Elementi di sicurezza e crittografia

LAB61

Ponte della Ghisolfa, 20 Ottobre 2016

Nessun software proprietario è stato utilizzato per realizzare questa presentazione

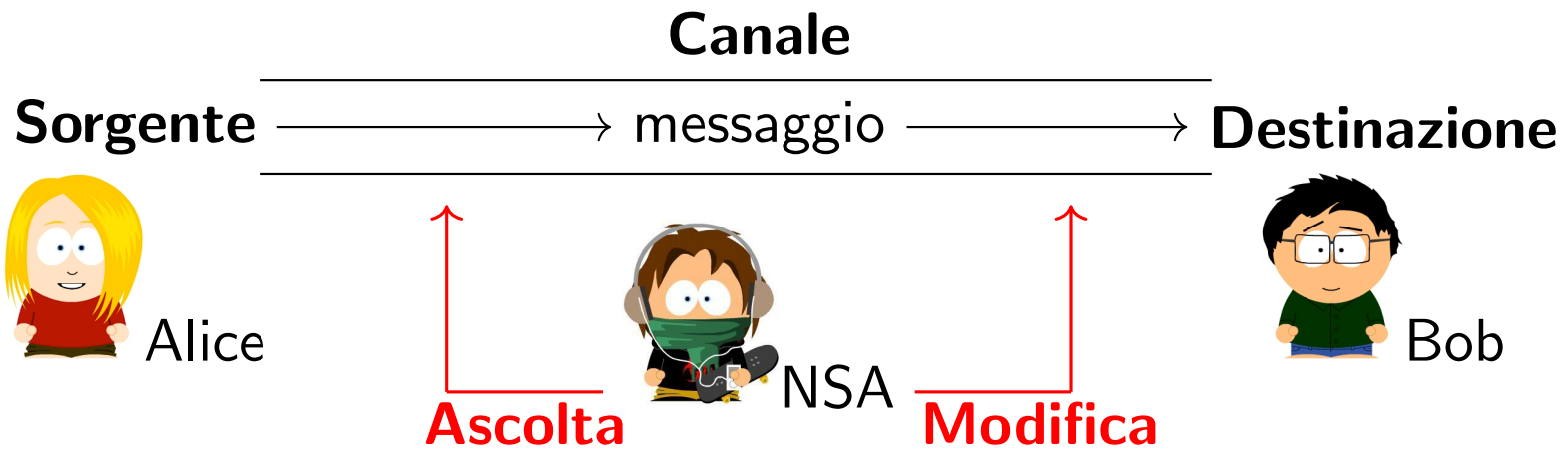
La comunicazione

Definizione

Definiamo un modello di comunicazione:
Sorgente (S) - **Canale** (C) - **Destinazione** (D).
Il **messaggio** per arrivare da S a D transita per C.

La necessità della sicurezza

Quando comunichiamo spesso necessitiamo di certe proprietà di **sicurezza**.



Le proprietà fondamentali (1)

Confidenzialità

Definizione

È la proprietà che assicura che il messaggio non venga compreso da un utente esterno mentre transita nel canale.

Autenticità

Definizione

È la proprietà che assicura che il messaggio sia stato spedito realmente da chi ci aspettiamo che l'abbia spedito.

Le proprietà fondamentali (2)

Disponibilità

Definizione

È la proprietà che assicura che una volta arrivato, il messaggio sia subito disponibile.

Integrità

Definizione

È la proprità che ci assicura che il messaggio non sia cambiato dal momento dell'invio a quello della ricezione, ovvero durante il transito nel canale.

Soluzioni? (1)

Soluzione banale

Non comunico.

Spesso è la maniera migliore di risolvere il problema, rimuovendo il messaggio rimuovo anche il pericolo che altri lo conoscano.

Soluzione meno banale

Nascondo il messaggio.

