettivo principale quello di conservare privata una comunicazione che si svolge su un mezzo pubblico, potenzialmente insicuro al quale chiunque può avere facile accesso. La possibilità di mantenere privata la comunicazione dipende dal grado di sicurezza della tecnica crittografica adottata.

Gli obiettivi principali delle diverse tecniche crittografiche utilizzate sono:

- Riservatezza: solo il destinatario deve essere in grado di leggere il messaggio
- Autenticazione: il destinatario deve essere sicuro dell'identità del mittente
- Integrità: il destinatario deve essere sicuro che il messaggio non abbia subito alcuna modifica durante la trasmissione

- Non ripudiabilità: il destinatario può fare risalire, senza possibilità di incertezza, l'origine del messaggio al mittente.

Con la crittografia, un messaggio o, un qualunque file di dati (testo, immagini, musica, ecc.) viene trasformato in un insieme di segni e simboli assolutamente privi di significato per chi non conosca la "chiave" giusta per decifrarli. La chiave consiste in un ‘metodo’ applicato al testo in chiaro per ottenere un testo cifrato:



I procedimenti crittografici si differenziano in base al tipo di trasformazione applicata sul testo in chiaro e al numero di chiavi utilizzate:

- Tipo di trasformazione usata:
  - Sostituzione: Viene concordato un alfabeto permutato. Il mittente trasforma ogni simbolo del testo in chiaro in un simbolo dell'alfabeto permutato, ottenendo così un simbolo del testo cifrato. Il destinatario, ricevuto il crittogramma effettuerà la stessa operazione al contrario per ottenere nuovamente il testo in chiaro.
  - Trasposizione: Ogni simbolo del testo in chiaro viene cambiato di posto, ossia trasposto, secondo una regola stabilita in modo che la ricostruzione del testo in chiaro sia possibile solo a chi conosce quella regola.
  - Sostituzione e trasposizione (utilizzo combinato di entrambe le metodologie)
- Tipo di chiave di codifica e decodifica:
  - Sistemi a chiave privata;
  - Sistemi a chiave pubblica.

I SISTEMI A CHIAVE PRIVATA

Sono quei sistemi in cui l'invio di messaggi segreti è sempre basato sulla comune conoscenza, tra chi invia un messaggio e chi lo riceve, di un codice, una procedura, una chiave da utilizzare per crittografare i messaggi e decrittografarli.

Tali metodologie vengono dette anche a chiave simmetrica e possono essere utilizzati per implementare servizi di sicurezza quali:

- Riservatezza: che protegge l'informazione da visione non autorizzata. Spesso la protezione riguarda solo il corpo del messaggio e non la testata, trasmessa in chiaro per semplificare l'instradamento del messaggio fino al destinatario.
- Integrità: che garantisce che l'informazione non venga alterata e che il messaggio arrivi esattamente come è stato spedito. Tecniche combinate di cifratura e controlli algoritmici (tipo checksum, CRC, ecc) vengono usate per implementare questo servizio.
- Autenticazione: per prevenire la dissimulazione degli utenti; consente al vero mittente di includere nel messaggio informazioni che lo identifichino con certezza.

Le principali debolezze di questi sistemi sono la necessità di comunicare preventivamente la chiave segreta al destinatario e l'uso ripetuto della chiave. Chi si impossessa della chiave è anche in grado di inviare falsi messaggi o alterare gli originali, senza che il destinatario si renda conto della sofisticazione.

I codici cifrati simmetrici possono criptare qualunque testo in bit, byte, una parola o gruppi di parole alla volta.

Possono distinguersi in:

- codice cifrato a flusso dove la chiave si applica ad un bit, un byte o una parola alla volta;
- codice cifrato a blocchi: la chiave viene applicata a blocchi (nei quali è suddiviso il messaggio).

L'utilizzo di un codice cifrato a flussi o a blocchi dipende dall'applicazione per la quale deve essere utilizzato. Normalmente si utilizza la cifratura a blocchi.

Sono quattro i modelli di codice a blocchi più diffusi:

- ECB (Electronic Codebook): ogni blocco del testo viene cifrato in successione sempre con la stessa chiave.
- CBC (Cipher Block Chaining): i blocchi di testo cifrato sono concatenati con i propri predecessori nascondendo le parti ripetute.
- CFB (Cipher Feedback): i blocchi sono concatenati fra loro ma dopo la cifratura del blocco viene fatto lo XOR con il blocco di testo in chiaro successivo, spezzettato in segmenti più piccoli.
- OFB (Output Feedback): utilizza la connessione (feedback) che avviene tra l'output della cifratura precedente e il blocco corrente.

Algoritmi più noti di cifratura simmetrica

DES (Data Encryption Standard)

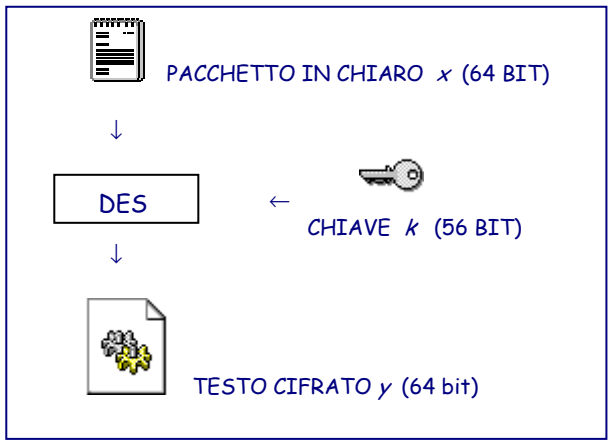
Nel 1972 negli Stati Uniti il National Bureau of Standard (NBS), una parte dell'US Department of Commerce, iniziò un programma per la stesura di uno standard per la protezione dei dati in seguito ad una legge del 1969 nota come Brooks Act, che sottolineava l'esigenza di nuovi standard in materia di sicurezza dati al fine di una migliore utilizzazione dei calcolatori governativi.

