ESAME - Sicurezza e Affidabilità

Fabio Ferrario
@fefabo

2023/2024

Indice

Capitolo 1

Crittografia

simmetrica vs asimmetrica Si spieghino le differenze tra crittografia simmetrica e assimmetrica

Risposta:

Simmetrica Nella crittografia simmetrica si utilizza una sola chiava, sia per cifrare che per decifrare un messaggio: Il mittente cifra il messaggio con la chiave k e lo invia al destinatario, che dovrà decifrare il messaggio con la stessa chiave k

Asimmetrica Nella crittografia asimmetrica ogni utente genera una coppia di chiavi (legate matematicamente), una pubblica e una privata. La chiave pubblica è accessibile in chiaro a tutti, quella privata invece rimane segreta e conosciuta solo a chi l'ha generata. Queste chiavi sono fatte in modo che se una viene utilizzata per cifrare un messaggio esso potrà essere decifrato solo con l'altra.
Quindi se devo inviare un messaggio a un destinatario lo cifrerò con la sua chiave pubblica, di modo che soltanto esso potrà decifrarlo con la sua chiave privata.

Si descriva la relazione fra numero di chiavi e utenti per la crittografia simmetrica e asimmetrica

Risposta:

simmetrica Per la crittografia simmetrica ogni coppia di utenti ha bisogno di una chiave segreta per potersi scambiare messagi, quindi il numero di chiavi necessario è $\frac{N(N-1)}{2}$

Asimmetrica Nella crittografia asimmetrica invece è solo necessaria una coppia di chiavi per ogni utente, quindi $2N$ chiavi.

Si spieghi il funzionamento della crittografia a **chiave pubblica**, indicando in particolare come si può usarla per implementare **firme digitali**

Risposta:

Crittografia a chiave pubblica Nei sistemi asimmetrici a chiave pubblica genero una coppia di chiavi, una pubblica e una privata.
Le due chiavi sono generate matematicamente in modo che un messaggio criptato con una chiave può essere decrpitato solo con la rispettiva altra chiave. Quindi se devo inviare un messaggio ad un altro utente, cripto il messaggio con la mia chiave privata e lo invio ad un altro utente che lo decripterà con la mia chiave pubblica (che è sempre disponibile).

Firme Digitali Per realizzare firme digitali, si crea un digest del messaggio tramite un algoritmo di Hashing e lo si critta con la chiave privata del mittente. Il messaggio viene quindi inviato al destinatario insieme al digest crittato, che verificherà la mia identità decrittando il digest con la mia chiave pubblica.
In questo modo avrà sia conferma che il mittente sono io, sia la conferma che il messaggio è integro verificando a sua volta con il digest del messaggio inviato.

2 Si descriva come si possono combinare crittografia a chiave asimmetrica e algoritmi di Message Digest per ottenere meccanismi efficienti di **firma digitale**

Risposta: Firmare un messaggio intero è computazionalmente molto costoso, quindi si effettua prima un digest (ad esempio con MD5) del messaggio e poi si usa RSA per crittare il digest.
Quindi i passaggi sono:

1. Il mittente crea il digest del messaggio da inviare.
2. Cifra poi il digest del messaggio con la sua chiave privata ottenendo così la firma digitale.
3. Infine invia il messaggio insieme alla firma.
4. Il destinatario, ricevuti il messaggio e la firma, decifra la firma con la chiave pubblica del mittente ottenendo così il messaggio e il relativo digest.
5. Per controllare l'autenticità del messaggio genera a sua volta un digest di esso e lo confronta con il digest ricevuto.