WIKIPEDIA

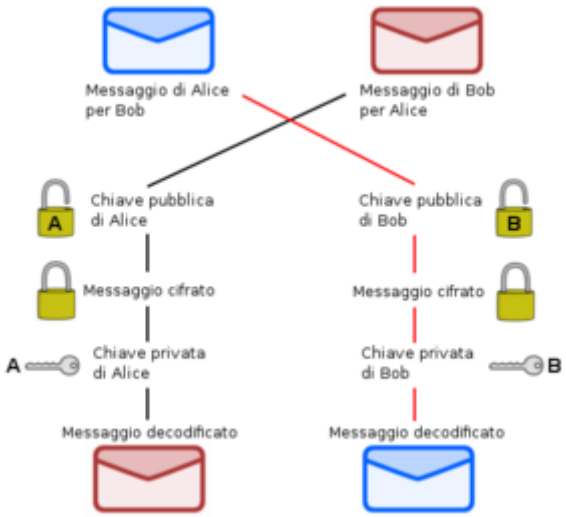
Crittografia asimmetrica

Da Wikipedia, l'enciclopedia libera.

La **crittografia asimmetrica**, conosciuta anche come **crittografia a coppia di chiavi**, **crittografia a chiave pubblica/privata** o anche solo **crittografia a chiave pubblica**, è un tipo di crittografia dove, come si deduce dal nome, ad ogni attore coinvolto nella comunicazione è associata una coppia di chiavi:

- La chiave pubblica, che deve essere distribuita;
- La chiave privata, appunto personale e segreta

evitando così qualunque problema connesso alla necessità di uno scambio in modo sicuro dell'unica chiave utile alla cifratura/decifratura presente invece nella crittografia simmetrica. Il meccanismo si basa sul fatto che, se con una delle due chiavi si cifra (o codifica) un messaggio, allora quest'ultimo sarà decifrato solo con l'altra.



Esempio di corrispondenza elettronica utilizzando un sistema di crittografia asimmetrica

Indice

Generalità

Ci sono due funzioni che possono essere realizzate: cifrare messaggi con la chiave pubblica per garantire che solo il titolare della chiave privata possa decifrarlo oppure usare la chiave pubblica per autenticare un messaggio inviato dal titolare con la chiave privata abbinata.

In un sistema di crittografia a chiave pubblica, chiunque può cifrare un messaggio usando la chiave pubblica del destinatario, ma tale messaggio può essere decifrato solo con la chiave privata del destinatario. Per fare ciò, deve essere computazionalmente facile per un utente generare una coppia di chiavi pubblica e privata da utilizzare per cifrare e decifrare. La forza di un sistema di crittografia a chiave pubblica si basa sulla difficoltà di determinare la chiave privata corrispondente alla chiave pubblica.

La sicurezza dipende quindi solo dal mantenere la chiave privata segreta, mentre la chiave pubblica può essere pubblicata senza compromettere la sicurezza.

I sistemi di crittografia a chiave pubblica spesso si basano su algoritmi di crittografia basati su problemi matematici che attualmente non ammettono alcuna soluzione particolarmente efficiente, quelli che riguardano la fattorizzazione di un numero intero, il logaritmo discreto e le relazioni delle curve ellittiche. Gli algoritmi a chiave pubblica, a differenza degli algoritmi a chiave simmetrica, non richiedono un canale sicuro per lo scambio iniziale di una (o più) chiavi segrete tra le parti.

A causa del peso computazionale della crittografia asimmetrica, essa di solito è usata solo per piccoli blocchi di dati, in genere il trasferimento di una chiave di cifratura simmetrica (per esempio una chiave di sessione). Questa chiave simmetrica è utilizzata per cifrare messaggi lunghi. La cifratura/decifratura simmetrica è basata su algoritmi semplici ed è molto più veloce. L'autenticazione del messaggio include hashing del messaggio per produrre un "digest" (risultato dell'output dell'algoritmo di hash), e crittografando il digest con la chiave privata per produrre una firma digitale. Da lì in poi chiunque può verificare questa firma:

1. calcolando l'hash del messaggio;
2. decifrando l'hash del messaggio;
3. confrontando la firma del messaggio.