L'algoritmo fu scelto dal National Institute of Standard and Technology (NIST) come standard di cifratura nel 1977 con validità quinquennale, poi riconfermato fino al 1998. Fu il risultato dell'implementazione, per lo più hardware dell'algoritmo 'Lucifer' dell' IBM nato nel '70. L'ANSI (American National Standards Institute) lo adottò come uno standard (X3.92) nel settore privato, chiamandolo Data Encryption Algorithm.

Il sistema DES spezza il messaggio in stringhe da 64 bit.

Cifra una stringa *x* di 64 bit in una stringa *y* utilizzando una chiave *k* di 64 bit (di cui solo 56 utilizzabili, i restanti 8 sono bit di parità) e ottenendo il messaggio cifrato *y* (di 64 bit):

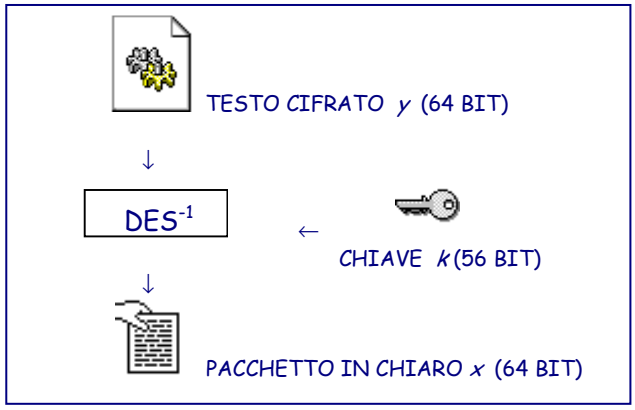
$$y = DES_k(x)$$



L'algoritmo di decifratura DES con chiave *k*, indicato come DES^{-1} ha la seguente proprietà:

$$DES_k^{-1}(DES_k(x)) = x = DES_k(DES_k^{-1}(x))$$

per ogni messaggio in chiaro *x* e per ogni chiave *k*.

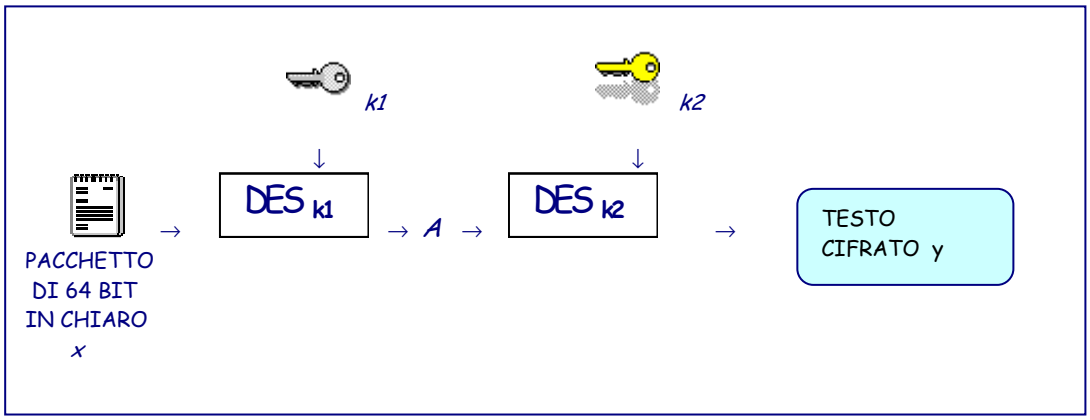


Una delle debolezze del DES relative alla sicurezza è la lunghezza della chiave che, essendo pari a 56 bit fornisce un range delle chiavi piuttosto piccolo: con un attacco che esamina lo spazio delle chiavi in maniera esaustiva, sono necessari in media 2^{55} tentativi per indovinare la chiave. Di fronte a queste problematiche si è progettato un cifrario successivo al DES: il **DOPPIO DES**: cifrando due volte il messaggio con due chiavi diverse (una per ogni passo di cifratura). La chiave diventa lunga 56×2 = 112 bit con un grosso incremento del range di chiavi probabili.

La cifratura avviene in questo modo:

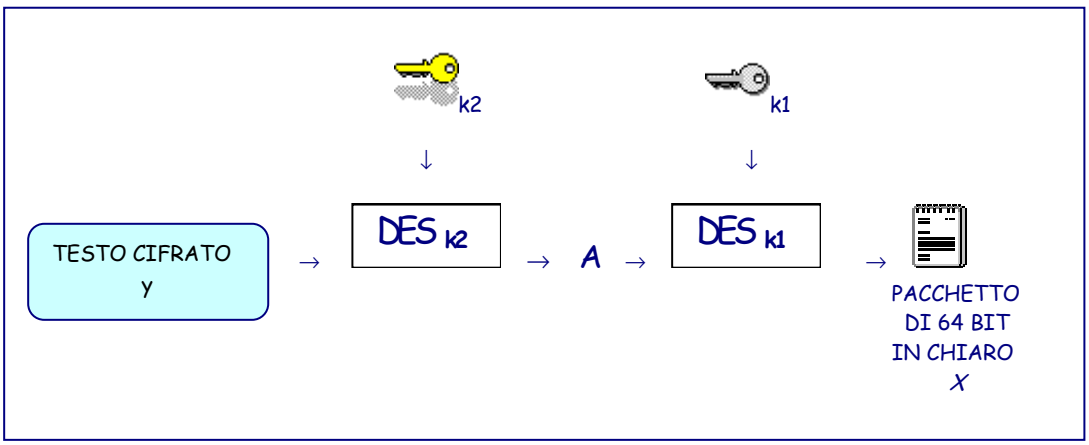
Dato un blocco x di 64 bit del testo in chiaro e 2 chiavi k_1 e k_2 a 56 bit, cifriamo x con la chiave k_1 ed otteniamo un blocco A di 64 bit; cifriamo quindi A con la chiave k_2 ed otteniamo il corrispondente testo cifrato y:

$y = DES_{k2}\,(DES_{k1}\,(x))$



La Decifratura è analoga alla cifratura, ma richiede che le chiavi siano applicate nell'ordine inverso. In particolare, dato un blocco y di 64 bit del testo cifrato e 2 chiavi k_1 e k_2 a 56 bit, decifriamo y con la chiave k_2 ed otteniamo un blocco A di 64 bit; decifriamo, quindi, A con la chiave k_1 ed otteniamo il corrispondente testo in chiaro x:

$x = DES_{k1}^{-1}\,(DES_{k2}^{-1}(y))$



Con il DES si possono usare tutti i quattro modelli di codice a blocchi: ECB è eccellente per la cifratura delle chiavi; CFB è usato tipicamente per cifrare caratteri individuali; OFB è usato per cifrare comunicazioni via satellite (dove è necessario ridurre al minimo la possibilità di errori); ed infine entrambi CBC e CFB possono essere usati per l'autenticazione di dati.

