Crittografia e sicurezza dei sistemi Informatici

Le Reti di Computer

A. S. 2008-2009

Tiso Emanuele

Sicurezza nei sistemi informatici

- La sicurezza dei sistemi informatici riguarda:
  - Aspetti Hardware legati a guasti
  - Aspetti Software legati a malfunzionamenti
  - Aspetti legati agli Accessi ai dati
- Il concetto giuridico di sicurezza informatica è collegato a quel complesso di accorgimenti tecnici e organizzativi che mirano a tutelare i beni giuridici:
  - della **confidenzialità o riservatezza** (legato ad accessi non autorizzati)
  - della **integrità** (non cancellazione o modifica di dati)
  - della **disponibilità delle informazioni registrate** (affidabilità legate ad eventi accidentali)
- All' Art. 615 ter della legge 547/93 l'accesso non autorizzato a un sistema informatico viene equiparato alla "violazione di domicilio" quindi un delitto contro l'inviolabilità del domicilio anche se si dimostra di non aver alcuna intenzione di rubare

Calamità Naturali

- Alcuni Eventi:
  - Tifoni, Terremoti, Incendi, Alluvioni
- Le aziende provvedono a dotarsi di procedure particolate che consentano di far ripartire le attività in pochi giorni.
- Creare norme e depositi sicuri (edifici bunker e resistenti al fuoco, sistemi di rilevamento fumi e antincendio) per le apparecchiature vitali per la ripresa.
- Definire una scaletta di interventi articolata e prestabilita per una corretta ripresa.

Attentati Terroristici

- Il sistema informatico di un'azienda è il punto nevralgico dell'azienda. Un blocco può paralizzare l'intera attività economica
- Attentati a scopo di estorsione e ricatto o semplicemente da parte di mitomani; non è un evento da sottovalutare.
- La strategia di protezione è quella di collocare le apparecchiature in luoghi sempre più protetti con adeguati protocolli di protezione.

Guasti e Interruzioni Hardware

- Problema particolarmente sentito nelle aziende, con sistemi di elaborazione (downtime), che non consentono l'interruzione dell'attività come banche, supermercati, ecc..
- La sicurezza può essere garantita esclusivamente con tecniche di duplicazione di parti dell'intero sistema e tecniche di subentro automatici.
- Vengono attuate tecniche di "fault tolerance" che riguarda principalmente:
  - L'alimentazione
  - Le memorie di massa
- Per le interruzioni dell'alimentazione (black-out) si prevedono:
  - Sistemi di alimentazione alternativa con gruppi di continuità UPS (Uninterruptible Power Supply) dotati di accumulatori statici e gruppi elettrogeni

Guasti e Interruzioni Hardware

- Livelli di “fault tolerance” per le memorie di massa:
  1. Mirroring → Copia identica dello stesso disco o solo alcuni archivi vitali. In caso di errore in I/O l’accesso passa automaticamente alla copia alternativa (copia di Mirroring)
  2. Duplexing → Duplicazione sia dei dischi che delle unità di controllo (controller). Il sistema può continuare a funzionare anche in presenza di guasti fisici al controller dei dischi.
  3. Duplicazione dell’intero sistema → Duplicazione dell’intero server eventualmente collocati in luoghi fisicamente diversi
- Vi sono inoltre tecniche meno costose rispetto alla duplicazione parziale del sistema:
  - Tecnica RAID → Distribuzione dei dati su vari dischi con tecniche di ricostruzione matematica di tutti i dati eventualmente persi su uno dei dischi.

Errori del Personale

- Enormi quantità di dati sono spesso archiviate in piccoli spazi per cui bastano anche errori banali per produrre disastri
- Norme preventive:
  - Netta separazione fra ambiente di esercizio e ambiente di sviluppo (Nelle fasi di prove è bene che si lavori in un ambiente di sviluppo con dati di prova per evitare errori accidentali)
  - Copia periodica di tutti i dati aziendali su supporti da riporre in luogo sicuro
  - Utilizzare personale di un certo livello nelle manutenzioni ai software
  - Definizione di regole organizzative e figure professionali preposte che verifichino costantemente i dati in input e output
  - Favorire attività di formazione del personale per sviluppare e consolidare le conoscenze informatiche specifiche dell'azienda

