Usi della crittografia: scambio di chiavi, firme digitali, certificati

Lezione 7 di Sicurezza dei sistemi informatici 1

Docente: Giuseppe Scollo

Università di Catania, sede di Comiso (RG)
Facoltà di Scienze Matematiche, Fisiche e Naturali
Corso di Studi in Informatica applicata, AA 2007-8

Indice

scambio di chiavi

come si è visto in una lezione precedente, crittografia simmetrica e asimmetrica possono assolvere funzioni **complementari** nella soluzione di problemi di sicurezza informatica, ecco un caso tipico:

la crittografia simmetrica è semplice e rapida, ma richiede la condivisione di una chiave segreta

la crittografia asimmetrica è lenta e complessa, ma non richiede una chiave condivisa

il **problema** della condivisione della chiave è **circolare:**

per la sicurezza della comunicazione occorre previamente stabilire una chiave segreta comune

per trasmettere la chiave in modo sicuro occorre già disporre di un canale di comunicazione sicuro, ovvero di una chiave segreta comune...

soluzione:

trasmettere con un sistema di crittografia asimmetrica
la chiave necessaria alla crittografia simmetrica

per proteggere la **riservatezza** della chiave trasmessa, e allo stesso tempo garantire l'**autenticità** del mittente, si adopera la doppia cifratura asimmetrica

il protocollo di Diffie-Hellmann

proposto nel classico articolo del 1976, il protocollo di Diffie-Hellmann permette di stabilire una chiave segreta condivisa fra due partner che non condividono alcun segreto

la soluzione al problema è analoga a quella del seguente **problema** (da manuale di spionaggio):

Alice vuole dare la sua bicicletta a Bob senza mai incontrarlo, ed impedirne il furto sebbene essi non dispongano di due copie della chiave di uno stesso lucchetto

... soluzione:

Alice porta la bici in un luogo convenuto e l'assicura con un suo lucchetto
quindi, Bob si reca nel luogo convenuto e ri-assicura la bici con un proprio lucchetto
Alice torna poi nel luogo convenuto e rimuove il primo lucchetto
infine Bob torna nel luogo convenuto, rimuove il secondo lucchetto e se ne va con la bici

il protocollo di Diffie-Hellmann presuppone che i partner A e B adoperino un opportuno grande numero primo p e un numero g di ordine (moltiplicativo) modulo p sufficientemente grande

N.B.: questa informazione, sebbene condivisa, non è segreta

A sceglie a caso il numero a e invia $y_a = g^a \bmod p$ a B

B sceglie a caso il numero b e invia $y_b = g^b \bmod p$ ad A

ora A e B dispongono di una comune chiave segreta: $y_a^b = y_b^a = g^{ab} \bmod p$

firme digitali

la simultanea garanzia di **riservatezza** e **autenticità** del mittente, fornita ad es. dalla doppia cifratura asimmetrica, trova applicazione anche nei sistemi di **firma elettronica**

altri requisiti di sicurezza essenziali per la firma elettronica:

- protezione dell'**integrità** del documento firmato e della firma
- **irripudiabilità** della firma da parte del suo autore
- **unicità** della coppia <documento firmato, firma>, ad es. per impedire la duplicazione dell'esecuzione di una transazione remota

la doppia cifratura asimmetrica supporta la soddisfazione dei requisiti di protezione dell'integrità e di irripudiabilità della firma, per la segretezza della chiave di autenticazione

per garantire la non duplicabilità dei documenti, i sistemi di apposizione di firma elettronica possono corredarli di informazione temporale (**timestamping**), o di altra informazione unica atta allo scopo

schemi di firma digitale

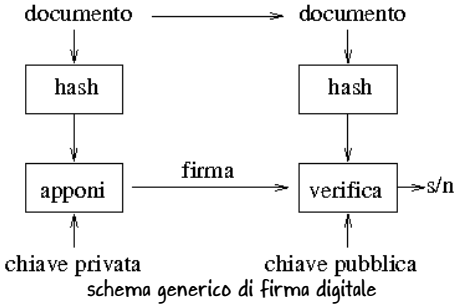
la cifratura asimmetrica semplice può bastare quando non occorre proteggere la riservatezza