L'uguaglianza tra i digests conferma che il messaggio non è stato modificato da quando è stato firmato, e che il firmatario, e nessun altro, intenzionalmente abbia eseguito l'operazione di firma, presumendo che la chiave privata del firmatario sia rimasta segreta. La sicurezza di questo tipo di procedura dipende dall'algoritmo di hash di questa data qualità che è computazionalmente impossibile modificare o trovare un messaggio sostituito che produca lo stesso digest, ma gli studi hanno dimostrato che con gli algoritmi MD5 e SHA-1, produrre un messaggio alterato o sostituito non è impossibile. L'attuale standard di hash per la crittografia è SHA-2. Lo stesso messaggio può essere usato al posto del digest.

Gli algoritmi a chiave pubblica sono ingredienti fondamentali della sicurezza dei crittosistemi, applicazioni e protocolli. Essi sono alla base dei diversi standard Internet, come ad esempio Transport Layer Security (TLS), S/MIME, PGP e GPG. Alcuni algoritmi a chiave pubblica forniscono una distribuzione di chiave e segretezza (ad esempio, scambio di chiavi Diffie-Hellman), alcuni di fornire firme digitali (ad esempio Digital Signature Algorithm), altri forniscono entrambe (esempio RSA).

La crittografia a chiave pubblica trova applicazione in vari campi, tra gli altri: nella disciplina di sicurezza informatica e nella sicurezza delle informazioni. La sicurezza delle informazioni si occupa di tutti gli aspetti per la protezione delle risorse informative elettroniche contro le minacce sulla sicurezza. La crittografia a

chiave pubblica viene utilizzata come metodo per assicurare la riservatezza, l'autenticazione e il non ripudio delle comunicazioni e per la memorizzazione dei dati.

Storia

Agli inizi della storia della crittografia, le due parti dovevano contare su una chiave che doveva essere scambiata per mezzo di un metodo sicuro, come un incontro faccia a faccia o per mezzo di un corriere di fiducia. Questa chiave, che entrambe le parti tenevano assolutamente segreta, poteva quindi essere utilizzata per lo scambio di messaggi cifrati. Questo tipo di approccio alla distribuzione delle chiavi comporta un certo numero di difficoltà significative. Nel 1874 William Stanley Jevons scriveva nel suo libro *I Principi della scienza*:

> "Può il lettore dire quali sono i due numeri moltiplicati tra loro che produrranno il numero 8616460799? Penso che sia improbabile che qualcuno ci riesca, a parte me stesso." - William Stanley Jevons[1]

In questo libro descriveva il rapporto tra le funzioni unidirezionali e la crittografia e continuava a discutere, in particolare, del problema della fattorizzazione utilizzato per creare una funzione botola. Nel luglio 1996, il matematico Solomon W. Golomb ha detto:

> "Jevons ha anticipato una caratteristica fondamentale dell'algoritmo RSA per la crittografia a chiave pubblica, anche se di certo non ha inventato il concetto di crittografia a chiave pubblica."[2] (nel 1869, Jevons ha inventato un calcolatore chiamato "Logica Piano").

Scoperta riservata

Nel 1970, James H. Ellis, crittografo inglese presso il Government Communications Headquarters (GCHQ), immaginò la possibilità di una "crittografia non segreta", (adesso chiamata crittografia a chiave pubblica), ma non riusciva a vedere alcun modo di implementarla.[3] Nel 1973, il suo collega Clifford Cocks realizzò quello che è diventato noto come algoritmo di crittografia RSA, dando un metodo pratico di "cifratura non segreta", e nel 1974, un altro matematico e crittografo, che faceva parte del GCHQ, Malcolm J. Williamson, sviluppò ciò che è oggi è conosciuto come scambio di chiavi Diffie-Hellman. Il progetto fu passato anche al NSA.[4] In un'ottica militare e con bassa potenza di calcolo disponibile, le potenzialità della crittografia a chiave pubblica non furono capite dalle due organizzazioni:

> Pensavo che fosse più importante per uso militare... se è possibile condividere la chiave rapidamente per via elettronica, si ha un grande vantaggio rispetto all'avversario. Solo alla fine dell'evoluzione di Berners-Lee la progettazione di un'architettura Internet aperta per il CERN, il suo adattamento e adozione per Arpanet... consentì alla crittografia a chiave pubblica di esprimere il suo massimo potenziale. Ralph Benjamin[5]

La loro scoperta non fu resa di dominio pubblico per 27 anni, fino a quando la ricerca è stata riclassificata dal governo britannico nel 1997.