È una soluzione praticabile e praticata, chiamata **steganografia**. I messaggi possono ad esempio essere nascosti in immagini o occultati nei modi più diversi.

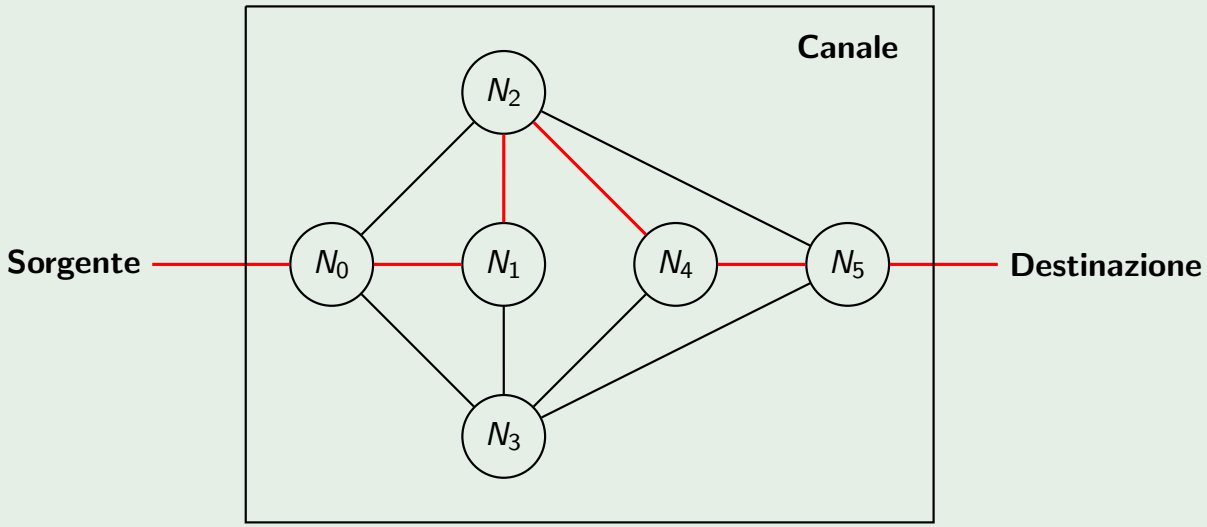
Soluzioni? (2)

Soluzione naïve

Blindare il canale.

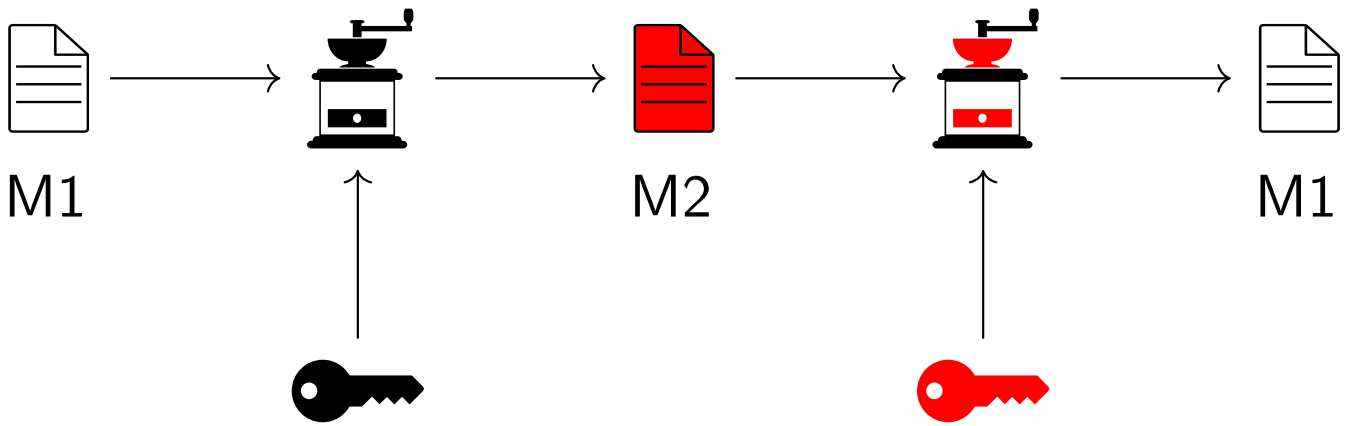
È una soluzione chiaramente inattuabile data la natura di internet. Internet è infatti una **rete distribuita** e i messaggi passano da molti intermediari prima di arrivare a destinazione.

