Privacy e posta elettronica

Laboratorio di Informatica Popolare

2 dicembre 2009

Sulla privacy

In un sistema di cose nel quale il controllo viene sempre più imposto come la panacea di tutti i mali, è opportuno fare chiarezza sui pericoli che la comunicazione via e-mail comporta e sulle contromisure che è possibile adottare

Struttura presentazione

- Privacy e posta elettronica - perché?
  - Introduzione sulla privacy
  - I rischi della tua casella di posta elettronica
- Privacy e posta elettronica - come?
  - Crittografia simmetrica
  - Crittografia asimmetrica
  - Crittogragia asimmetrica e posta elettronica
- Conclusioni

Introduzione sulla privacy

Privacy, in quali contesti?

- **Segreti non legati alle persone**: negoziati, finanza, giustizia, sanità ecc.
- **Segreti legati alle persone: vita personale**, intimità, sentimenti privati ecc.

Preoccuparsi della propria privacy, serve anche a proteggere quella dei propri corrispondenti

I rischi della casella di posta elettronica

Il percorso delle e-mail

I contenuti delle tue e-mail sono a rischio in vari modi:

- Quando spedisci un messaggio, per prima cosa il client di posta contatta un server attraverso un protocollo (SMTP) e trasferisce a quest'ultimo il messaggio. Questo trasferimento di solito avviene in chiaro
- Il server SMTP a sua volta contatta il server del destinatario e questo passaggio di solito avviene ancora in chiaro
- Inoltre ogni volta che spedisci una e-mail gli ISP ne memorizzano una copia

I rischi della casella di posta elettronica

Il percorso delle e-mail

Esempio:

Se dal csoa il Molino si invia una e-mail ad una persona che abita a Bellinzona, le copie che si creeranno della tua e-mail saranno perlomeno:

1. Il tuo pc invia l'e-mail ad un primo computer situato presso il tuo fornitore d'accesso (**copia 1**)
2. Il computer del fornitore d'accesso manda una copia (nel migliore dei casi) al computer del fornitore di accesso del tuo destinatario (**copia 2**)
3. Il computer dell'ISP del tuo destinatario mantiene una copia dell'e-mail (**copia 3**), in attesa che quest'ultimo scarichi la posta (**copia 4**)

I rischi della casella di posta elettronica

Il contenuto di una e-mail può essere quindi facilmente letto da persone diverse dal nostro destinatario.
È dovere morale di un utente proteggere i suoi dati. Un po' come usare una busta chiusa per inviare una lettera, o parlarsi in modo riservato quando si sta in un ambiente affollato

I rischi della casella di posta elettronica

Riassumendo:

- *Target dell'attacco*:
  Le comunicazioni tramite posta elettronica
- *Modalità di attacco*:
  A seconda di chi entra in possesso dei dati, essi potranno essere analizzati, raccolti ecc.
- *Contromisura*:
  Comunicare in modo che i dati non siano comprensibili a nessuno ad eccezione del destinatario

Crittografia

La crittografia è la scienza che studia la scrittura e la lettura di messaggi in codice

Crittografia

Viene utilizzata per assicurare:

- **Riservatezza**: stabilisce l'identità di mittente e destinatario
- **Integrità**: garantisce che i dati non siano alterati
- **Non ripudio**: garantisce che nessuno, al di fuori di mittente e distinatario siano in grado di interpretare i dati

Tipi di crittografia

Funzioni crittografiche per l'autenticazione, l'integrità e la segretezza dei dati:

- Crittografia simmetrica
- Crittografia asimmetrica (o a chiave pubblica)

Crittografia simmetrica

Due persone che desiderano comunicare devono accordarsi su di un **algoritmo** e su di una **chiave** comune