Scoperta resa pubblica

Nel 1976 Whitfield Diffie e Martin Hellman pubblicarono un sistema di crittografia a chiave asimmetrica, influenzato dal lavoro di Ralph Merkle sulla distribuzione della chiave pubblica. Questo metodo di scambio di chiavi, che utilizza un'elevata potenza in un campo infinito, divenne nota come scambio di chiavi Diffie-Hellman. Questo era il metodo pratico pubblicato per stabilire una chiave segreta condivisa su un canale

autenticando (ma non confidenziale) le comunicazioni senza l'utilizzo di una chiave segreta precedentemente condivisa. La "tecnica a chiave pubblica accordata" di Merkle fu conosciuta come *algoritmo del puzzle*, fu inventata nel 1974 e pubblicata nel 1978.

Nel 1977, la generalizzazione del sistema di Cocks è stato indipendentemente inventato da Ron Rivest, Adi Shamir e Leonard Adleman, altri del MIT. Questi ultimi autori hanno pubblicato il loro lavoro nel 1978 e l'algoritmo è venuto ad essere conosciuto con il nome RSA, dalle loro iniziali. RSA utilizza l'elevamento a potenza in modulo di due numeri primi molto grandi moltiplicati, per la crittografia e decrittografia, eseguendo sia la crittografia a chiave pubblica e la firma digitale a chiave pubblica. La sua sicurezza è collegata alla estrema difficoltà di fattorizzare grandi numeri, un problema per cui non è nota una tecnica generale efficiente. Nel 1979, Michael Rabin pubblicò un crittosistema correlato che probabilmente è protetto finché la fattorizzazione della chiave pubblica resta difficile, resta un presupposto che RSA gode anche questa sicurezza.

Dal 1970, un gran numero di tecniche di crittografia, firma digitale, accordo della chiave e altre sono state sviluppate nel campo della crittografia a chiave pubblica. Il sistema di crittografia ELGamal, inventato da Taher ElGamal si basa sul simile e relativo alto livello di difficoltà del problema logaritmo discreto, così come lo strettamente correlato DSA, che è stato sviluppato presso l'US National Security Agency (NSA) e pubblicato dal NIST come Standard proposto.

L'introduzione della crittografia a curva ellittica da parte di Neal Koblitz e Victor Miller, indipendentemente e contemporaneamente a metà degli anni 80, ha dato nuovi algoritmi a chiave pubblica basati sul problema del logaritmo discreto. Anche se matematicamente è più complessa, le curve ellittiche forniscono chiavi più piccole e più veloci, e la sicurezza risulta essere approssimativamente equivalente.

Descrizione

L'idea base della crittografia con coppia di chiavi diviene più chiara se si usa un'analogia postale, in cui il mittente è Alice ed il destinatario Bob, i lucchetti fanno le veci delle chiavi pubbliche e le chiavi recitano la parte delle chiavi private:

1. Alice chiede a Bob di spedirle il lucchetto già aperto. La chiave dello stesso verrà però gelosamente conservata da Bob;
2. Alice riceve il lucchetto di Bob e, con esso, chiude il pacco e lo spedisce a Bob;
3. Bob riceve il pacco e può aprirlo con la chiave di cui è l'unico proprietario.

Se adesso Bob volesse mandare un altro pacco ad Alice, dovrebbe farlo chiudendolo con il lucchetto di Alice (che lei dovrebbe aver preventivamente dato a Bob) che solo lei potrebbe aprire.

Si può notare come per mettere in sicurezza il contenuto dei pacchi ci sia bisogno del lucchetto del destinatario, mentre per aprirli viene usata esclusivamente la propria chiave segreta, rendendo l'intero processo di cifratura/decifratura asimmetrico (una chiave per cifrare ed una differente per decifrare). Chiunque intercettasse il lucchetto (aperto) o il messaggio chiuso con il lucchetto non potrebbe leggerne il contenuto poiché non ha la chiave. Uno dei vantaggi della crittografia asimmetrica sta nel fatto che le chiavi pubbliche possono essere scambiate anche utilizzando un mezzo insicuro, come Internet.

Usando un'altra analogia si può dire che il metodo è analogo a quello di una cassaforte che abbia due chiavi distinte, una usata per aprirla (chiave segreta), l'altra per chiuderla (chiave pubblica).

Nella crittografia simmetrica invece, che basa la sicurezza del sistema sulla segretezza della chiave di codifica/decodifica utilizzata, si rende necessario utilizzare un canale sicuro per la trasmissione della chiave, poiché l'intercettazione della stessa, da parte di terzi, vanificherebbe la sicurezza del sistema stesso.

