

# Informatica

Lezione 9

Laurea magistrale in Psicologia  
Laurea magistrale in Psicologia dello sviluppo e dell'educazione  
Anno accademico: 2008-2009

## La sicurezza nelle reti

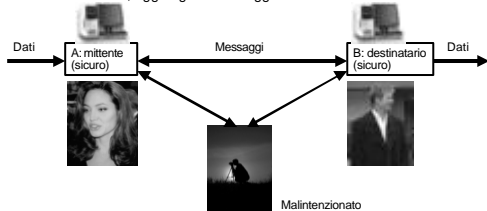
- Proprietà necessarie per la sicurezza in rete:
  - *Riservatezza* solo il mittente e il destinatario dovrebbero essere in grado di comprendere il contenuto del messaggio trasmesso
    - Un messaggio può essere intercettato: quindi dovrebbe essere *cifrato* (dal mittente) e *decifrato* (dal destinatario)
    - Il messaggio cifrato dovrebbe essere incomprensibile a chi non possiede il codice di decifratura
    - Esistono altri tipi di riservatezza: per esempio, forse il mittente vuole mantenere segreto non solo il contenuto del messaggio mandato al destinatario, ma anche il fatto che sta comunicando con il destinatario

## La sicurezza nelle reti

- Altre proprietà necessario per la sicurezza in rete:
  - *Autenticazione* il mittente e il destinatario devono essere reciprocamente sicuri della loro identità
  - *Integrità del messaggio* il contenuto di una comunicazione non deve subire alterazioni durante la trasmissione
    - Alterazioni: per esempio, a manipolazioni

## La sicurezza nelle reti

- Durante la comunicazione, un malintenzionato potrebbe:
  - Ascoltare i messaggi in transito (per esempio, per rubare una password)
  - Cancellare, aggiungere messaggi o modificare il loro contenuto



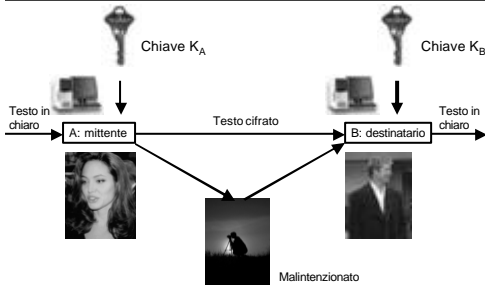
## Crittografia

- *Crittografia*: consente al mittente di mascherare i dati in modo che un malintenzionato non possa comprendere il contenuto
- Il destinatario deve essere in grado di risalire ai dati originali
- *Testo in chiaro* (plaintext o cleartext): il messaggio originario scritto dal mittente
- *Messaggio cifrato* (ciphertext): la versione cifrata del messaggio

## Crittografia

- In molti casi le tecniche di crittografia sono di dominio pubblico
  - Occorrono delle informazioni segrete che impediscono ai malintenzionati di decifrare i messaggi: le *chiavi*
  - Il mittente ha una chiave  $K_A$  usata per generare la versione cifrata  $K_A(m)$  del messaggio  $m$  di testo in chiaro
  - Il destinatario ha una chiave  $K_B$  e un algoritmo di decifratura che restituisce il messaggio  $m$  di testo in chiaro: cioè calcola  $K_B(K_A(m))=m$

## Crittografia



## Chiave simmetrica

- Le chiavi di A (mittente) e B (destinatario) sono identiche e segrete
- Per esempio: un antico algoritmo - cifrario di Cesare
  - Considerare un messaggio di testo
  - Sostituire ogni carattere del testo con un altro sfasato (rispetto al primo) di un numero  $k$  di posti nell'alfabeto
  - Per esempio: se  $k=3$ , "a" diventa "d", "c" diventa "f", ecc.
  - Ciclico: una volta terminato l'alfabeto si ricomincia con la lettera "a"
  - La chiave è il valore  $k$
  - "Brad, I love you. Angelina" (con  $k=3$ ) diventa "Eudg, L oryh brx. Dqjholqd" (nell'alfabeto inglese)

## Chiave simmetrica

- Per esempio: cifrario monoalfabetico
  - Considerare un messaggio di testo
  - Sostituire ogni carattere del testo con un altro, ma la sostituzione avviene seguendo uno schema arbitrario
  - Però una data lettera è sostituita con sempre la stessa lettera
  - Per esempio:

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
m	n	b	v	c	x	z	a	s	d	f	g	h	j	k	l	p	o	i	u	y	t	r	e	w	q

"Brad, I love you. Angelina" diventa "Nomv, S gkct wky. Mjzcgsljm"

## Chiave simmetrica

- Nel caso di cifratura monoalfabetica: un attacco può essere basato sulla ricerca tra tutti le combinazioni possibili (un attacco detto di "forza bruta")
  - Alcune lettere e gruppi di lettere (in italiano, "che", "zione" e "mente") ricorrono con maggiore frequenza: rende più facile un attacco al codice
- Cifratura polialfabetica: usa molteplici sostituzioni monoalfabetiche
  - Per esempio, la sequenza C1 C2 C2 C1 C2
  - Cifrare la prima lettera del messaggio usando C1, la seconda lettera con C2, ..., la quinta con C2
  - Poi ripetiamo la sequenza: la sesta lettera è cifrata con C1, la settima con C2, ecc.