- l'autore adopera in tal caso la chiave privata a garanzia di autenticità e integrità

queste proprietà sono peraltro garantite anche da hash con chiave segreta (MAC)

- cosa impedisce l'uso di MAC per la firma digitale?
- irripudiabilità e autenticità della firma → l'autore detiene il **segreto esclusivo** della chiave
- autenticità della firma **verificabile da terzi**, in caso di controversia
- → crittografia asimmetrica

schema generico di firma digitale:



schema generico di firma digitale

schema di firma digitale Elgamal

la cifratura asimmetrica con chiave privata non è l'unico schema possibile di firma digitale

lo schema di firma Elgamal (Elgamal, 1984) lo dimostra

come per il protocollo di Diffie-Hellmann, la sua sicurezza dipende dalla difficoltà di calcolo del logaritmo discreto

schema essenziale: siano

p : un grande numero primo opportuno
g : un intero di ordine p-1 mod p
a : la **chiave privata di firma** dell'autore, e
$y = g^a \bmod p$: la corrispondente **chiave di verifica**
m : il documento da firmare, o un suo hash, in modo che si abbia $0 \leq m < p$

apposizione della firma:

scelta di un numero casuale k, con $0 \leq k < p$, tale che $\gcd(k, p-1) = 1$
calcolo di $r = g^k \bmod p$, e soluzione dell'equazione in s : $a\,r + k\,s \equiv m \bmod p-1$
→ la coppia (r, s) è la **firma** di m

verifica : deve valere l'equazione $y^r\, r^s \equiv g^m \bmod p$

standard di firma digitale

la sicurezza dello schema Elgamal dipende da quella del problema del logaritmo discreto (DLP), ma **non** è equivalente ad essa

anche la sicurezza del protocollo di Diffie-Hellmann dipende da quella del DLP, ma **non è noto** se sia equivalente ad essa o meno

sono state sviluppate varianti dello schema Elgamal più sicure e più efficienti; alcune fra queste sono state tradotte in **norme tecniche** di uso pubblico:

Digital Signature Algorithm (DSA), (NIST, 2000)
Elliptic Curve DSA (ECDSA), (ANSI X9.62, 2005)

per ulteriori informazioni su norme tecniche relative alla firma digitale, v. http://csrc.nist.gov/groups/ST/toolkit/digital_signatures.html

autenticità e certificazione

la verifica di autenticità, del mittente di un messaggio o autore di un testo, permessa dalla crittografia asimmetrica **presuppone** la certezza dell'associazione di una chiave pubblica all'identità, nota o conclamata, di una persona ...

problema: come acquisire tale certezza?

quando la persona non è nota, occorre una **certificazione**, della sua identità e/o di altre credenziali da essa conclamate, da parte di un **terzo**, degno di **fiducia**

in organizzazioni a **struttura gerarchica**, quale ad es. l'albero di un organigramma aziendale, la certificazione può basarsi su tale struttura, dove ciascun nodo dell'albero certifica la veridicità delle credenziali conclamate dai suoi nodi figli

> in tal caso, la certificazione che accompagna una comunicazione include la **catena delle certificazioni** dai livelli successivi fino al vertice, e ognuna di queste contiene la chiave pubblica per la decodifica della comunicazione prodotta al livello inferiore

quando la certificazione non può basarsi su una struttura gerarchica predefinita, si può fare ricorso ad un'**autorità di certificazione** che goda della fiducia delle parti interessate

riferimenti

Elgamal, T. (1984) :

A public key cryptosystem and a signature scheme based on discrete logarithms,
in: Proc. CRYPTO 84 on Advances in cryptology, Springer-Verlag (1984), pp. 10-18;

or:

IEEE Trans. on Information Theory **31**(4), 469-472, 1985.

NIST (2000) :

Digital Signature Standard (DSS),
FIPS PUB 186-2, NIST, 2000.

ANSI X9.62 (2005) :

Public Key Cryptography for the Financial Services Industry:
The Elliptic Curve Digital Signature Algorithm (ECDSA)
ANSI X9.62-2005.