Due degli usi più conosciuti della crittografia asimmetrica sono:

- crittografia a chiave pubblica, nel quale i messaggi sono crittografati con la chiave pubblica del destinatario. Il messaggio non può essere decriptato da chi non possiede la chiave privata corrispondente, che viene così presupposto di essere il proprietario di quella chiave e la persona associata con la chiave pubblica. Questo è utilizzato nel tentativo di garantire la riservatezza;
- firma digitale, in cui un messaggio viene firmato con la chiave privata del mittente e può essere verificato da chiunque abbia accesso alla chiave pubblica del mittente. Questa verifica dimostra che il mittente ha avuto accesso alla chiave privata ed è pertanto probabile che sia la persona associata alla chiave pubblica. Questo assicura anche che il messaggio non è stato manomesso, ogni manipolazione del messaggio comporterà modifiche al digest, che altrimenti rimarrebbe invariato tra il mittente e ricevente.

Differenze con la crittografia tradizionale (simmetrica)

Nella tradizionale crittografia simmetrica, viene utilizzata un'unica chiave sia per codificare, sia per decodificare i messaggi. Delle due informazioni (la chiave e l'algoritmo) necessarie a chi deve inviare il messaggio, la chiave è quindi identica a quella necessaria a chi deve riceverla, mentre l'algoritmo è facilmente reversibile in quello di decifrazione. Per concordare una chiave con il proprio interlocutore, c'è bisogno di mettersi preventivamente in contatto con lui incontrandolo di persona, telefonandogli, scrivendogli una lettera, mandandogli un messaggio o in qualsiasi altro modo. In qualunque caso, esiste il pericolo che la chiave venga intercettata durante il tragitto, compromettendo quindi l'intero sistema comunicativo.

La crittografia a chiave pubblica permette invece a due (o più) persone di comunicare in tutta riservatezza senza usare la stessa chiave, anche se queste non si sono mai incontrate precedentemente.

Breve panoramica sull'implementazione

Il principio generale della crittografia asimmetrica ha una solida base matematica che lo giustifica; tale base, riassunta e semplificata all'estremo, si fonda sull'uso di un problema complesso, ovvero un'operazione matematica semplice da eseguire, ma difficile da invertire, cioè dal cui risultato è difficile risalire agli argomenti di partenza. L'esempio classico è il problema della fattorizzazione di un numero (trovare i numeri primi che lo producono se moltiplicati tra loro: ad esempio, è facile moltiplicare 17×23 ottenendo 391, ben più difficile è per esempio fattorizzare il numero 377 nei fattori primi 13 e 29) usata nel primo e più famoso sistema crittografico a chiave pubblica: **RSA**. Le conoscenze di matematica pura sviluppate dall'uomo negli ultimi secoli hanno reso sempre più efficiente fattorizzare, ma nessuno è mai riuscito a far fare quel passo che porta il problema da complesso a non complesso; il problema diventa quindi intrattabile per numeri oltre una certa dimensione.

Attualmente, per la crittografia RSA vengono considerati "sicuri" numeri che in base 10 hanno almeno 600 cifre, il che significa chiavi di 2048 bit e oltre.

Altro esempio di problema complesso è il logaritmo discreto, usato nella nascente crittografia ellittica.

La crittografia è comunque una scienza basata sulle probabilità: i problemi complessi vengono considerati complessi basandosi sul fatto che centinaia di anni di studio non hanno saputo risolverli in modo rapido (ricordiamoci che c'è sempre almeno un modo non immediato per risolvere un problema: provare a fare l'operazione diretta con tutti i numeri fino alla dimensione necessaria; questo tipo di soluzione, in genere, non è neanche contemplata, in quanto il tempo necessario aumenta vertiginosamente con la dimensione dei

numeri usati), ma nessuno dei problemi usati in crittografia ha un teorema che ne dimostra la complessità (l'unico sistema crittografico dimostrato è lo One Time Pad, ma sfortunatamente è un sistema simmetrico – ovvero non a chiave pubblica – ed estremamente scomodo da usare).

Utilizzo della crittografia asimmetrica

Con l'istruzione HTTP Strict Transport Security il server invia i messaggi di risposta alle richieste di connessione HTTP con una intestazione che impone per un certo tempo a qualsiasi user agent (*browser* e qualsiasi altro tipo di client) di connettersi in maniera cifrata con HTTPS, e non col semplice HTTP.