## Chiavi asimmetriche

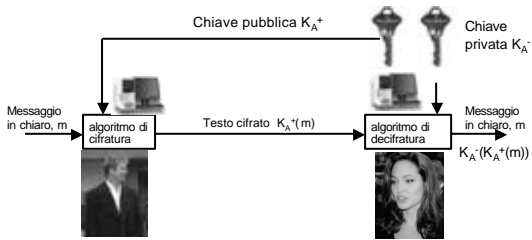
- Svantaggio delle chiavi simmetriche: le due parti coinvolte nella comunicazione devono conoscere la chiave
  - Ma come? Comunicata fisicamente? Tramite un canale sicuro? Non è sempre possibile
- Una soluzione: chiavi asimmetriche
  - Il sistema usa due chiavi:
    - Una chiave pubblica ( $K^+$ ): disponibile a chiunque, anche ai malintenzionati
    - Una chiave privata ( $K^-$ ): conosciuta solo al proprietario

La chiave privata spesso viene memorizzata su una smart card e protetta da un PIN

## Chiavi asimmetriche

- Analogia:
  - Chiavi **simmetriche**:
    - Angelina mette il messaggio segreto in una cassetta e la chiude con un lucchetto di cui ha la chiave; spedisce la cassetta tramite posta e Brad la apre con una copia della chiave, che ha ottenuto precedentemente
  - Chiavi **asimmetriche**:
    - Angelina e Brad hanno due lucchetti diversi. Brad manda ad Angelina il lucchetto, tenendo per sé la chiave; Angelina chiude il messaggio segreto nella cassetta e la spedisce a Brad, che può aprirla con la propria chiave

## Chiavi asimmetriche



Notazione:  $K_A^+(m)$  indica che il messaggio  $m$  viene cifrato con la chiave  $K_A^+$

## Chiave pubblica: RSA

- Il sistema a chiave pubblica RSA è il più noto dei sistemi a chiave pubblica
  - RSA: nome derivato dalle iniziali degli inventori Rivest, Shamir e Adleman
  - Due punti fondamentali:
    - La scelta della chiave pubblica e di quella privata
    - Gli algoritmi di cifratura e di decifratura
  - Basato sui numeri primi
  - *numeri primi*: i numeri naturali che sono divisibili solo per 1 e per se stessi: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, ...
  - *Fattori di un numero naturale z*: qualsiasi insieme di interi che, moltiplicati tra di loro, danno  $z$
  - Notazione:  $y \text{ mod } z$  sta per il resto della divisione  $y/z$

## Chiave pubblica: RSA

- Per ottenere la chiave pubblica e la chiave privata, si deve:
  1. Scegliere due numeri primi,  $p$  e  $q$  (tanto più grande sarà il loro valore tanto più difficile risulterà violare RSA: si raccomanda che il prodotto di  $p$  e  $q$  sia dell'ordine di 1024 o 2048 bit (con 1024 bit si può rappresentare un numero con oltre 300 cifre!))
  2. Calcolare  $n = pq$  e  $z = (p-1)(q-1)$
  3. Scegliere un numero  $e$  (encryption), tale che  $e < n$ ,  $e > 2$  e che non abbia fattori in comune con  $z$
  4. Scegliere un numero  $d$  (decryption), tale che  $d < n$ ,  $ed - 1$  sia un multiplo di  $z$  (in altri termini, tale che il resto della divisione  $ed/z$  sia 1)

La chiave **pubblica**  $K^+$  è la coppia  $(n, e)$ ,  
La chiave **privata**  $K^-$  è la coppia  $(n, d)$

## Chiave pubblica: RSA

- Brad vuole inviare a Angelina un numero  $m$ , tale che  $m < n$
- Per codificarlo, Brad usa la chiave pubblica di Angelina  $K_A^+ = (n, e)$  per calcolare il messaggio cifrato  $c$ , dove
 
$$c = m^e \text{ mod } n$$
- Per decifrare il messaggio ricevuto, Angelina usa la propria chiave privata  $K_A^-$  per calcolare
 
$$m = c^d \text{ mod } n$$
- La scelta di  $e$  e  $d$  garantisce che
 
$$(m^e \text{ mod } n)^d \text{ mod } n = m$$

## Chiave pubblica: RSA

- Esempio (artificiale):
  - Angelina sceglie  $p=5$  e  $q=7$
  - Poi  $n = pq = 35$ , e  $z = (p-1)(q-1) = 24$
  - Angelina sceglie  $e = 5$  (5 e 24 non hanno fattori in comune)
  - Angelina sceglie  $d = 29$  ( $5 \cdot 29 - 1$  è divisibile per 24)
  - Angelina rende pubblica la chiave (35, 5) e mantiene segreta la chiave (35, 29)
  - Brad vuole inviare le lettere "l", "o", "v", "e" ad Angelina
  - Interpretiamo le lettere come numeri fra 1 e 26 (i numeri corrispondono alle posizioni delle lettere nell'alfabeto inglese)