Virus

- Tra i problemi di sicurezza che coinvolgono i sistemi software (applicazioni e dati) vi sono i virus
- I virus sono programmi costruiti allo scopo di:
  - Infettare un programma senza alterarne il funzionamento
  - Rendersi visibile in qualche modo strano
  - Distruggere i dati e/o i programmi
  - Autoriprodursi in modo da creare un'epidemia
- Sono prodotti per gioco o per finalità ricattatorie

Virus

- La protezione dai virus:
  - Controllo sistematico dei supporti utilizzati
  - Utilizzo di software specifici che evitano l'infezione o ne riconoscono la presenza fornendo uno strumento per l'eliminazione
- Spesso l'eliminazione di un virus richiede l'eliminazione del programma ospite, pertanto è fondamentale prevenire l'infezione
- Prevedere un protocollo sistematico di aggiornamento devirus
- Effettuare comunque sempre una copia di sicurezza dei dati importanti per eventuale ripristino in caso di corruzione o cancellazione da parte di virus.

Archivi e DataBase

- Gli archivi e i DataBase sono la risorsa più importante per un'azienda e possono essere utilizzate da più persone e/o programmi
- La sicurezza degli archivi è legata principalmente alla **perdita** e agli **accessi non autorizzati**
- La perdita è legata al malfunzionamento dei dischi e/o errori degli operatori
  - Esecuzione di backup (salvataggio) giornaliero dei dati che garantisce un restore (ripristino) quasi integralmente dei dati
- Gli accessi ai dati devono essere autorizzati (da un gestore) e controllati mediante password con limiti non più ampi di quanto necessario
  - A livello di sistema operativo (password di ingresso)
  - A livello di DBMS
  - A livello di applicazioni che utilizzano i dati

Sicurezza nelle reti

- I problemi di sicurezza sono notevolmente amplificati se i computer sono collegati alla rete aziendale e se questa e accessibile all'esterno
  - Virus informatici
  - Furti di dati e cancellazione di dati
  - Rallentamento e interruzione della attività dell'azienda
- La protezione dagli "Hacker" (persona che si collega ai sistemi informativi senza l'autorizzazione) si basa principalmente sul rigoroso controllo degli accessi
  - Sistemi di identificazione
    - Con password complesse
    - Con sistemi di riconoscimento con tessere magnetiche
  - Sistemi di log (tener traccia delle operazioni svolte dopo l'autenticazione

Sicurezza nelle reti
Internet

- Il grado di interconnessione sta aumentando in modo massiccio e con essa la necessità di una crescente sensibilità all'aspetto sicurezza
- L'implementazione di sistemi di protezione non può però impedire la comunicazione fra sistemi il cui grado di affidabilità è sconosciuto.
- Vi sono purtroppo sempre delle vulnerabilità strutturali nelle connessioni di computer e queste vengono sfruttate per produrre effetti disastrosi.
- Nello sviluppo di applicazioni è quindi importantissimo prevedere sempre adeguate strategie di protezione.
- E' necessario trovare un giusto equilibrio fra necessità di anonimato nell'utilizzo di applicazioni e l'imputabilità che presuppone il riconoscimento degli utenti che utilizzano le applicazioni.