Il Des, come conseguenza dell'aumento delle capacità elaborative delle moderne CPU è sempre più vulnerabile ad attacchi del tipo 'exhaustive-search' ossia attacchi nei quali viene effettuata la scansione esaustiva di tutte le possibili chiavi fino a trovare quella giusta. Infatti con l'utilizzo di apposite macchine dette (DES-cracker) con un notevole costo hardware, è possibile recuperare una chiave DES in tempi relativamente brevi (secondo la legge di Moore che riduce sempre più l'impegno necessario alla 'rottura' di un algoritmo di cifratura in termini di tempo e apparecchiature). Il 17 luglio 1998, l'EFF (Electronic Frontier Foundation) è riuscita a implementare un sistema di schede multiprocessore in grado di violare un sistema DES a 64 bit in meno di 5 giorni, generando tutte le 2^{56} chiavi possibili. In seguito alla consapevolezza della riduzione dei tempi in cui è possibile identificare una chiave DES, il NIST (National Institute of Standards and Tecnology, agenzia del Dipartimento del Governo americano) ha da tempo consentito l'utilizzo nell'amministrazione americana del DES solo per i sistemi legacy mentre per i nuovi progetti l'algoritmo da utilizzare è il Triplo DES.

Il **TRIPLO DES** corrisponde alla specifica ANSI X9.52 del 1998 e allo standard FIPS (Federal Information Processing Standard) 46-3. Consiste nel riutilizzare DES criptando più volte consecutivamente il messaggio con diverse chiavi. Il 3DES usa tre chiavi a 56 bit per un totale di 162 bit di chiave, funziona come il Doppio DES ma con un'ulteriore terza cifratura. Ovviamente, l'algoritmo 3DES diventa così tre volte più lento del DES e, sebbene più resistente ad un possibile attacco, non offre lo stesso livello di sicurezza di un algoritmo di cifratura realmente in grado di supportare chiavi lunghe.

Nel 1997, il NIST indisse un concorso pubblico per la ricerca di un algoritmo da utilizzare per l' Advanced Encryption Standard (**A.E.S**.). L'obiettivo fondamentale del NIST era quello di stabilire un nuovo standard che diventasse il punto di riferimento nel prossimo secolo nel campo della sicurezza. Nel novembre 2001 è stato approvato in via definitiva l'algoritmo di Rijndael quale nuovo standard AES (FIPS 197).

Lo standard prevede una taglia del blocco di input di 128 bit, mentre per la chiave di cifratura prevede tre possibili lunghezze 128, 192 e 256 bit (rispettivamente AES-128, AES-192 e AES-256). Lo standard diventerà effettivo il 26 Maggio del 2002, sei mesi dopo la sua approvazione.

L'esigenza di avere un'alternativa a Triple-des non è nata dal fatto che non sia un algoritmo robusto ma piuttosto perché ha una limitata velocità di elaborazione ed è abbastanza difficile implementarne versioni per processori con limitate risorse elaborative e di memoria, come quelli delle smart-card. Con AES si ritiene che lo sforzo implementativo sia ridotto. Prodotti che implementano l'algoritmo di Rijndael sono già disponibili, Tuttavia lo standard AES è molto recente e non è stato reso ancora disponibile dal NIST un test di conformità per i prodotti che lo implementano.

Altro algoritmo di cifratura a chiavi simmetriche è **IDEA** (International Data Encryption) nato nel 1991. Come il DES è un codice cifrato a blocchi con blocchi di 64 bit, la chiave però è di 128 bit, che rende più difficile la possibilità di riuscita di ricerca esaustiva nello spazio delle chiavi. Anche questo come il DES può essere usato nei 4 modelli di cifratura a blocchi sopra citati: ECB, CBC, CFB e OFB. A differenza del DES, che era stato progettato per implementazioni hardware, IDEA è stato creato per il software.

La cifratura con IDEA comporta una divisione di un blocco di 64 bit di testo in chiaro in 4 sottoblocchi di 16 bit. Ogni sottoblocco subisce 8 cicli in cui sono coinvolte 52 sottochiavi diverse a 16 bit ottenute dalla chiave a 128 bit. Le sottochiavi sono generate in questo modo:

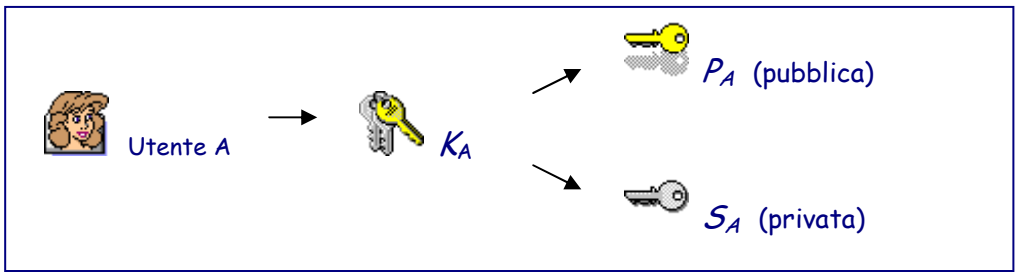
- La chiave a 128 bit è divisa in 8 stringhe di 16 che sono le prime 8 sottochiavi;
- Le cifre della chiave a 128 sono slittate di 25 bit a sinistra in modo da generare una nuova combinazione, il cui raggruppamento ad 8 bit fornisce le successive 8 sottochiavi;
- Il secondo passo è ripetuto finché le 52 sottochiavi sono generate.