## Chiave pubblica: RSA

- Esempio:
  - Codifica di Brad (chiave pubblica  $K_A^+ : n=35, e=5$ )

Lettere in chiaro	$m$ : rappresentazione numerica	$m^e$	Testo cifrato $c = m^e \text{ mod } n$
l	12	248832	17
o	15	759375	15
v	22	5153632	22
e	5	3125	10

- Decodifica di Angelina (chiave privata  $K_A^- : n=35, d=29$ )

Testo cifrato $c$	$c^d$	$m = c^d \text{ mod } n$	Lettere in chiaro
17	481968572106750915091411825223071697	12	l
15	12783403948858939111232757568359375	15	o
22	851643319086537701956194499721106030592	22	v
10	10000000000000000000000000000000	5	e

## Chiave pubblica: RSA

- Perché funziona RSA?
    - $(m^e \bmod n)^d \bmod n = (m^{ed} \bmod n) \bmod n = m^{ed} \bmod n$
    - Teorema: se  $p$  e  $q$  sono primi, e  $n = pq$ , allora:
 
$$x^e \bmod n = x^{ed \bmod ((p-1)(q-1))} \bmod n$$
    - Applicando questo risultato, possiamo scrivere:
 
$$m^{ed} \bmod n = m^{ed \bmod ((p-1)(q-1))} \bmod n$$
    - Ricordiamo che  $e$  e  $d$  sono tali che  $ed - 1$  sia divisibile per  $(p-1)(q-1)$
    - Quindi il resto di  $(p-1)(q-1) \mid ed - 1$
    - Così  $ed \bmod ((p-1)(q-1)) = 1$
    - Dato che  $m < n$ , abbiamo:
 
$$m^{ed \bmod ((p-1)(q-1))} \bmod n = m^1 \bmod n = m$$
    - Così abbiamo il risultato che volevamo:
 
$$m^{ed} \bmod n = m$$
- (Cioè, cifrando un messaggio  $m$  con  $c = m^e \bmod n$  e decifrandolo con  $c^d \bmod n$  otteniamo il messaggio iniziale)

## Chiave pubblica: RSA

- Efficacia di RSA:
  - Non si conoscono algoritmi veloci per la fattorizzazione dei numeri interi
  - Quindi, anche con la conoscenza del numero  $n$ , è computazionalmente proibitivo calcolare i fattori  $p$  e  $q$
  - Per es., per fattorizzare un numero di 663 bit (200 cifre) un gruppo di ricerca ha impiegato tre mesi usando un cluster di 80 computer (oltre 55 anni con un computer solo)
  - Se venisse scoperto un algoritmo veloce per la fattorizzazione, il sistema RSA non sarebbe più sicuro
- È fondamentale proteggere la propria chiave privata: se viene compromessa, il "ladro" sarà in grado di leggere i nostri messaggi cifrati (e di spacciarsi per noi)

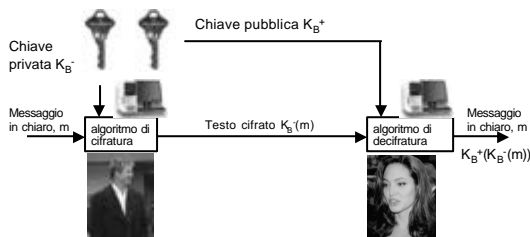
## Firme digitali

- Firme digitali: usate come le firme nel mondo "non-informatico"
  - Per esempio, per indicare il titolare di un documento, o di dichiarare di approvare del contenuto di un documento
  - Utilizzate per garantire autenticità e integrità
  - Devono essere verificabili, non falsificabili e non riproducibili
  - Anche in questo caso usiamo la crittografia a chiave pubblica, con il ruolo invertito: cifriamo con la chiave privata e decifriamo con la chiave pubblica

## Autenticità

- Il mittente è proprio chi dichiara di essere
- Esempio:
  - Brad vuole firmare digitalmente un documento  $m$  che manda a Angelina
  - Calcola  $K_B^-(m)$  usando la propria chiave privata
  - Angelina riceve  $K_B^-(m)$  da Brad e vuole convincere un giudice che il documento è stato firmato da Brad
  - Angelina applica la chiave pubblica di Brad per calcolare  $K_B^+(K_B^-(m)) = m$ , che corrisponde al documento originale

## Autenticità



## Autenticità

- Il giudice conclude che Brad ha firmato il documento, perché:
  - Il testo è stato cifrato con la chiave privata  $K_B^-$
  - Solo Brad è in possesso della propria chiave privata
- Si noti che per un altro messaggio  $m' \neq m$ ,  $K_B^+(K_B^-(m')) \neq m$