Per utilizzare questo tipo di crittografia, è necessario creare una coppia di chiavi. Quando vengono generate le due chiavi sono equivalenti (una delle due indifferentemente può essere resa pubblica). La proprietà fondamentale delle due chiavi è che un messaggio cifrato usando una delle due chiavi può essere decifrato soltanto usando l'altra chiave e viceversa. Ciò significa sostanzialmente che le due chiavi funzionano "insieme" pur non essendo possibile dall'una desumere l'altra.

Quando una delle due chiavi viene resa pubblica e l'altra privata, è possibile utilizzarle insieme fondamentalmente per due scopi:

1. Inviare un messaggio cifrato ad un destinatario. Per fare ciò il mittente cifra il messaggio con la chiave pubblica del destinatario. Per la proprietà delle due chiavi, l'unico a poter decifrare il messaggio è il destinatario, possessore della chiave privata.
2. Verificare l'autenticità di un messaggio. In questo caso il possessore della chiave privata cifra il messaggio con la sua chiave privata. Il destinatario verifica l'autenticità del messaggio decifrando con la chiave pubblica del mittente. Si noti che in questo caso tutti i possessori della chiave pubblica del mittente potranno leggere il messaggio, verificandone l'autenticità.

Affinché tutto funzioni, ovviamente, è necessario che il possessore della chiave privata custodisca gelosamente tale chiave e la faccia rimanere tale.

La coppia di chiavi pubblica/privata viene generata attraverso un algoritmo (ad esempio RSA o DSA) a partire da dei numeri casuali. Gli algoritmi asimmetrici sono studiati in modo tale che la conoscenza della chiave pubblica e dell'algoritmo stesso non siano sufficienti per risalire alla chiave privata e tale meccanismo è reso possibile grazie all'uso di funzioni unidirezionali. In realtà, in molti casi, l'impossibilità di risalire alla chiave privata non è dimostrata matematicamente, ma risulta dallo stato attuale delle conoscenze in matematica e della potenza di calcolo disponibile. Per esempio, è sufficiente un piccolo computer e qualche millesimo di secondo per moltiplicare due numeri primi da 150 cifre, ma occorre il lavoro di decine di migliaia di computer per un anno per trovare i fattori primi di quel numero. Un altro problema simile è quello della funzione unidirezionale esponenziale modulo n (aritmetica modulare) e del rispettivo problema inverso del calcolo del suo logaritmo discreto.

A questo punto, il gioco è fatto: ogni utilizzatore si crea la propria (o le proprie, in casi particolari) coppia di chiavi; la chiave privata viene tenuta segreta e non viene mai rivelata a nessuno (nemmeno alle persone con le quali si comunica); viceversa, la chiave pubblica viene diffusa in vari modi: può essere aggiunta automaticamente in coda a ciascun proprio messaggio nelle varie conferenze elettroniche cui si partecipa, o può essere depositata in archivi pubblici (keyserver) a disposizione di chi la desideri. È importante che la chiave pubblica sia liberamente accessibile, perché chiunque voglia comunicare con la persona che l'ha generata dovrà preventivamente munirsi di questa, con la quale cifrerà il messaggio.

Negoziazione iniziale delle chiavi

Lo scambio delle chiavi asimmetriche avviene in una fase iniziale di negoziazione in cui gli utenti adottano temporaneamente una chiave di sessione simmetrica di supporto alla fase di *handshake* ovvero di avvio di una sessione con crittografia simmetrica per negoziare la chiave di sessione, il protocollo e gli altri aspetti della connessione cifrata.

La chiave di sessione è temporanea e "usa e getta": non appena è definito tutto ciò che riguarda la connessione cifrata, inizia lo scambio con crittografia a chiave asimmetrica, e la chiave di sessione non è più utilizzata: se la chiave privata di un utente viene compromessa o perde la sua segretezza, è possibile derivare la chiave di sessione e tramite questa la chiave privata scambiata dall'altro utente, e decifrare l'intera comunicazione. Per evitare questo rischio, la Forward secrecy, genera la chiave di sessione a partire da una chiave a lungo termine, diversa da quella pubblica e privata degli utenti.