Ogni ciclo comporta calcoli come XOR, addizione modulare e moltiplicazioni modulari. Durante i cicli il secondo e il terzo blocco si scambiano di posto mentre al ciclo finale i 4 sottoblocchi vengono concatenati per produrre un blocco di testo cifrato a 64 bit. La decifratura è identica eccetto il fatto che le sottochiavi sono ottenute in maniera diversa dalla chiave principale a 128. L'uso non commerciale di IDEA è libero.

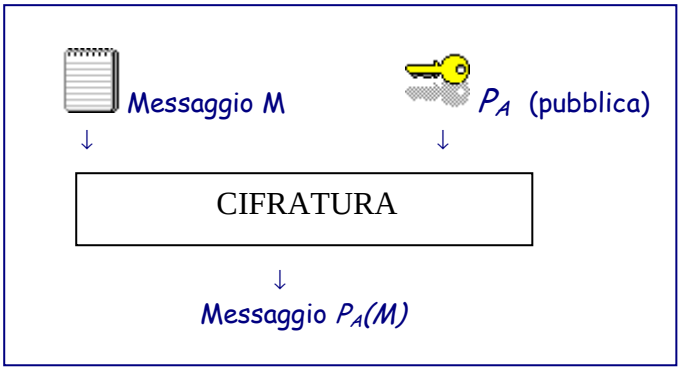
I SISTEMI A CHIAVE PUBBLICA

Sono chiamati anche sistemi a due chiavi o asimmetrici, Nascono nel 1976 ad opera di Whitfield Diffie e Martin Hellman. Differiscono dai sistemi crittografici simmetrici perché non c'è una singola chiave segreta che deve essere necessariamente comunicata e condivisa da una coppia di utenti, ma si basa sul concetto fondamentale che un messaggio codificato con una precisa chiave pubblica può essere decodificato solo con la corrispondente chiave privata che è unica ed è associata strettamente a quella pubblica.

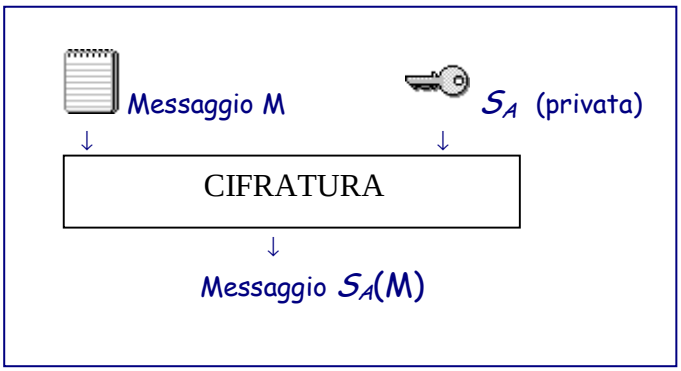
Un generico utente A ha una propria coppia di chiavi $K_A = (P_A , S_A)$, dove P_A è pubblica e S_A è privata. Le chiavi pubbliche vengono memorizzate e rese disponibili agli utenti di quel sistema di crittografia.



La chiave pubblica P_A effettua una trasformazione pubblica su un certo messaggio M generando il messaggio $P_A(M)$:



La chiave privata S_A effettua una trasformazione privata generando il messaggio S_A(M).



Detto M l'insieme dei messaggi, le funzioni P_A(M) e S_A(M) sono definite, rispettivamente, funzioni di cifratura e decifratura. Il principale requisito di questa funzione è che deve essere del tipo one-way (facile da calcolare ma difficile da invertire).

Quindi per garantire sicurezza: Supponiamo che A voglia spedire un messaggio M in maniera sicura B. Allora:

- A ottiene la chiave pubblica di B, P_B
- A calcola il testo cifrato $C = P_B$ (M) e lo spedisce a B;
- B riceve il testo cifrato C e usa la sua chiave privata S_B per ottenere il messaggio in chiaro.

Se un estraneo intercetta la trasmissione da A, non può decifrarla perché S_B è privata. Tuttavia il destinatario B non può essere certo dell'identità del mittente.

Supponiamo che A voglia mandare un messaggio a B garantendo l'autenticità (cioè facendo in modo che B sia sicuro che A è proprio il mittente di quel messaggio):

- A calcola quella che si definisce la sua firma digitale C utilizzando la sua chiave privata: C = S_A (M);
- A spedisce la coppia (M, C) (messaggio + firma);
- Quando B riceverà la coppia (M, C) potrà verificare che questo provenga da A essendo P_A la chiave pubblica di A, verificando l'equazione M = P_A (C).

Differenze tra sistemi a chiave pubblica e i sistemi a chiave privata

Nella crittografia a chiave privata:

- La chiave di cifratura è uguale a quella di decifratura, e comunque ciascuna può essere facilmente calcolata dall'altra.
- La chiave è conosciuta dal mittente e dal destinatario.
- La chiave deve essere tenuta segreta da entrambi.

Con la crittografia a chiave pubblica invece:

- La chiave di cifratura è completamente diversa dalla chiave di decifratura.
- La chiave di cifratura si considera nota in quanto è resa pubblica dal destinatario.
- La chiave di decifratura deve essere tenuta segreta dal destinatario.
- Le funzioni di cifratura e decifratura sono note a tutti.

Algoritmi più noti di cifratura asimmetrica

RSA (Rivest, Shamir, Adleman) nasce nel 1978. Il punto di forza su cui si basa tale metodologia è che la derivazione della chiave segreta da quella pubblica è molto complessa, anche su un calcolatore con notevoli capacità elaborative. Si basa sulla fattorizzazione di numeri interi. La funzione unidirezionale è costituita sfruttando il fatto che è facile calcolare il prodotto di due numeri primi molto grandi, ma dato il loro prodotto, è molto difficile risalire ai fattori che lo compongono.