Sicurezza nelle reti
Protezioni nel Web

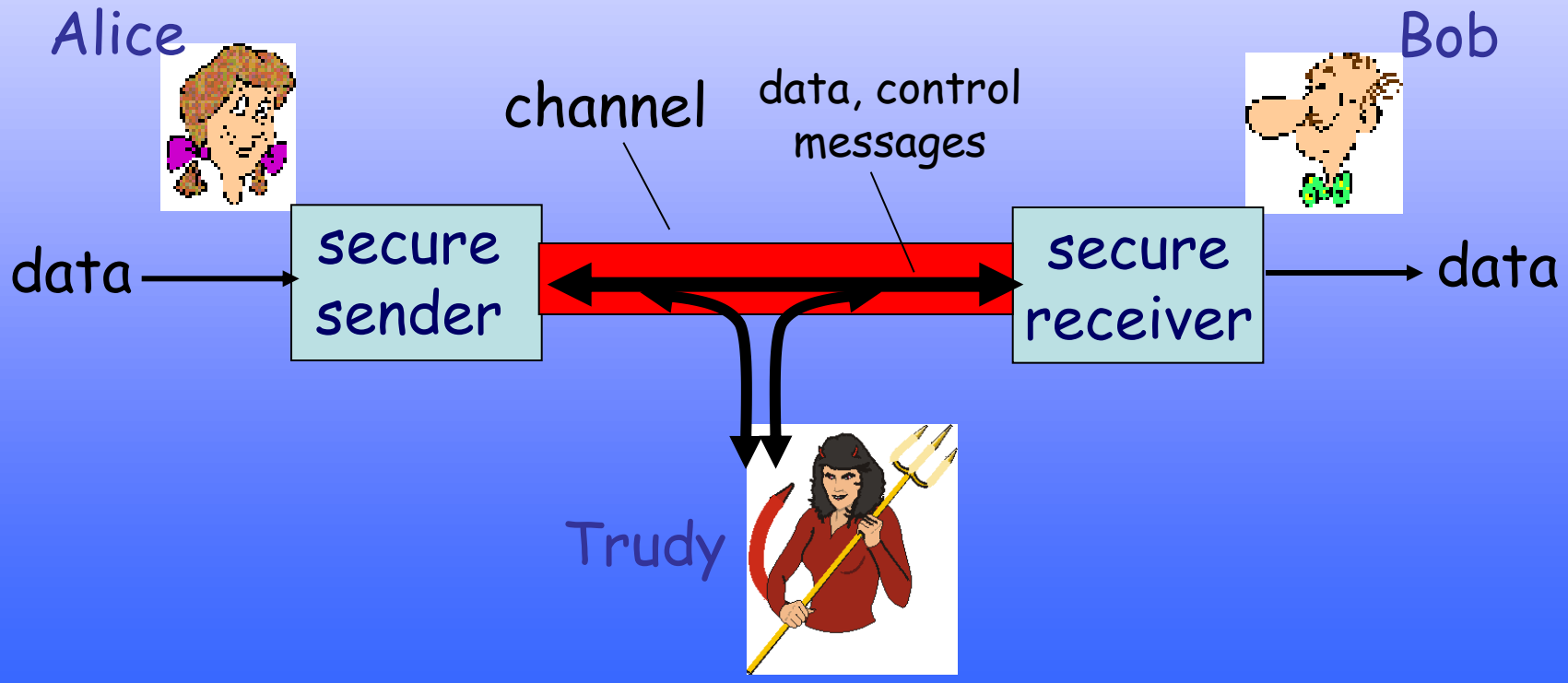
- I Browser vengono utilizzati per la visualizzazione di pagine Web e richiedono una corretta impostazione dei livelli di sicurezza affinché non diventino oggetto di attacco esterno.
- Evitare la connessione a siti non affidabili o l'esecuzione di "script" e "applet" che possono produrre l'inserimento di virus nel sistema o accesso fraudolento ai dati del disco.
- Alcuni siti utilizzano la tecnica di inserire dei "cookie" nel computer dell'utente allo scopo di memorizzare informazioni sull'utente
  - Per proporre una visualizzazione personalizzata (teoricamente non dannosa)
  - Per raccogliere informazioni presenti sul computer per secondi fini senza il consenso dell'utente
- E' possibile impostare i browser per impedire la memorizzazione dei cookie, oppure la loro cancellazione alla chiusura del browser

Cos’è la sicurezza di rete ?

- Confidenzialità (Segretezza):
  - Solo il mittente ed il destinatario legittimo devono *capire* il contenuto del messaggio
    - il mittente cifra (cripta) il messaggio
    - il ricevente lo decifra (decripta)
    - Chiunque può averlo, ma non saprà interpretarlo
- Autenticazione (Garanzia dell’identità):
  - Sia mittente che destinatario vogliono essere sicuri dell’identità della controparte
- Integrità
  - Mittente e destinatario vogliono potersi rendere conto se il messaggio è stato alterato
    - durante la spedizione o anche dopo essere stato registrato
- Accessibilità:
  - Gli utenti devono essere in grado di utilizzare comunque i servizi offerti dalla rete

Amici e nemici: Alice, Bob, Trudy

- Nomi tipici nel campo della network security
- Bob, Alice (amanti?) vogliono comunicare *in sicurezza*
- Trudy (l'intrusa) potrebbe voler intercettare, cancellare o generare messaggi



Chi potrebbero essere Bob e Alice ?

… a parte le due persone reali ...

