Elementi di sicurezza e crittografia

LAB61

Ponte della Ghisolfa, 20 Ottobre 2016

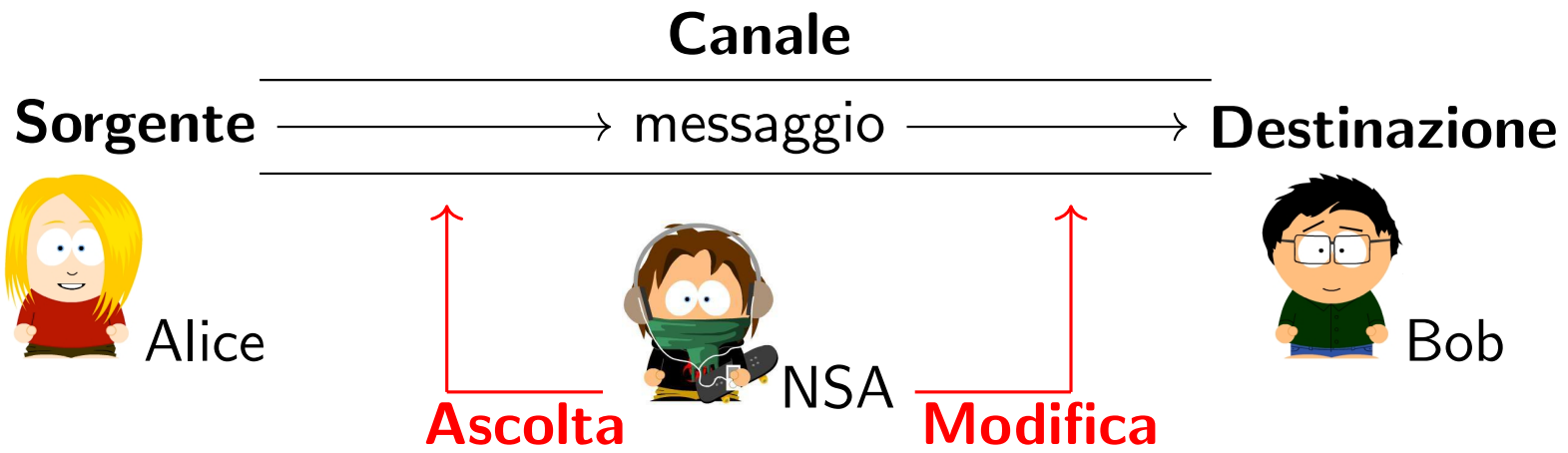
La comunicazione

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.

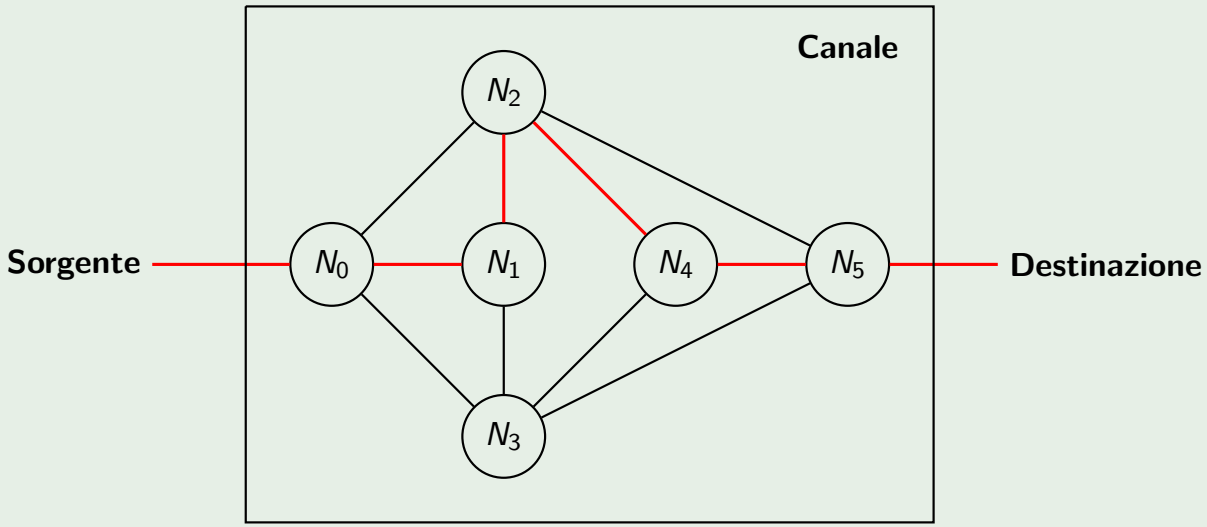
Soluzioni? (2)

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 $k \in \mathcal{K}$.