Vediamo un esempio di calcolo delle due chiavi di un mittente generico:

- Genera due numeri primi molto grandi, all'interno di un range predefinito (io utilizzerò per comodità due numeri primi molto piccoli):

  $p = 17 \qquad q = 11$

- Calcola N che è il prodotto di p x q: $N = 17 \times 11 = 187$
- Calcolo $T = (p - 1) \times (q - 1)$: $T = 16 \times 10 = 160$
- Genera un altro numero intero P_A da utilizzare come chiave pubblica, che sia primo rispetto a T : $P_A = 23$

- Calcolo l'intero S_A , da utilizzare come chiave privata, per il quale risulta che

  $(P_A * S_A)$ Mod T = 1 : $(23 \times d)$ Mod 160 = 1

  ottengo alcuni valori: 161, 321, 481

  Tra i risultati vado a prendere quello compreso tra T e N quindi: 161

- Il nostro mittente rende pubblici: N = 187

  P_A = 23

Mantiene segreta la sua chiave S_A (161).

Il destinatario eseguirà la stessa procedura generandosi le sue due chiavi: privata S_B e pubblica P_B e rendendo pubblica quest'ultima.

Quindi riassumendo:

Per ottenere sicurezza:

- Il mittente cifra il messaggio con la chiave pubblica P_A del destinatario;
- Il destinatario, ricevuto il messaggio lo decifra con la sua chiave privata S_A.

Per ottenere sicurezza e autenticazione:

- Il mittente cifra il messaggio con la sua chiave privata S_A
- Poi cifra ulteriormente il risultato con la chiave pubblica P_B del destinatario;
- Il destinatario decifra il messaggio con la sua chiave privata S_B ;
- Poi decifra il risultato con la chiave pubblica del mittente P_A .

Si considera generalmente sicuro con chiavi sufficientemente lunghe (a 512 bit e' poco sicuro, a 768 bit moderatamente sicuro, da 1024 bit in su, sicuro).

FUNZIONI HASH

Al fine di garantire l'integrità del messaggio cioè la corrispondenza tra ciò che il mittente invia e ciò che riceve il destinatario, normalmente si procede alla cifratura (usando chiavi asimmetriche) non dell'intero messaggio ma della sua impronta (si può definire anche 'riassunto') che prende il nome di Message Digest. E' molto più veloce cifrare l'impronta invece dell'intero messaggio in chiaro. Il Message Digest (MD) viene generato attraverso l'applicazione di algoritmi di hash.

Il mittente quindi trasmetterà oltre al messaggio anche il suo MD affinchè il destinatario possa ritrovare il riassunto del messaggio ricevuto, se l' MD ricevuto è uguale a quello ricalcolato significa che il messaggio non è stato modificato lungo il percorso.

La creazione di quest'impronta (MESSAGE Digest) consente:

- La sua unicità cioè l'impossibilità di ottenere esattamente la stessa impronta partendo da due file di dati diversi, quindi se si modificasse anche un solo carattere del messaggio originale, la riapplicazione della funzione di hash creerebbe un risultato diverso.
- L'impossibilità di ricostruire il file originario conoscendo l'impronta e l'algoritmo utilizzato.

Quindi un utente A che intende inviare un proprio messaggio M:

1. Calcola z = MD(M)
2. Firma l'impronta z costruendo y tramite la sua chiave privata.
3. Trasmette all'utente B la coppia (M,y).

Una volta che il messaggio firmato è stato trasmesso, il destinatario B effettua le seguenti operazioni:

1. Applica a y la chiave pubblica del mittente ottenendo z
2. Calcola z' mediante la funzione hash pubblica
3. Se $z' = z$ allora il messaggio non è stato modificato durante la trasmissione.

Alcuni algoritmi di hash:

MD2 - (Message Digest 2) produce un valore di hash di 128 bit e richiede come input multipli di 16 byte.

MD4 - Come il precedente, produce valori di hash di 128 bit ma i calcoli sono ottimizzati per i registri a 32 bit. Richiede PAD (aggiunta di bit al messaggio in ingresso) a multipli di 512 bit.

MD5 - Non cambia molto sulla struttura, è solo un'estensione dell'MD4 anche se un po' più lento.

SHA-1 – (Secure Hash Algorithm-1). L'algoritmo assomiglia all'MD5, genera un'impronta di 160 bit.

RIPEMD-160 (RIPE Message Digest – 160 bit), nella versione originale generava un digest a 128 bit, poi elevati a 160.

FIRMA DIGITALE

La firma digitale si può definire come un'informazione aggiunta a un documento informatico al fine di:

- attribuirne la paternità al mittente
- assicurarne la riservatezza
- permettere il non ripudio: chi ha prodotto il documento non può negare di averlo fatto.

Nel caso dell'utilizzo della forma scritta tradizionale, il contenuto di un documento è direttamente attribuibile ad un determinato soggetto attraverso la sua firma: chi sottoscrive un documento ne assume la paternità.

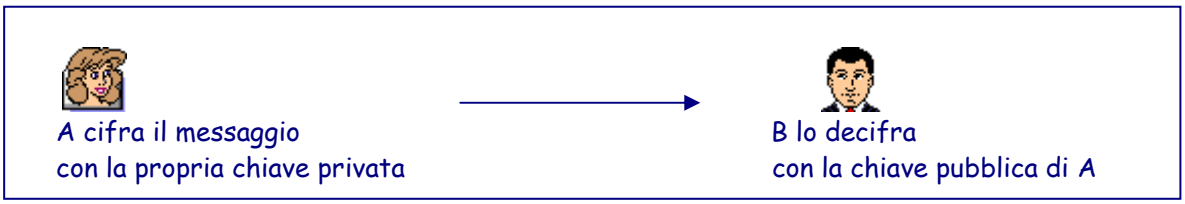
Con l'utilizzo del documento informatico si è creata una scissione tra il contenuto del documento e il supporto sul quale è conservato. Le eventuali rettifiche apportate non si distinguono dal documento originario: il destinatario che legge il documento finale non è in grado di accertare in alcun modo se sono state apportate modifiche e quali sono state.

Per ottenere la “certezza” del documento informatico è necessaria la "firma digitale" o più precisamente un processo di crittografia a chiavi asimmetriche che lega in maniera certa e indissolubile il documento all’identità del mittente.

