Sicurezza

- Fondamenti -

dott. ing. Massimiliano Kraus

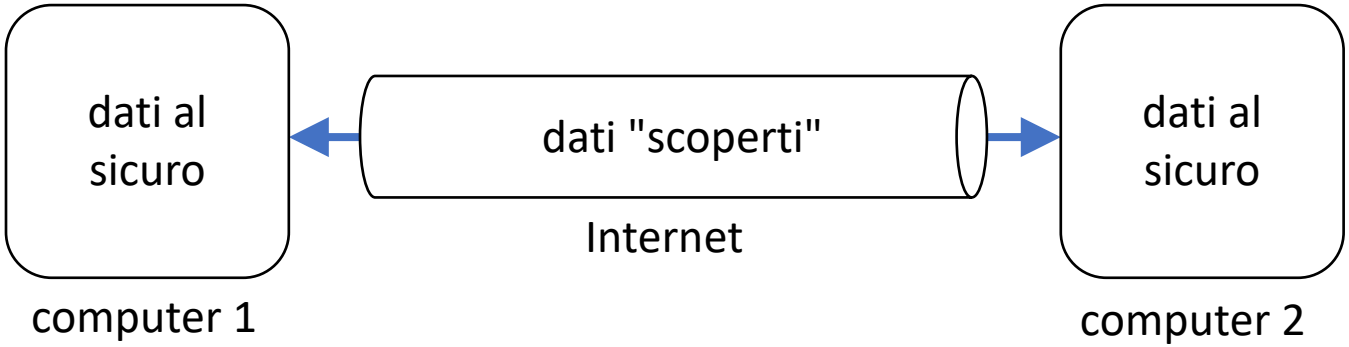
Intro

La sicurezza informatica si articola in:

- Segretezza
- Autenticazione
- Autorizzazione
- Integrità
- Non-ripudio

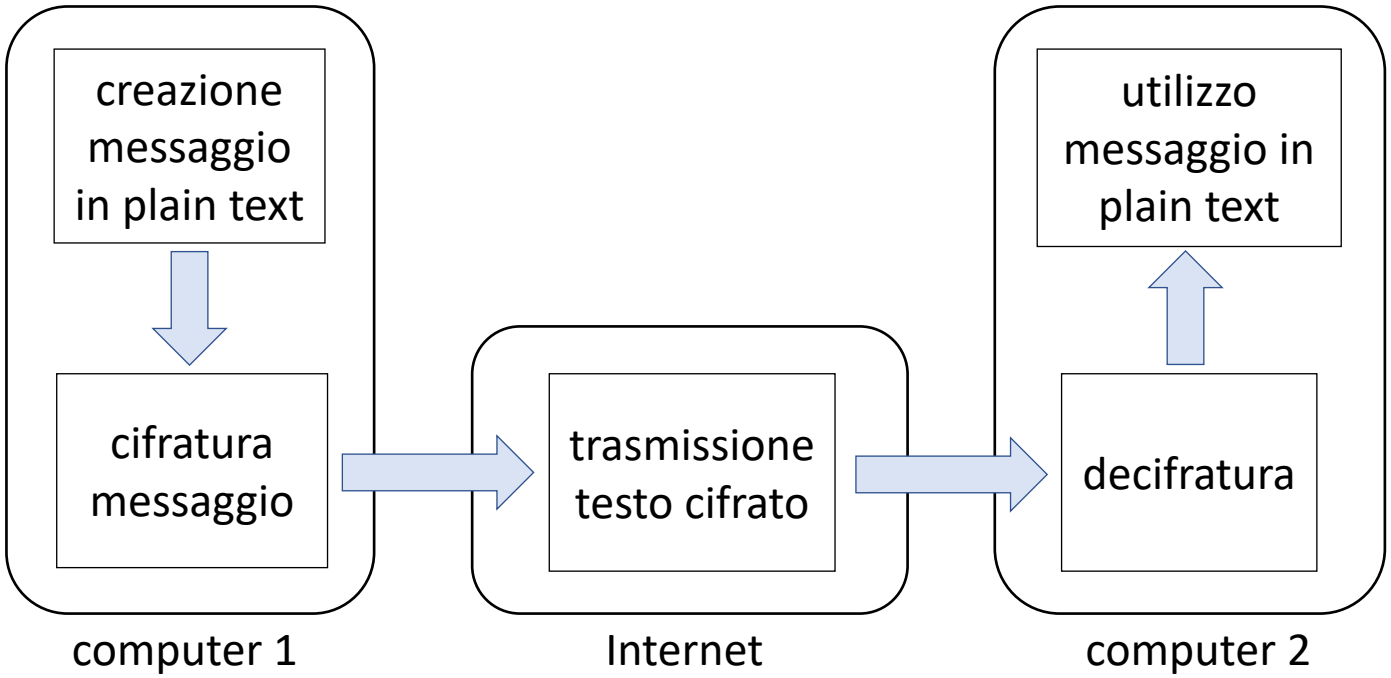
Il problema

Per comunicare in modo veloce dobbiamo utilizzare la rete Internet, un canale assolutamente insicuro!