Firma digitale

Oltre alla cifratura dei dati di una comunicazione, la crittografia asimmetrica presenta altri possibili impieghi: firma digitale per verificare l'autenticazione del mittente e l'integrità informativa del messaggio, fornire una condizione di *ending* e per i programmi che tentano la forzatura delle chiavi. Un utente può firmare un messaggio utilizzando la propria chiave privata; per far ciò, viene creata un'impronta (*digest*) del messaggio da firmare e questa, criptata con la chiave privata, rappresenta la firma ed è inviata assieme al messaggio (l'impronta, generata per mezzo di un algoritmo di Hash, è tale che varia sensibilmente al minimo variare del messaggio). Tutti i destinatari del messaggio possono verificare l'integrità del messaggio stesso e l'autenticazione dell'autore/mittente creando, a partire dal messaggio ricevuto, un'impronta (o *digest*, utilizzando in maniera simmetrica la stessa funzione hash utilizzata dall'autore del messaggio) e confrontandola poi con quella ricevuta assieme al messaggio e decifrata con la chiave pubblica del presunto autore: se le due impronte risultano identiche il messaggio è integro, ovvero non ha subito modifiche da parte di terzi (ad esempio attraverso attacchi del tipo *man in the middle*) da quando l'autore a monte l'ha firmato.

Il mittente "attacca" l'hash in fondo al messaggio. Può allora scegliere se codificare (firmare) con la propria chiave privata tutto l'insieme (messaggio e hash), oppure lasciare il messaggio in chiaro e cifrare con la chiave privata solo l'hash. In entrambi i modi, chiunque decodifichi con la chiave pubblica del mittente è certo che sono autenticati il mittente e il contenuto del messaggio (volendo si può aggiungere anche una marca temporale che certifica anche il momento di invio e di ricezione).

La firma digitale fornisce anche una condizione di termine per i programmi che tentano di forzare la cifratura. Tali programmi tentano di ricostruire la chiave privata del destinatario per leggere il messaggio. Il programma ha come riferimento la firma digitale del messaggio, o meglio la decifra con la chiave pubblica del mittente e utilizza l'hash. Il programma propone *n* chiavi private, per ognuna decifra il messaggio, ne calcola l'hash e lo confronta con quello ricavato dalla firma digitale: se coincidono, è stata trovata la chiave privata giusta ed è visibile il contenuto del messaggio originale.

Sicurezza

La sicurezza di alcuni sistemi di crittografia può essere verificata sulla base della difficoltà computazionale presunta di un problema matematico, come ad esempio la fattorizzazione di un numero intero e il calcolo di logaritmi discreti. Si noti che "sicuro" qui ha un significato matematico preciso, e ci sono diverse definizioni di ciò che significa per uno schema di crittografia essere "sicuro".

Un messaggio che un mittente cripta con la chiave pubblica del destinatario può essere decifrato solo con la chiave privata accoppiata, che in questo caso è la chiave privata del destinatario. Ciò è utile nella pratica solo se non è stato scoperto nessun difetto nell'algoritmo utilizzato.

Un'applicazione della crittografia a chiave pubblica è la firma digitale. I sistemi a firma digitale possono essere utilizzati per l'autenticazione del mittente e per il non ripudio. Il mittente calcola la firma digitale per il messaggio che deve inviare e invia la firma (contemporaneamente al messaggio) al destinatario previsto. Le politiche della firma digitale sono tali che le firme possono essere calcolate solo con la conoscenza della chiave privata corretta. Per verificare che un messaggio è stato firmato da un utente e non è stato modificato, il ricevente deve solo conoscere la corrispondente chiave pubblica. In altri casi (ad esempio RSA), un singolo algoritmo può essere utilizzato per crittografare e creare firme digitali. In altri casi (ad esempio DSA), ogni algoritmo può essere utilizzato solo per uno scopo specifico.

Per raggiungere l'autenticazione e la riservatezza, il mittente deve includere il nome del destinatario del messaggio, usando la chiave privata, e quindi criptare sia il messaggio che la firma utilizzando la chiave pubblica del destinatario.

Queste caratteristiche possono essere usate per costruire molti protocolli e applicazioni crittografiche, come ad esempio: pagamenti online, protocolli non-ripudio, ecc.

Problematiche

In realtà, il problema della sicurezza riguardante la segretezza della comunicazione non è del tutto risolto con questo tipo di crittografia, in quanto passibile di attacchi di tipo man in the middle: non si può essere certi infatti che la chiave (per esempio una chiave presente sul keyserver) appartenga davvero alla persona nominata nell'intestazione della chiave stessa, apportando così attacchi di tipo spoofing in assenza di un meccanismo di autenticazione tra le parti in causa. Una soluzione resta sempre il contatto fisico tra i due interlocutori, i quali, scambiandosi le chiavi pubbliche hanno una reciproca autenticazione.