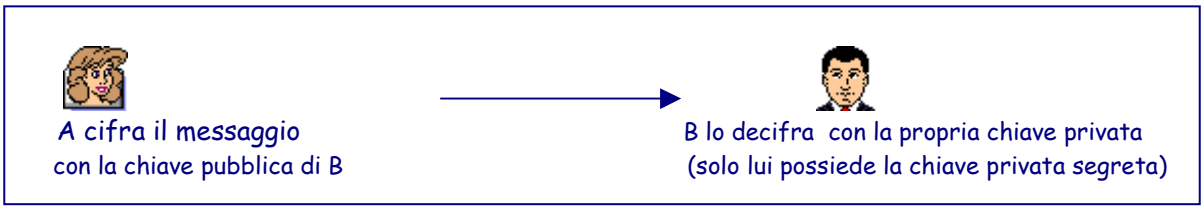
Con la firma digitale quindi, chi vuole inviare un messaggio deve possedere due chiavi: una pubblica e una privata, diverse tra loro, la prima segreta, la seconda invece conosciuta da chiunque perché pubblicata su registri tenuti da un apposito certificatore: Certification Autority (CA) che garantisce l’identità fisica del titolare della chiave. Le due chiavi sono strettamente legate tra loro ma dalla chiave pubblica nessuno deve essere in grado di risalire alla chiave privata.

Riepilogando il concetto di chiavi asimmetriche: Se il mittente A deve trasmettere un documento informatico a B assicurando a quest’ultimo la sua paternità lo cifrerà con la propria chiave privata e lo invierà a B.

A sua volta B, procuratasi la chiave pubblica di A riuscirà a decifrarlo.



Per assicurare la segretezza:



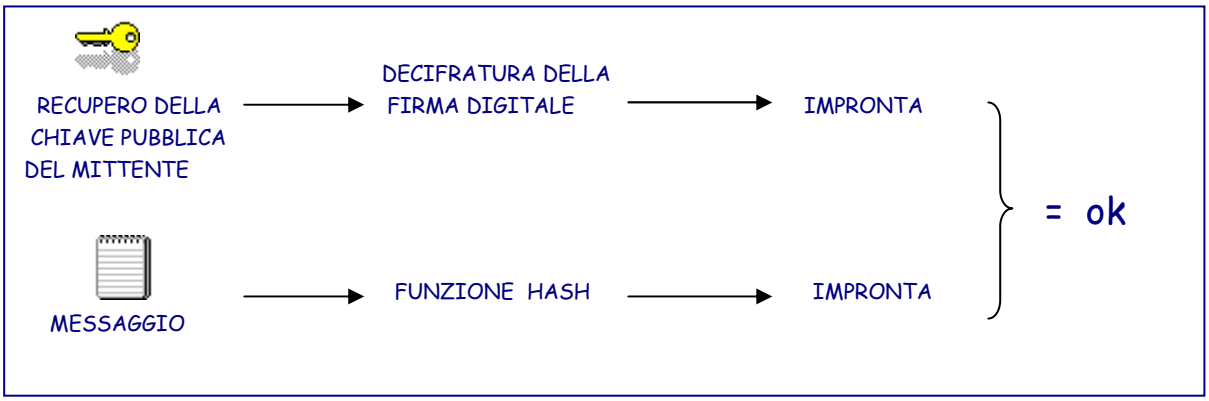
Le due funzioni possono poi essere combinate assicurando quindi riservatezza, autenticazione e non ripudiabilità, sempre che si ritenga sicura l’identità del mittente (a questo scopo esistono le CA).

Poiché la cifratura di un intero documento è una procedura lunga, per abbreviare i tempi ottenendo le stesse certezze si utilizzano le funzioni hash che, come già spiegato, producono un'impronta di lunghezza notevolmente ridotta rispetto al messaggio originale. L'impronta è di lunghezza fissa e dipende dal metodo usato: 160 bit per SHA1 (Secure Hash Algorithm oppure 128 bit per MD5 (Message Digest 5). Si cifrerà quindi la sola impronta con la chiave privata del mittente ottenendo così la firma digitale che verrà collegata al documento originale. Il destinatario riceverà il documento con la "firma digitale" e il certificato rilasciato dalla competente autorità di certificazione (CA) a garanzia della titolarità della chiave pubblica necessaria per decriptare la firma digitale.

Attività del mittente:

Chi riceve il messaggio procederà all'apertura e alla verifica dello stesso mediante il proprio software per l'attività di firma. Si 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. Poi 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 della provenienza del documento.

Attività del destinatario:



ASPETTO NORMATIVO

La legislazione ed in particolare nell'art. 15 comma 2 della Legge 15 marzo 1997 n. 59 definisce: "Gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonchè la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge".

E' da notare come la normativa riguardi sia gli atti e i documenti informatici della pubblica amministrazione che del settore privato e che sia volta a riconoscere come giuridicamente validi tali documenti.

Nel D.P.R. 10 novembre 1997, n. 513 sono contenute normative per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici.

Nell'art. 1 di tale D.P.R. si definisce: "per firma digitale, il risultato della procedura informatica (validazione) basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al sottoscrittore tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici;"

Nell'art. 8 di tale D.P.R. si indica che chiunque intenda utilizzare un sistema a chiavi asimmetriche (valido agli effetti di legge) deve disporre di una idonea coppia di chiavi e rendere pubblica una di esse mediante la procedura di certificazione. Le attività di certificazione sono effettuate da certificatori inclusi, in apposito elenco pubblico, consultabile in via telematica, predisposto tenuto e aggiornato a cura dell'Autorità per l'Informatica nella Pubblica Amministrazione (AIPA).

Nell'art. 17 e nell'art. 62 delle Regole Tecniche (DPCM 8 febbraio 1999), le pubbliche amministrazioni possono provvedere autonomamente alla certificazione di chiavi pubbliche per i propri organi e uffici nell'ambito dell'attività amministrativa di competenza; nella circolare A.I.P.A/CR/27 del febbraio 2001 viene indicato che:

"Le pubbliche amministrazioni che intendono svolgere l'attività di certificazione … devono inoltrare all'Autorità per l'informatica nella pubblica amministrazione, domanda di iscrizione nell'elenco pubblico" dei certificatori.