Segretezza

Per comunicare lungo un canale insicuro è necessario cifrare il testo del messaggio.

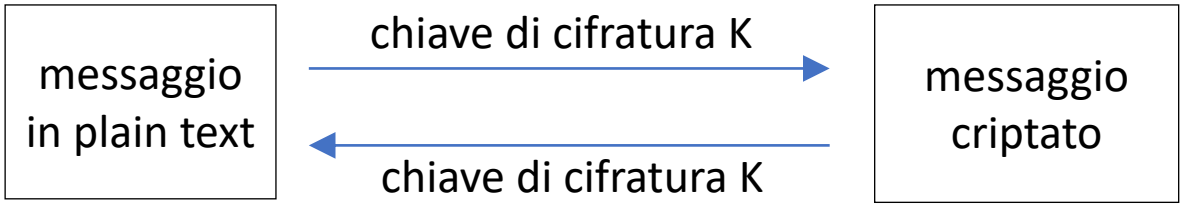


Segretezza

Poiché il testo che passa lungo il canale insicuro è criptato, chiunque lo veda non può capirlo, perché vede solo una sequenza alfanumerica apparentemente senza senso

Crittografia a chiave simmetrica

Una soluzione è quello di criptare il testo piano con una chiave numerica; la chiave può essere usata anche per ri-trasformare il testo criptato in testo piano.



Problemi

C'è il rischio che un terzo agente scopra la chiave, e quindi possa decifrare il testo.

Può succedere se:

- Vengono provate tutte le chiavi (attacco "brute force")
- La chiave viene rubata

Problema "brute force"

Provare tutte le chiavi per trovare quella giusta deve essere impraticabile.

Questo significa che la chiave deve essere abbastanza complicata, in modo che calcolarle tutte richieda troppo tempo.

=> Più i computer diventano potenti, più le chiavi devono complicarsi!

Problema furto

Per cominciare una comunicazione sicura, ho bisogno di una chiave condivisa con l'altra parte.

Ma come faccio a scambiarmi le chiavi inizialmente, se il canale è insicuro?

Problema furto

- È impraticabile per un sito web spedire ad ogni singolo utente una chiave diversa con altri mezzi (posta, …)
- È impraticabile per l'utente medio ricevere una chiave complessa e inserirla nel computer per ogni singola comunicazione da fare.

Crittografia a chiave asimmetrica

Per lo scambio di chiavi simmetriche, all'inizio della comunicazione viene usato un sistema a chiave *asimmetrica*.

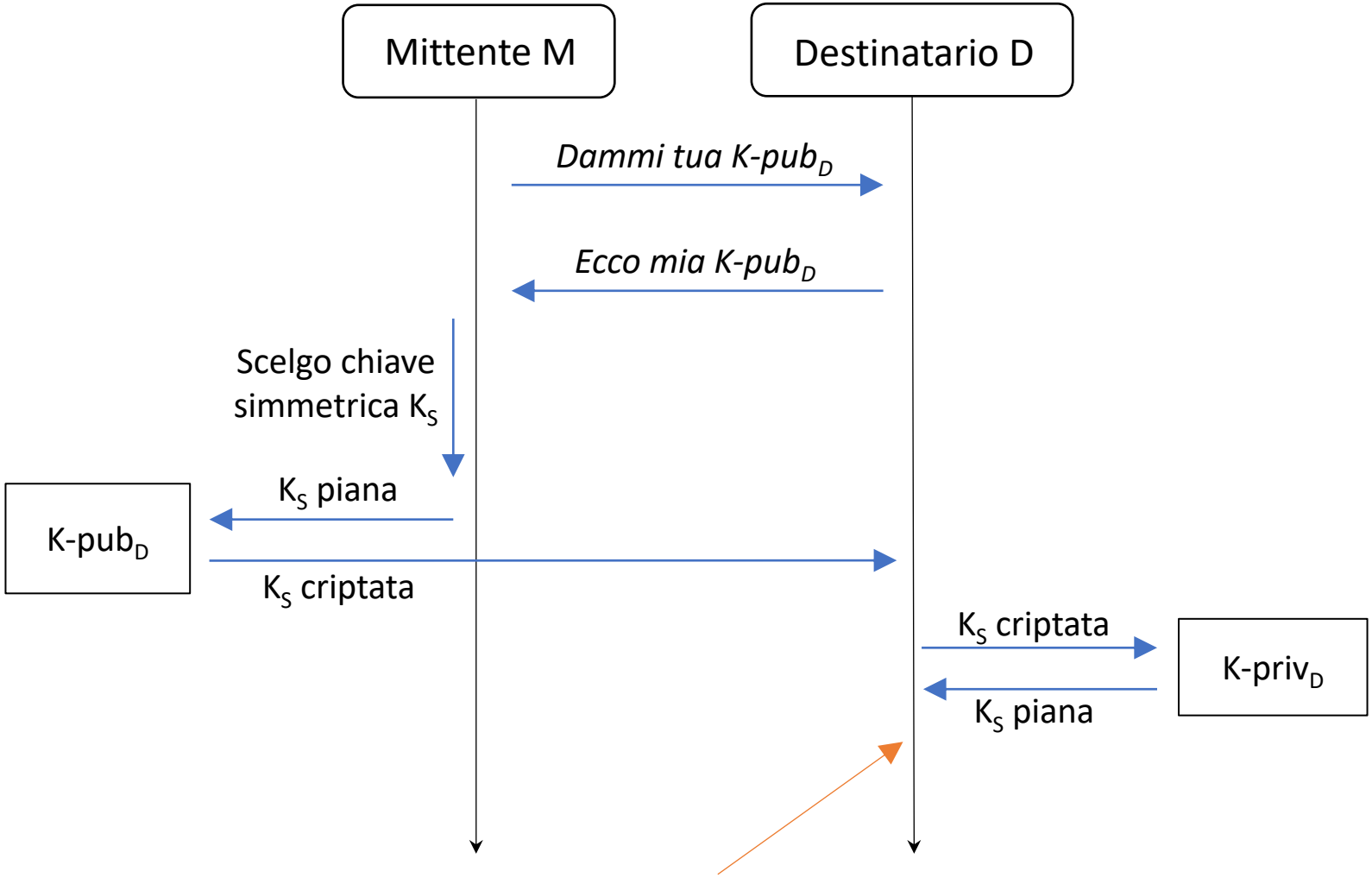
C'è sempre una coppia di chiavi:

- con una chiave cifro il testo piano;
- con l'altra decifro il testo criptato.

Crittografia a chiave asimmetrica

Meccanismo consentito grazie a proprietà matematiche particolari di certe coppie di numeri.

- un numero detto **chiave privata (K-pri)** è in possesso del destinatario;
- l'altro numero è detto **chiave pubblica (K-pub)**, ed è accessibile a tutti.



Da qui in poi hanno entrambi (e solo loro) la chiave simmetrica K_S e possono quindi criptare e decriptare i messaggi che si devono scambiare.

Crittografia a chiave asimmetrica

D può mandare la stessa chiave pubblica a qualunque mittente M e attraverso un mezzo insicuro: per decifrare il testo criptato la chiave pubblica è inutile, serve la chiave privata.

=> La chiave privata va custodita con molta cura.

Crittografia a chiave asimmetrica

Durante la comunicazione vera e propria si usa una crittografia a chiave simmetrica perché i calcoli per criptare e decriptare il testo sono molto più veloci (da 10 a 100 volte) rispetto alla crittografia asimmetrica.

Crittografia a chiave asimmetrica

Problema: il destinatario dice di essere D… ma è proprio D?

ES: mi collego al sito della mia banca online. Sono sicuro che sia proprio la mia banca e non un sito fraudolento? Qualsiasi sito può crearsi una coppia di chiavi asimmetriche!

Certificati

M ha bisogno di qualcuno che verifichi l'identità di D.

=> Sistema di **certificati**.

D manda:

- chiave pubblica K-pub$_D$;
- certificato di una certa Certification Authority che conferma l'autenticità di K-pub$_D$ (C-CA$_D$).

Certificati

M riceve K-pub$_D$ e C-CA$_D$.

Come fa M a verificare K-pub$_D$ tramite C-CA$_D$?

M ha installate alcune Certification Authority nel computer.

M trova la CA indicata nel certificato.

Tramite quella CA verifica K-pub$_D$

Certificati

Meccanismo opposto a quello dello scambio di messaggi:

- D chiede a CA di certificarlo.
- CA usa la propria K-pri$_{CA}$ per criptare il nome di D.
- CA distribuisce la sua K-pub$_{CA}$.
- M può usare K-pub$_{CA}$ per decriptare il certificato C-CA$_{D}$ mandato da D e verificarne così l'identità.

Integrità

Ora M sa come verificare l'indentità di D e come essere sicuro che i dati scambiati siano segreti.

Ma come fa ad essere sicuro che siano anche integri?

ES: un server tra M e D potrebbe cercare di iniettare del contenuto esterno nella comunicazione.

Message Authentication Code (MAC)

Ogni messaggio viene elaborato calcolando una piccola stringa di hash, detta MAC.

Il MAC viene inviato in coda al messaggio.

Il ricevente fa un controllo incrociato tra il MAC da lui calcolato sul testo decifrato, e il MAC inviato in coda dal mittente.

Se non coincidono… il messaggio non è integro!