- Web browser/server per transazioni economiche on-line
- Client/server per on-line banking
- DNS server
- Router che si scambiano aggiornamenti di tabelle interne

Crittografia

- L'E-busniss ha la necessità di garanzie riguardo l'inviolabilità (integrità) dei dati trasmessi
- Negli ultimi anni sono stati sviluppati protocolli e tecniche valide per la sicurezza

- La Crittografia è la tecnica di rendere visibile le informazioni soltanto alle persone a cui sono destinate.
- La Crittografia è nota fin dall'antichità e si è sviluppata soprattutto per scopi militari.
- Il testo che può essere letto da tutti viene detto "testo in chiaro"
- Con la tecnica di "cifratura"(codifica) si trasforma un testo da leggibile in illeggibile "testo cifrato"
- L'operazione inversa viene chiamata "decifratura" (decodifica) che produce nuovamente il testo in chiaro

Crittografia

- La codifica e decodifica sono eseguite da uno o più "algoritmi crittografici" che fanno uso di una "chiave"
- Tecnica utilizzata da Giulio Cesare noto con il nome di "**cifrario a sostituzione**":
  - La chiave era costituita semplicemente da un numero intero e provocava la sostituzione delle lettere con le lettere di posizione incrementata della chiave prevista

Es: GIULIO CESARE

↕ Chiave = 3

LNAONR FHVDUH

Crittografia

- Altra tecnica di crittografia "**cifrario a trasposizione**"
  - La chiave è costituita da una parola
    1. Si costruisce una tabella con un numero di colonne pari alla parola chiave
    2. Si colloca il testo in chiaro nelle celle sottostanti da sinistra a destra e dall'alto verso il basso
    3. Il messaggio cifrato viene generato prendendo le colonne della tabella seguendo l'ordine alfabetico

Crittografia

- **“cifrario a trasposizione”**

Es: Parola chiave = *vince*

Testo in chiaro = *la cavalleria deve attaccare sull’ala sinistra*

v	i	n	c	e
l	a	c	a	v
a	l	l	e	r
i	a	d	e	v
e	a	t	t	a
c	c	a	r	e
s	u	l	l	a
l	a	s	i	n
i	s	t	r	a

aeetrlir c vrvaeana e alaacuas i cldtalst n laiecsli v

Testo cifrato = aeetrlirvrvaeanaalaacuascldtalstlaiecsli

Il destinatario conoscendo la parola chiave è in grado di ricostruire la tabella e riprodurre il testo in chiaro

Crittoanalisi

- Tecniche sviluppate al fine di violare le comunicazioni cifrate.
- Il testo cifrato è noto mentre l'algoritmo di crittografia e la chiave non sono note
- In alcuni casi l'algoritmo di crittografia è noto ma non si conosce la chiave
- L'algoritmo di Giulio Cesare può essere violato tranquillamente con una successione di prove "esaustive" finchè non si ottiene il testo in chiaro.
  Il numero di chiavi possibili possono essere al massimo 21 pari all'alfabeto italiano.

Crittografia a chiave simmetrica

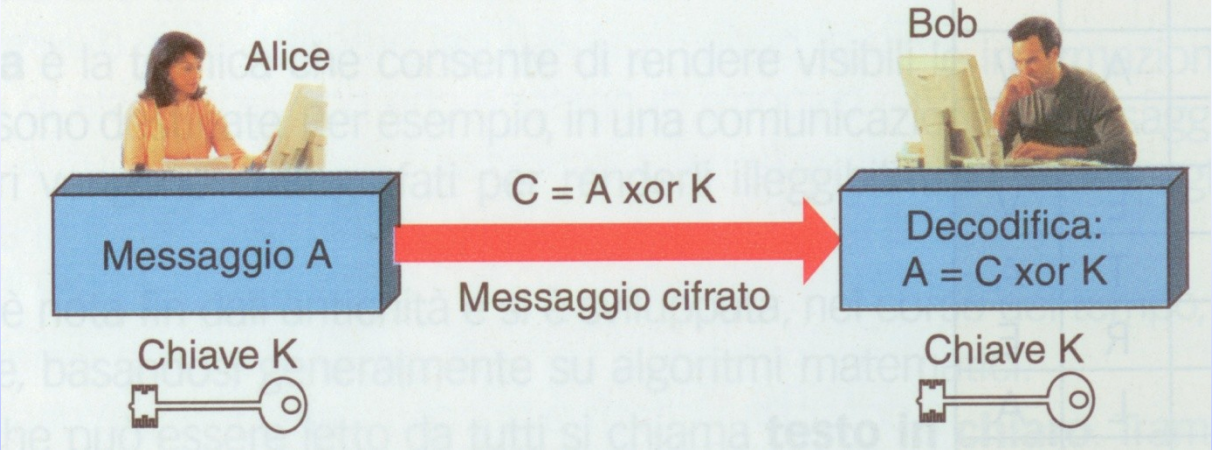
- Il mittente ed il destinatario **devono possedere la stessa chiave** (come per la tecnica di Giulio Cesare)
- L'operazione effettuata nella codifica e decodifica è l'operazione logica XOR
- L'algoritmo si basa sulla considerazione che applicando due volte l'operatore XOR si ottiene il messaggio di partenza