Esempio



L'idea della crittografia

Perciò nasce l'idea della crittografia, ovvero un meccanismo che permette di trasformare il messaggio M1 in un altro altro M2, incomprensibile per chiunque, e che solo il possessore della chiave potrà ritrasformare in quello originale M1.



Formalmente

Definizione

Un **crittosistema** Ξ è una quintupla $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ dove:

- $\mathcal{P}$ è l'insieme dei messaggi in chiaro,
- $\mathcal{C}$ è l'insieme dei messaggi cifrati,
- $\mathcal{K}$ è l'insieme delle chiavi,
- $\mathcal{E} = \{E_k | \, k \in \mathcal{K}\}$ è la famiglia di funzioni di cifratura iniettive tale che $E_k : \mathcal{P} \to \mathcal{C}$ per ogni $k \in \mathcal{K}$,
- $\mathcal{D} = \{D_k | \, k \in \mathcal{K}\}$ è la famiglia di funzioni di decifratura biiettive tale che $D_k : \mathcal{C} \to \mathcal{P}$ per ogni $k \in \mathcal{K}$,

tale che per ogni $e \in \mathcal{K}$ esiste unica $d \in \mathcal{K}$ tale $D_d(E_e(m)) = m$, per ogni $m \in \mathcal{P}$.

Le tecniche

Esistono fondamentalmente due diversi meccanismi di cifratura: a **chiave pubblica** e a **chiave privata** che a loro volta si basano su diversi tipi di **algoritmi**.

Crittografia simmetrica	**Crittografia asimmetrica**
DES	Diffie-Hellman
3DES	Curve ellittiche
AES	RSA
...	...

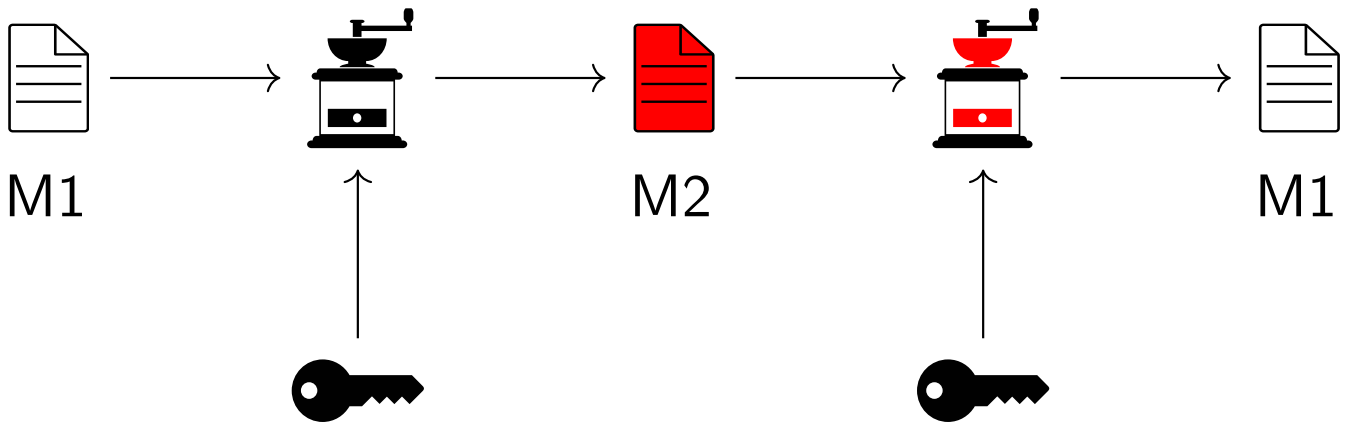
Gli algoritmi che permettono l'effettivo funzionamento della crittografia si basano su della matematica parecchio avanzata e in particolare sulla teoria dei numeri, sull'algebra (tipicamente dei campi finiti), sulla teoria della probabilità e sulla teoria della complessità computazionale.