PGP, il primo sistema crittografico di massa che si avvale delle idee della crittografia asimmetrica consiglia, dopo essersi scambiati le chiavi per e-mail o altro mezzo, di telefonarsi e di leggersi i fingerprint (letteralmente "impronte digitali"), ovvero un codice (codice di hash) associabile in modo sicuro alla chiave stessa, ma da cui non si può ricavare la chiave; in questo modo, riconoscendo le rispettive voci, si certifica anche la validità della chiave ottenuta.

Un altro problema da non escludere è quello dell'effettiva protezione della chiave privata: questa, infatti, risiede nel disco rigido del proprietario ed è generalmente cifrata con una password (quindi con crittografia simmetrica). Data la relativa semplicità di accesso alla chiave (basta inserire una password per "sbloccarla"), con particolari trojan/keylogger programmati ad-hoc è quindi possibile ricavare dal PC della vittima sia il file contenente la chiave privata sia la password per utilizzarla, violando a tutti gli effetti l'efficienza della crittografia asimmetrica.

Esempi

Esempi di tecniche a chiave pubblica ben considerati sono:

- Diffie-Hellman
- DSS (Digital Signature Standard), che incorpora il Digital Signature Algorithm
- ElGamal
- Rabin
- Crittografia a curve ellittiche
- Password-authenticated key agreement
- Paillier cryptosystem
- RSA (PKCS)

- HFE (Equazioni a Campi Nascosti)

Esempi di algoritmi non sicuri:

- Merkle-Hellman l'algoritmo dello zaino
- Algoritmo del puzzle (solo istruttivo)
- Algoritmo Blum-Goldwasser

Esempi di protocolli che usano algoritmi di chiave asimmetrica:

- GPG (un'implementazione di OpenPGP)
- Internet key exchange (IKE)
- PGP
- SSH
- TLS (ex SSL)
- SILC

Note

1. **^** *Principles of Science*.
2. **^** Solomon W. Golomb, *Cryptologia*.
3. **^** *The unsung genius who secured Britain's computer defences and paved the way for safe online shopping*, su *telegraph.co.uk*. URL consultato il 1º luglio 2016 (archiviato dall'url originale il 23 marzo 2019).
4. **^** Tom Espiner, *GCHQ pioneers on birth of public key crypto | ZDNet*, su *ZDNet*. URL consultato il 1º luglio 2016.
5. **^** *GCHQ pioneers on birth of public key crypto*, su *zdnet.com*.

Voci correlate

- Crittografia funzionale
- Crittografia simmetrica
- Differenza tra cifratura simmetrica e asimmetrica
- Distribuzione a chiave quantistica
- Firma digitale
- Key signing party
- OpenPGP
- Public key infrastructure vs Web of trust
- S/MIME
- Trusted computing

Collegamenti esterni

-
- (**EN**) *Crittografia asimmetrica*, su *Enciclopedia Britannica*, Encyclopædia Britannica, Inc.
- (**EN**) *The GNU Privacy Guard*, su *gnupg.org*.
- (**EN**) *GPGTools*, su *gpgtools.org*.

- Cos'è la crittografia? (http://www.caressa.it/pdf/crypto.pdf) brevi note di Paolo Caressa (2005)
- *Crittografia asimmetrica...come, quando e perché*, su *firmadigitalefacile.it*.
- *Elenco mondiale dei database delle chiavi pubbliche per Pretty Good Privacy*, su *www-swiss.ai.mit.edu*. URL consultato il 17 gennaio 2016 (archiviato dall'url originale il 18 ottobre 2001).

Controllo di autorità	Thesaurus BNCF 60691 (https://thes.bncf.firenze.sbn.it/termine.php?id=60691) · LCCN (EN) sh00004804 (http://id.loc.gov/authorities/subjects/sh00004804) · GND (DE) 4209133-0 (https://d-nb.info/gnd/4209133-0) · BNF (FR) cb13554544f (https://catalogue.bnf.fr/ark:/12148/cb13554544f) (data) (https://data.bnf.fr/ark:/12148/cb13554544f) · NDL (EN, JA) 00966793 (https://id.ndl.go.jp/auth/ndlna/00966793)