Il certificatore è tenuto ad identificare in maniera certa la persona che richiede la certificazione. Deve informare i richiedenti il certificato, della prassi di certificazione e dei requisiti tecnici per accedervi. Non deve essere depositario di alcuna chiave privata. Deve procedere alla revoca o alla sospensione del certificato in caso di richiesta da parte del titolare o del terzo dal quale derivino i poteri di quest'ultimo, di perdita del possesso della chiave, di provvedimento dell'autorità, di acquisizione della conoscenza di cause limitative della capacità del titolare, di sospetti abusi o falsificazioni; e deve provvedere alla pubblicazione della revoca o della sospensione della coppia di chiavi asimmetriche.

L'utilizzo della firma digitale quindi necessita di un apposito certificato digitale rilasciato dalla CA. La CA compie una serie di atti (identificazione dell'utente, rilascio del certificato e sua pubblicazione unitamente alla chiave pubblica, gestione delle procedure di revoca e sospensione) che assolvono ad una vera e propria funzione pubblicitaria nei confronti dei terzi, idonea ad ingenerare in essi un legittimo affidamento.

I certificati devono avere un formato conforme allo standard internazionale ITU (International Telecommunication Union) **X.509:** standard che definisce il formato dei certificati digitali utilizzato per la gestione delle chiavi pubbliche degli utenti. Esso è composto da una serie di informazioni organizzate in campi che specificano: numero del certificato, il certificatore emittente, il nome dell'utente certificato, la sua chiave pubblica, il periodo di validità del certificato e altre informazioni per indicare l'uso per il quale il certificato è stato rilasciato.

La cosa fondamentale è che rappresenta il legame tra una persona e la sua chiave pubblica, questa relazione è appunto garantita da un certificatore al di sopra delle parti. Così il destinatario del messaggio potrà verificare sul certificato la firma digitale dell'organo di certificazione con la chiave pubblica di quest'ultimo e potrà essere assolutamente sicuro dell'identità del mittente e della sua intenzionalità nell'invio del messaggio (viene così soddisfatto il requisito della "non ripudiabilità" del messaggio in quanto non è possibile che il mittente possa successivamente rinnegarne la paternità).

Nel nostro paese i certificati debbono contenere almeno le seguenti informazioni (secondo quanto indicato nel DPCM 8 febbraio 1999):

- numero di serie del certificato;
- ragione o denominazione sociale del certificatore;

- codice identificativo del titolare presso il certificatore;
- nome cognome e data di nascita ovvero ragione o denominazione sociale del titolare;
- valore della chiave pubblica;
- algoritmi di generazione e verifica utilizzabili;
- inizio e fine del periodo di validità delle chiavi;
- algoritmo di sottoscrizione del certificato.

Per richiedere un certificato il soggetto, del quale la CA ha verificato l'identità certa, invia la propria chiave pubblica al certificatore. Il certificatore produce il certificato digitale, lo firma digitalmente e lo recapita telematicamente al titolare con l'apposizione della relativa marca temporale che garantisce la certezza della data e dell'ora di emissione e pubblicazione nel registro pubblico.

Il certificatore stabilisce la scadenza del certificato e la durata di validità delle chiavi a seconda dell'algoritmo utilizzato, della lunghezza delle chiavi e della motivazione del rilascio. Di solito la validità di un certificato non è superiore ai 3 anni.

Un soggetto A crea la sua coppia di chiavi, dopodiché presenta la chiave pubblica a un'autorità di certificazione, la quale verificherà l'identità di A e prenderà ogni altro provvedimento volto ad assicurarsi che A è realmente chi sostiene di essere. A questo punto la CA consegna un certificato che attesta la connessione tra A e la sua chiave pubblica. Quando B riceverà il messaggio, potrà consultare un registro telematico per ottenere il certificato di A, recuperare la chiave pubblica di quest'ultimo, decifrare il messaggio stesso con la sicurezza che a quella chiave corrisponde la persona, fisica o giuridica, di A.

Il titolare della chiave privata deve conservare la/e chiave/i privata/e all'interno di un apposito dispositivo di firma, non deve duplicare né il dispositivo né le firme e in caso di perdita o difettosità delle chiavi contenute nei dispositivi di firma deve chiedere immediatamente la revoca delle certificazioni.

Nel Decreto del Presidente del Consiglio dei Ministri 8 febbraio 1999 sono contenute le regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione dei documenti informatici. In particolare si indica:

“Per la generazione e la verifica delle firme digitali possono essere utilizzati i seguenti algoritmi:

RSA (Rivest-Shamir-Adleman algorithm) / DSA (Digital Signature Algorithm).

La generazione dell'impronta si effettua impiegando una delle seguenti funzioni di hash, definite nella norma ISO/IEC 10118-3:1998:

- Dedicated Hash-Function 1, corrispondente alla funzione RIPEMD-160;
- Dedicated Hash-Function 3, corrispondente alla funzione SHA-1.

La lunghezza minima delle chiavi è stabilita in 1024 bit.”

Per ciascuna chiave di certificazione il certificatore deve generare un certificato sottoscritto con la chiave privata della coppia cui il certificato si riferisce. Prima di emettere il certificato deve accertarsi dell'autenticità della richiesta, verificare che la chiave pubblica di cui si richiede la certificazione non sia già stata certificata da un altro certificatore. Deve poi chiedere la prova del possesso della chiave privata e verificare il corretto funzionamento della coppia di chiavi.

Il certificatore deve rendere pubblico il registro dei certificati rilasciati. In questo elenco debbono essere presenti: i certificati da lui emessi, le liste dei certificati revocati e sospesi. Il certificatore può replicare il registro dei certificati su più siti, purché sia garantita la consistenza e l'integrità delle copie.

La revoca di un certificato determina la cessazione anticipata della sua validità e può avvenire su diretta richiesta del titolare, su iniziativa del certificatore o di un terzo interessato. La revoca viene effettuata dal certificatore mediante il suo inserimento in una delle liste di certificati revocati (CRL) da lui gestite ed è efficace a partire dal momento della pubblicazione della lista che lo contiene e ha carattere definitivo.