Crittografia simmetrica

Definizione

La **crittografia simmetrica** è un meccanismo che utilizza la stessa chiave per cifrare e decifrare il messaggio.

Formalmente $D_k(E_k(m)) = m$ per ogni $m \in \mathcal{P}$ e per ogni $k \in \mathcal{K}$, con D_k e E_k semplici (veloci) da calcolare.



Problema!

E lo scambio della chiave?

Nella crittografia simmetrica sia il mittente che il ricevente devono conoscere la chiave, cioè devono essersela scambiata in qualche momento. A questo punto però lo scambio della chiave come fa ad avvenire in maniera sicura? Se utilizzassimo di nuovo un metodo di cifratura simmetrico per cifrare la chiave saremmo al punto di partenza.

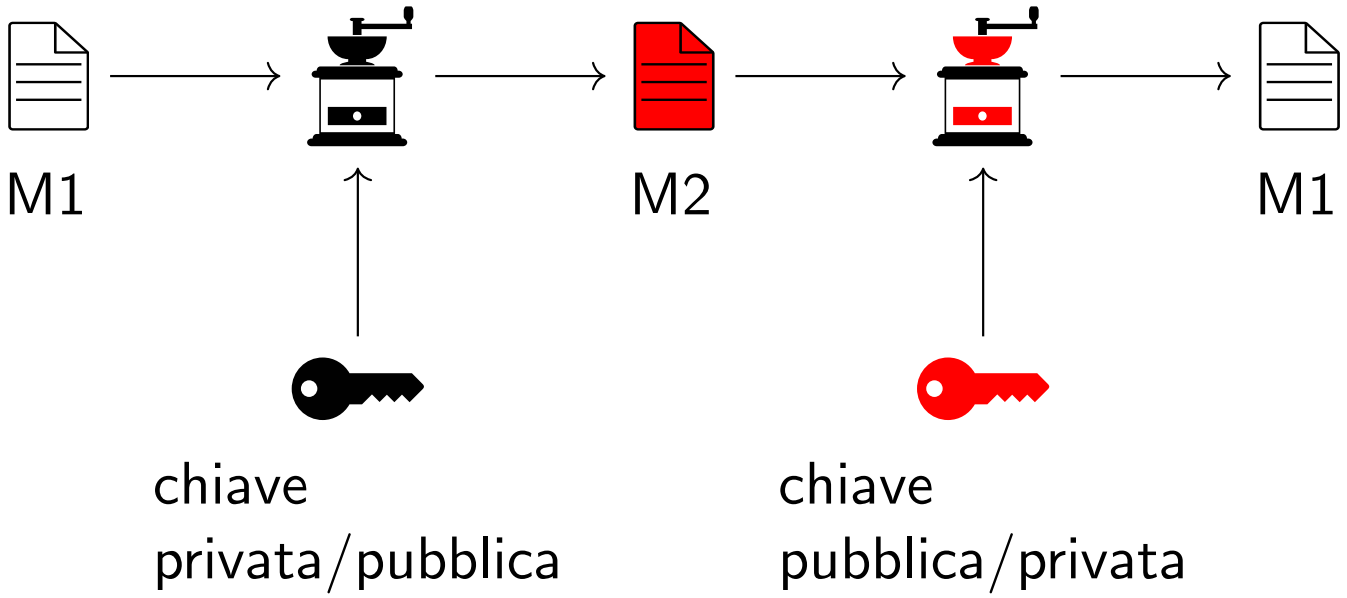
Per questo tipicamente o si utilizza per scambiare la chiave un altro canale considerato sicuro oppure si ricorre alla...