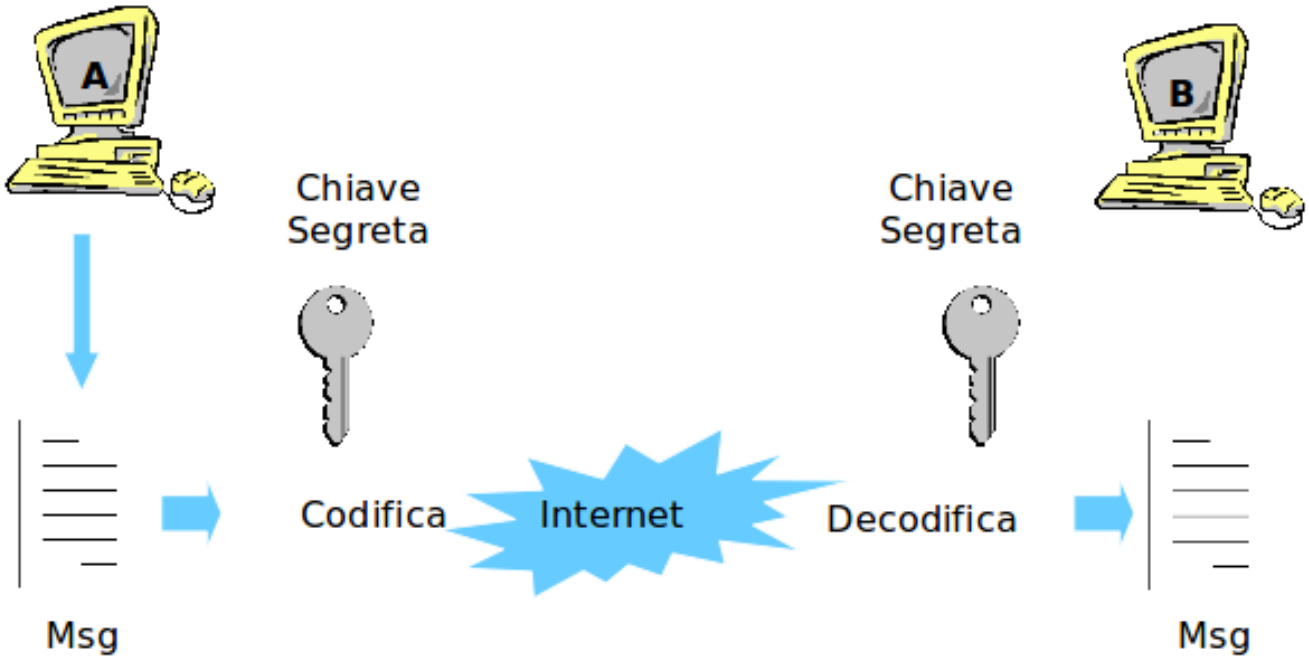
Crittografia simmetrica

Esempio: il cifrario di Cesare (n=5)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E