A livello europeo l’ultima direttiva sull’argomento è la Direttiva 1999/93/CE che si propone di sviluppare il commercio elettronico predisponendo un ambito legale uniforme su tutto il territorio dell'Unione al fine di incentivare i rapporti commerciali per via telematica. In tale ottica la direttiva europea è meno rigida della normativa italiana nell'intento di diffondere, fra i cittadini degli stati membri, l'uso della firma digitale attraverso il suo riconoscimento legale.

Ciascun paese membro non può limitare la prestazione di servizi di certificazione originati in un altro Stato membro.

In attuazione della direttiva 1999/93/CE, relativa ad un quadro comunitario per le firme elettroniche, sono state individuate, con il decreto legislativo 23 gennaio 2002, n. 10, diverse modalità di sottoscrizione elettronica dei documenti informatici, che si distinguono in base al loro livello di affidabilità e sicurezza. Il sistema più sicuro resta quello della sottoscrizione del documento informatico con firma digitale o con un altro tipo di firma elettronica avanzata, che fa piena prova della provenienza del documento. Il documento sottoscritto con firma elettronica è, invece, valutabile, in base alle sue caratteristiche di qualità e sicurezza, mentre il semplice documento informatico è valido solo se non ne viene disconosciuta la sua conformità.

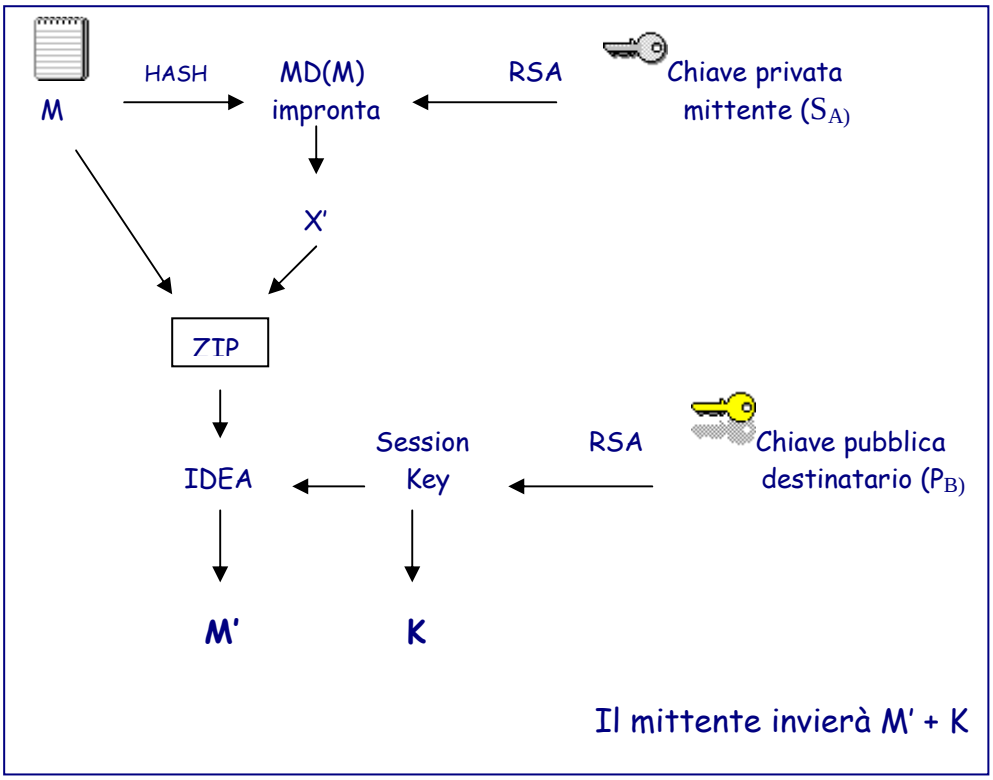
PGP (Pretty Good Privacy)

È un software di crittografia distribuito gratuitamente su Internet, nasce nel 1991 ad opera di Philiph Zimmermann. E' attualmente il più usato come mezzo di autenticazione per comunicazioni tramite posta elettronica su Internet. Con questo programma si può cifrare l'intero messaggio, ma anche allegare ad un messaggio in chiaro una firma digitale ricavata dalla propria chiave privata, attraverso la quale chi riceve il messaggio può verificare l'autenticità o meno dello stesso. Le chiavi pubbliche PGP sono reperibili presso Public Key Server, ossia server addetti alla memorizzazione e alla distribuzione delle chiavi pubbliche. Ogni volta che un utente installa per la prima volta il programma, deve provvedere a generare le proprie chiavi (quella pubblica e quella privata) e spedire quella pubblica al server (attività non obbligatoria ma utile affinché la sua chiave pubblica sia conosciuta a chiunque voglia comunicare con lui). Per garantire che la chiave pubblica sia effettivamente quella del proprietario il PGP utilizza il metodo delle certificazioni cioè delle firme sulla chiave stessa di altri utenti di PGP che si impegnano a garantire che quella chiave appartiene a chi dice di appartenere. La filosofia del PGP è quella della "Web of trust" per la quale ogni parte può certificare l'identità dell'altra.

Il PGP si basa sia su algoritmi simmetrici che asimmetrici. Utilizzandoli insieme, il problema della distribuzione delle chiavi e la velocità di elaborazione migliorano, senza perdere in sicurezza.

Attività del mittente:

- Calcola il message digest sul messaggio in chiaro
- Firma il message digest utilizzando la sua chiave privata
- Il messaggio in chiaro e la firma del message digest vengono compressi (zippati)
- Viene generata una session-key (il PGP genera un numero casuale)
- La session-key generata è utilizzata per cifrare il messaggio compresso.
- La session-key viene cifrata con la chiave pubblica del destinatario.
- Il pacchetto costituito da session-key cifrata e messaggio cifrato vengono inviati.



Il PGP del destinatario spezza il pacchetto ricevuto (M' da K), decifra la session key con la propria chiave privata e potrà poi risalire al messaggio in chiaro (utilizzando la chiave pubblica del mittente).

Di questo applicativo esistono varie successive versioni. Le modifiche sono state implementate per l'utilizzo di algoritmo più sicuri, di chiavi più lunghe, di metodi di generazione di session key più sicuri e veloci. Lo scopo comunque resta quello di continuare a garantire diffusione, velocità, riservatezza e integrazione con altri software.