Crittografia asimmetrica

Definizione

La **crittografia asimmetrica** è un meccanismo che funziona con due chiavi. Se si cifra il messaggio con la prima, con la seconda lo si decifra e viceversa.

In realtà non è così, ma possiamo immaginarlo in questo modo.



Dogma della crittografia asimmetrica

La seguente regola è sempre da rispettare quando si utilizza un **sistema crittografico asimmetrico**.

Dogma

Ogni utente deve mantenere segreta una delle chiavi, che chiameremo **privata** e distribuire l'altra, che chiameremo **pubblica**.

Funzionamento nella comunicazione - confidenzialità

Vediamo ora come utilizzare la **crittografia asimmetrica** per ottenere la proprietà di **confidenzialità**.

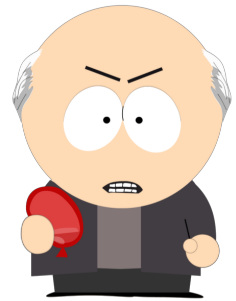
Per la comunicazione bisogna seguire questi passaggi:

Algoritmo per la comunicazione confidenziale

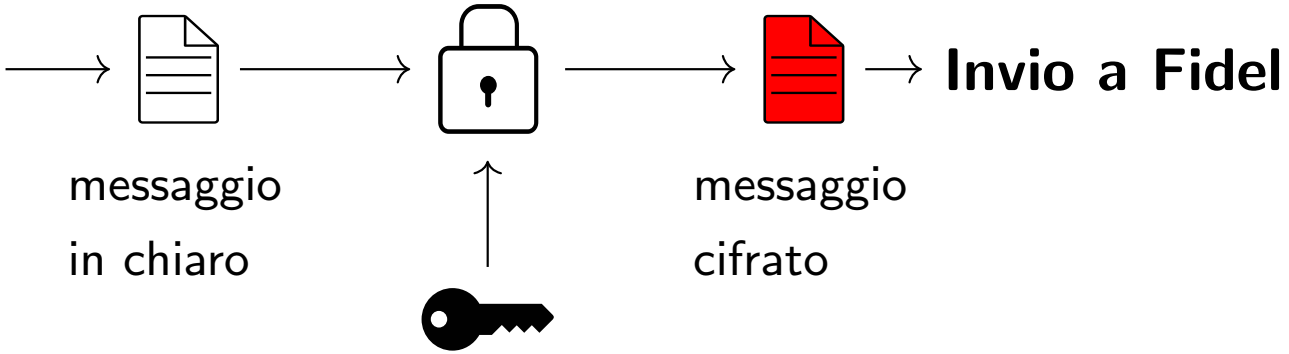
1° passo: cifro il messaggio con la chiave pubblica del destinatario.
2° passo: invio il messaggio cifrato.
3° passo: il destinatario lo decifra con la sua chiave privata.

In questa maniera mentre il messaggio transita nel canale il messaggio è cifrato e solo chi è in possesso della chiave privata corrispondente a quella pubblica con cui è stato cifrato potrà decrittarlo.