- Ciao a tutti
- Hnft j yzyyn

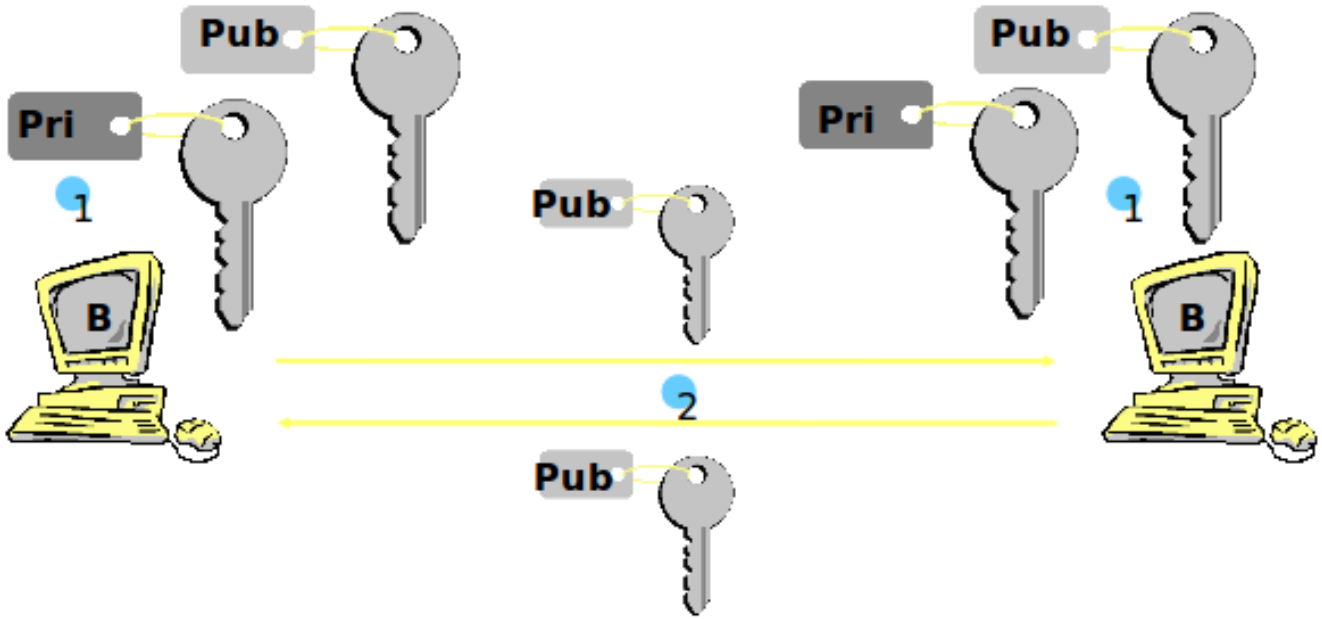
Crittografia simmetrica



Crittografia asimmetrica

- È chiamata anche Crittografia a chiave pubblica
- Risolve il problema della distribuzione sicura delle chiavi, infatti per comunicare utilizzando la crittografia a chiave pubblica, A e B necessitano di una coppia chiave pubblica - chiave privata
- Onguno dei due deve creare la propria coppia di chiavi.
  Nelle comunicazioni fra loro, A e B utilizzeranno chiavi diverse per decodificare e decodificare i dati
- La crittografia a chiave asimmetrica risolve il problema della distribuzione sicura delle chiavi. Una chiave infatti è pubblica, mentre l'altra è privata

Crittografia asimmetrica



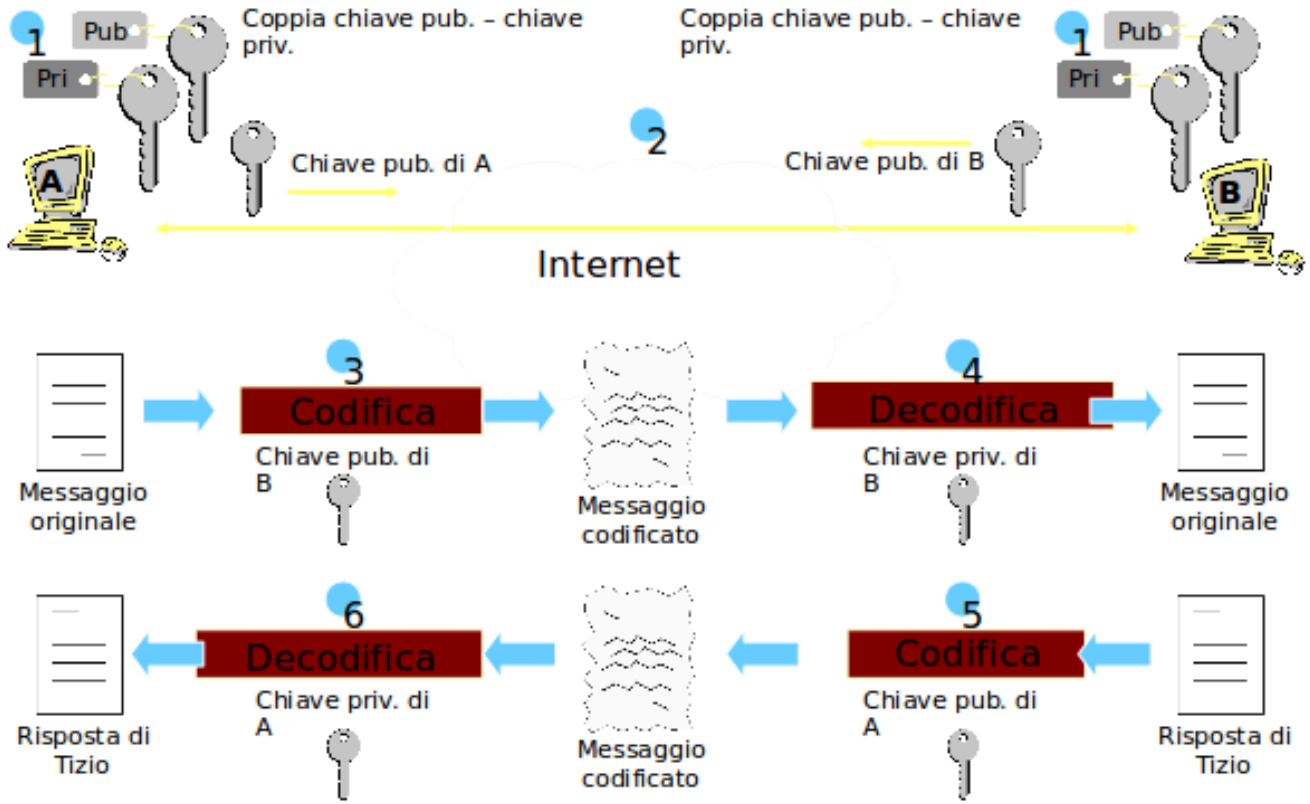
1. Crea una coppia chiave privata - chiave pubblica
2. Scambia solo chiavi pubbliche

