

Informatica

Lezione 11

Laurea magistrale in Psicologia
Laurea magistrale in Psicologia dello sviluppo e dell'educazione

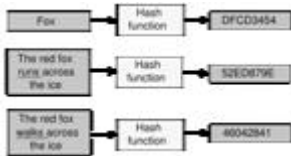
Anno accademico: 2008-2009

Integrità

- Assicurare che il documento ricevuto è integro e non è stato alterato
- Si basa sulle funzioni di hash; a partire da una sequenza di bit, restituisce un output univoco per ogni documento e ne è un identificatore. Inoltre, non è possibile ricostruire il documento originale a partire dalla stringa che viene restituita in output
- Simile all'ultima lettera del codice fiscale

Integrità

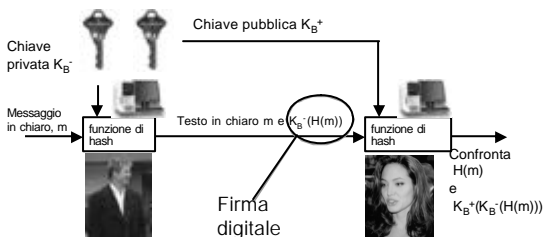
- Naturalmente, per evitare che un terzo sostituisca messaggio e hash, si cifra il hash con la chiave privata del mittente
→ firma digitale



Integrità

- Esempio:
 - Brad vuole firmare digitalmente un documento m che manda ad Angelina
 - Calcola la funzione hash $H(m)$ di m
 - Produce la firma digitale calcolando $K_B^-(H(m))$ usando la propria chiave privata
 - Angelina riceve m e $K_B^-(H(m))$ da Brad e vuole convincere un giudice che il documento è integro ed è stato spedito da Brad
 - Angelina calcola la funzione hash di m , $H(m)$, e la confronta con quella ottenuta applicando la chiave pubblica di Brad $K_B^+(K_B^-(H(m)))$
Se corrispondono, il documento non è stato alterato

Integrità

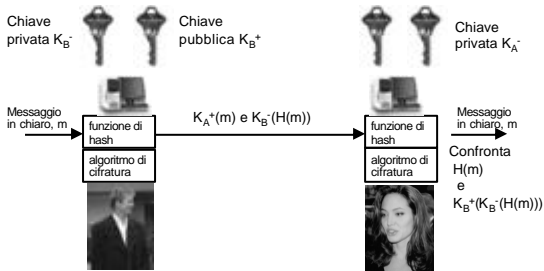


Integrità

- Il giudice conclude che il documento è l'originale spedito da Brad, perché:
 - La firma digitale è stata realizzata con la chiave privata K_B^-
 - Solo Brad è in possesso della propria chiave privata
- Abbiamo anche la garanzia che sia stato spedito proprio da Brad (autenticità)
- Si noti che per un altro messaggio $m' \neq m$, $H(m') \neq H(m)$ e $K_B^+(K_B^-(H(m'))) \neq K_B^+(K_B^-(H(m)))$

Riservatezza+Autenticazione+Integrità

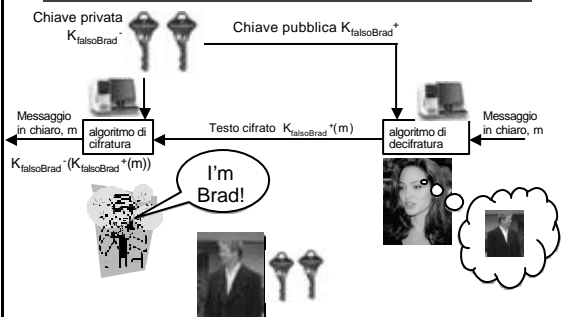
Le tecniche precedenti possono essere combinate



Certificati

- Problema: la struttura a chiavi asimmetriche descritta finora ha un punto debole, la trasmissione della chiave pubblica

Certificati



Certificati

- Angelina pensa di comunicare il messaggio cifrato a Brad, ma il paparazzo ha fornito la propria chiave pubblica, fingendo di essere Brad
 - Risultato: il paparazzo può leggere il messaggio cifrato
- (e Brad potrebbe leggerlo?)

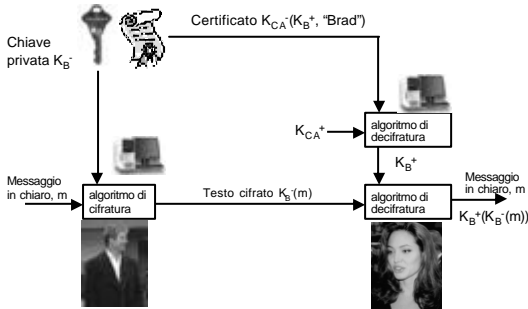
Certificati

- Possibile soluzione: le parti che vogliono comunicare si incontrano di persona e si scambiano le chiavi pubbliche
- Poco pratico in alcuni casi
- Altra soluzione: **certificato**
- È un'attestazione, emessa da una terza parte fidata, che la chiave pubblica appartiene a un individuo o un ente
- Emessi da una Certification Authority (CA)

Certificati

- Un certificato è composto da:
 - Chiave pubblica della persona o dell'ente
 - Nome della persona o dell'ente proprietari della chiave pubblica
 - Periodo di validità
 - Firma digitale del certificato, prodotta dalla CA con la propria chiave privata
 - Quale CA ha emesso il certificato
- Il certificato garantisce la corrispondenza tra la chiave pubblica e l'identità della persona o dell'ente, a patto che ci fidiamo della CA

Autenticità con certificato



Certificati

- Dubbio: non abbiamo semplicemente "spostato" il problema?
 1. Chi ci garantisce che la chiave pubblica della CA sia proprio della CA?
 2. Come si garantisce che la chiave pubblica certificata appartenga realmente alla persona designata?

Certificati

- In effetti il problema è spostato, ma:
 1. I browser e i sistemi operativi vengono forniti con le chiavi pubbliche delle CA preinstallate
 2. La CA identifica la persona o l'ente dietro presentazione di credenziali

→ occorre fidarsi della CA, cioè della sua affidabilità nella verifica delle credenziali e nella sua capacità di proteggere la propria chiave privata

SSL e TLS

Un utilizzo comune dei certificati è nei siti web:
Il protocollo nell'URL è **https**, cioè http su SSL (Secure Sockets Layer) o TLS (Transport Layer Security) (per es. <https://www.gmail.com>)
Viene segnalato dal browser con l'icona di un lucchetto

SSL e TLS

Quando ci si collega a un sito con SSL/TLS:

- il server spedisce il proprio certificato
- il browser controlla che l'URL del server coincida con l'identità contenuta nel certificato
- il browser e il server concordano una chiave segreta simmetrica (per motivi di efficienza) che useranno per cifrare il resto della comunicazione

Questo garantisce **autenticazione** del server (cioè che l'URL del server coincida con l'URL nel certificato) e **confidenzialità** della comunicazione

Non dà altre garanzie (es. identità delle persone che gestiscono il sito, uso corretto delle nostre informazioni, ...)