Uso della crittografia

per la sicurezza informatica

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 2006-7

Indice

hash: protezione dell'integrità

la crittografia è utile a garantire (con margini di errore molto bassi) che ad un testo non siano state apportate **alterazioni indebite**, ovvero a rilevare il contrario, ecco come:

un **codice di hash** crittografico è una funzione del testo, e di una chiave segreta per la protezione dell'integrità da alterazioni intenzionali, che gode di due proprietà:

- è molto improbabile che un'alterazione del testo ne dia uno con lo stesso codice di hash
- noti testo e codice di hash, è molto difficile dedurre la chiave

la crittografia impiegata può essere sia simmetrica che asimmetrica, tuttavia la prima è di uso più frequente per la sua efficienza, rapidità e semplicità

le funzioni di hash di solito codificano il testo, di lunghezza arbitraria, in un "riassunto" (digest, checksum, hash) di lunghezza fissa:

- si adopera spesso a tal scopo la **crittografia concatenata a blocchi**
- ovvero si frammenta il testo in blocchi della lunghezza richiesta e si adopera una crittografia a blocchi di lunghezza fissa (quale DES, AES, o altre più semplici) iterativamente, sommando (con XOR) a ciascun blocco il risultato della crittografia concatenata dei blocchi precedenti

funzioni di hash **più in uso:** MD4, MD5 (hash da 128 bit), SHA/SHS (hash da 160 bit)

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

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

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