Crittografia asimmetrica

Perché avvenga uno *scambio di dati segreto*, debbono verificarsi le seguenti condizioni:

1. A e B creano le proprie coppie di chiavi pubbliche e private
2. A e B si scambiano le chiavi pubbliche
3. A scrive a B e codifica il messaggio utilizzando la chiave pubblica di B prima di trasmetterlo via Internet
4. B utilizza la propria chiave privata per decifrare il messaggio
5. B risponde, codifica il messaggio utilizzando la chiave pubblica di A e lo trasmette via Internet
6. A utilizza la propria chiave privata per decifrare il messaggio

Crittografia asimmetrica



Crittografia asimmetrica

La segretezza è garantita dal momento che A trasmette il messaggio originale, in quanto solo B può decodificarlo con la propria chiave privata. Allo stesso tempo, viene assicurata anche l'integrità dei dati, perché il messaggio non può essere modificato se non con la chiave privata di B. Lo stesso vale per la risposta, in quanto solo A ha accesso alla propria chiave privata

Crittografia e intercettazioni

La crittografia è la tecnica che assicura la riservatezza dei dati

- A patto che l'altro comunicante (destinatario) la supporti
- A patto che si sia considerato correttamente il modello di minaccia
- A patto che l'implementazione non sia una trappola
- A patto d'aver badato alla sicurezza locale della macchina

Crittografia e posta elettronica

Che programma posso usare per crittare le mie e-mail?

- GPG (Gnu Privacy Guard): software rilasciato sotto licenza Gnu e di cui è verificabile il codice
  `http://it.wikipedia.org/wiki/GNU_Privacy_Guard`
  `http://www.gnupg.org/`

Crittografia e posta elettronica

Per usare GPG cosa devo fare?

- Avendo installato Thunderbird ed Enigmail sul computer, tutto quello che serve è creare un paio di chiavi
  `http://www.autistici.org/loa/web/doc/enigmail/`

Crittografia e posta elettronica

Nella pratica come funziona?

1. Con il software di crittazione si crea una chiave di due parti una pubblica e una privata. Alle persone con cui vuoi comunicare, trasmetti la parte pubblica della vostra chiave. Solo tu puoi usare la chiave privata
2. Quando scrivi un messaggio di posta elettronica, usi la chiave pubblica del destinatario per crittarlo
3. Il processo di crittazione inserisce una sorta di lucchetto elettronico nel tuo messaggio. Anche se questo è intercettato durante il suo tragitto, il suo contenuto è inaccessibile per mancanza della chiave
4. Quando il messaggio arriva, il destinatario inserisce una password (composta da una o più parole). Il software usa la chiave privata per verificare che per la crittazione sia stata usata la chiave pubblica del destinatario
5. Usando la chiave privata, il software sblocca la crittazione e consente di leggere il messaggio

Crittografia e posta elettronica... ultimo passo

Per poter utilizzare un sistema di crittazione asimmetrico è essenziale la diffusione della chiave pubblica. Se nessuno ha la tua chiave pubblica, nessuno potrà crittare messaggi diretti a te

- Uno dei server utilizzabili per questo scopo è `http://pgpkeys.mit.edu/`

Link utili

Alcuni link con tutorial realizzati per il LIP

- Come e perché tutelare la privacy della tua posta elettronica
  `http://tinyurl.com/leo-lip`
- Come crittare un'e-mail con Mac os x
  `http://tinyurl.com/om-lip1`

Contatti

leo@autistici.org
Key fingerprint:
3B6D 0688 6DEB 470B 1F8C F5A0 0B83 0507 9727 34BB