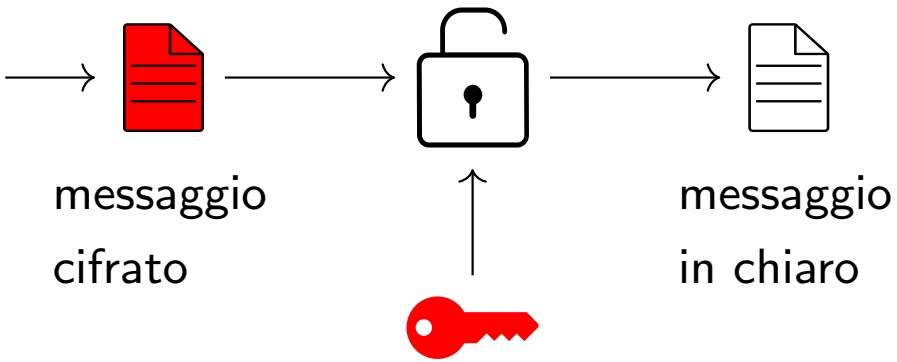
Esempio di comunicazione confidenziale



Krusciov



Fidel



Funzionamento nella comunicazione - autenticità

Vediamo ora come utilizzare la **crittografia asimmetrica** per ottenere la proprietà di **autenticità**.

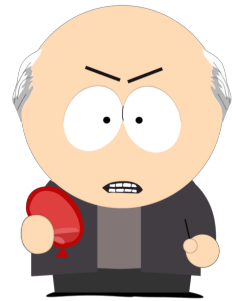
Per la comunicazione bisogna seguire questi passaggi:

Algoritmo per la comunicazione autentica

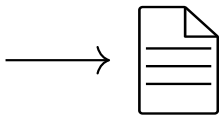
1° passo: cifro il messaggio con la mia chiave privata.
2° passo: invio il messaggio cifrato.
3° passo: il destinatario lo decifra con la mia chiave pubblica.

In questa maniera il destinatario è sicuro che il mittente sia proprio chi deve essere (ha infatti utilizzato la propria chiave privata) perché altrimenti non riuscirebbe a decrittare il messaggio con la sua chiave pubblica.

Esempio di comunicazione autentica



Krusciov



messaggio
in chiaro

chiave privata
di Nikita

messaggio
cifrato

Invio a Fidel

Fidel

messaggio
cifrato

chiave pubblica
di Nikita

messaggio
in chiaro

Mettiamo tutto insieme!

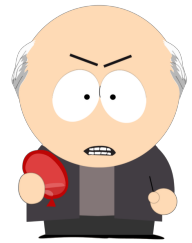
Combinando entrambe le metodologie riusciamo ad ottenere sia **confidenzialità**, sia l'**autenticità**.

Per la comunicazione sicura bisogna seguire questi passaggi:

Algoritmo per la comunicazione sicura

1° passo: cifro il messaggio con la mia chiave privata.
2° passo: cifro il messaggio con la chiave pubblica del destinatario.
3° passo: invio il messaggio cifrato.
4° passo: il destinatario lo decifra con la sua chiave privata.
5° passo: il destinatario lo decifra con la mia chiave pubblica.

Esempio conclusivo



Krusciov

messaggio in chiaro

chiave privata di Nikita

chiave pubblica di Fidel

messaggio cifrato

Invio a Fidel

Fidel

messaggio cifrato

chiave privata di Fidel

chiave pubblica di Nikita

messaggio in chiaro

Conclusioni

Non abbiamo parlato della **disponiblità** e dell'**integrità**.

La prima è assicurata dal fatto che operazioni di decrittazione sono "veloci".

Per l'**integrità** si può utilizzare uno dei tanti protocolli che calcolano l'**hash** di un testo, ovvero una "impronta digitale". Inviando insieme al testo anche l'hash il destinatario potrà ricalcolare l'hash sul testo arrivato e confrontarlo con quello arrivato. Se coincidono c'è un'altissima probabilità che il testo sia integro, se non coincidono certamente il testo arrivato è diverso da quello spedito.

Esempi di protocolli di hash sono **SHA** e **MD5**.

Bibliografia


http://web.math.unifi.it/users/fumagal/documenti/Crittografia_Capitoli1-6.pdf


http://poisson.phc.unipi.it/~papini/TCC.pdf


https://www.iacr.org/authors/tikz/


https://thenounproject.com/ - Viktor Vorobyev, Apirat Ditsayarak, Guilhem