(A xor K) xor K = A

Operatore Logico XOR

XOR		
0	0	0
0	1	1
1	0	1
1	1	0

Crittografia a chiave simmetrica



A	1	1	0	0	1	1	0	1	0
K	1	0	1	1	1	0	0	0	1
Cif	0	1	1	1	0	1	0	1	1

Criptaggio

invio

Cif	0	1	1	1	0	1	0	1	1
K	1	0	1	1	1	0	0	0	1
A	1	1	0	0	1	1	0	1	0

Decriptaggio

(A xor K) xor K = A

Crittografia a chiave simmetrica

- La chiave può essere costituita da un numero molto grande di bit.
- Maggiore è il numero di bit utilizzati e maggiore sarà la sicurezza del sistema contro attacchi "esaustivi"
- Con chiave di 20 bit potrò avere 2^{20} chiavi e nell'ipotesi di riuscire a provare una chiave ogni millisecondo (1000 chiavi al secondo), sono necessari 1048 sec cioè 17 minuti per trovare la chiave giusta.
- Vista le crescenti potenze di calcolo, ad oggi viene ritenuta sicura una chiave a 128 bit
- DES → sistema di crittografia sviluppato dalla IBM 1970 a 56bit (3DES usa un numero di bit maggiore)
- CAST e IDEA → sviluppati negli anni 90' utilizzano chiavi a 128bit

- **Con questo sistema la segretezza della chiave è fondamentale, pertanto il problema di base è la distribuzione in sicurezza della chiave.**

Crittografia a chiave simmetrica

PROBLEMA

- Trovare un artificio per garantire la:
  - **Segretezza** (nessuno può leggere il messaggio se non il destinatario)
  - **Integrità** (nessuno può modificare un messaggio)
- Trovare un artificio per il trasferimento chiave in rete oppure
  - Non avere una chiave simmetrica comune

Crittografia a chiave simmetrica

SOLUZIONE (ARTIFICIO MACCHINOSO MA FUNZIONALE)

- Il mittente codifica con la sua chiave segreta (ch1) e invia il messaggio crittografato al destinatario
- Il destinatario codifica con la sua chiave segreta (ch2) e invia il messaggio "doppiamente" crittografato al mittente
- Il mittente decodifica con la sua chiave segreta (ch1) e rinvia il messaggio che sarà ancora crittografato al destinatario
- Il destinatario decodifica con la sua chiave segreta (ch2) ottenendo il messaggio in chiaro.

Vantaggi

- Si è avuto quindi la segretezza del messaggio (nessuno ha potuto leggere il messaggio in chiaro se non il mittente ed il destinatario)
- Il messaggio è integro (nessuno modifica può essere stata fatta da altri)

Svantaggi

- Non ci sarà mai la garanzia dell'identità del mittente.

Evoluzione

- Si potrebbe inviare la chiave segreta (CH) utilizzando la tecnica sopra esposta per favorire le comunicazioni successive. (Ma allora avremmo avuto una chiave condivisa da due persone, siamo sicuri che non viene data ad altri?)

Crittografia a chiave asimmetrica
(anche detta a chiave pubblica)

- Introdotta nel 1975 con l'obiettivo di risolvere il problema della distribuzione sicura delle chiavi
- Si utilizzano una coppia di chiavi:
  - Una **chiave pubblica**
  - Una **chiave privata**
- I messaggi codificati con la chiave pubblica possono essere decodificati solo con la chiave privata corrispondente.
  I messaggi codificati con la chiave privata possono essere decodificati solo con la chiave pubblica corrispondente.

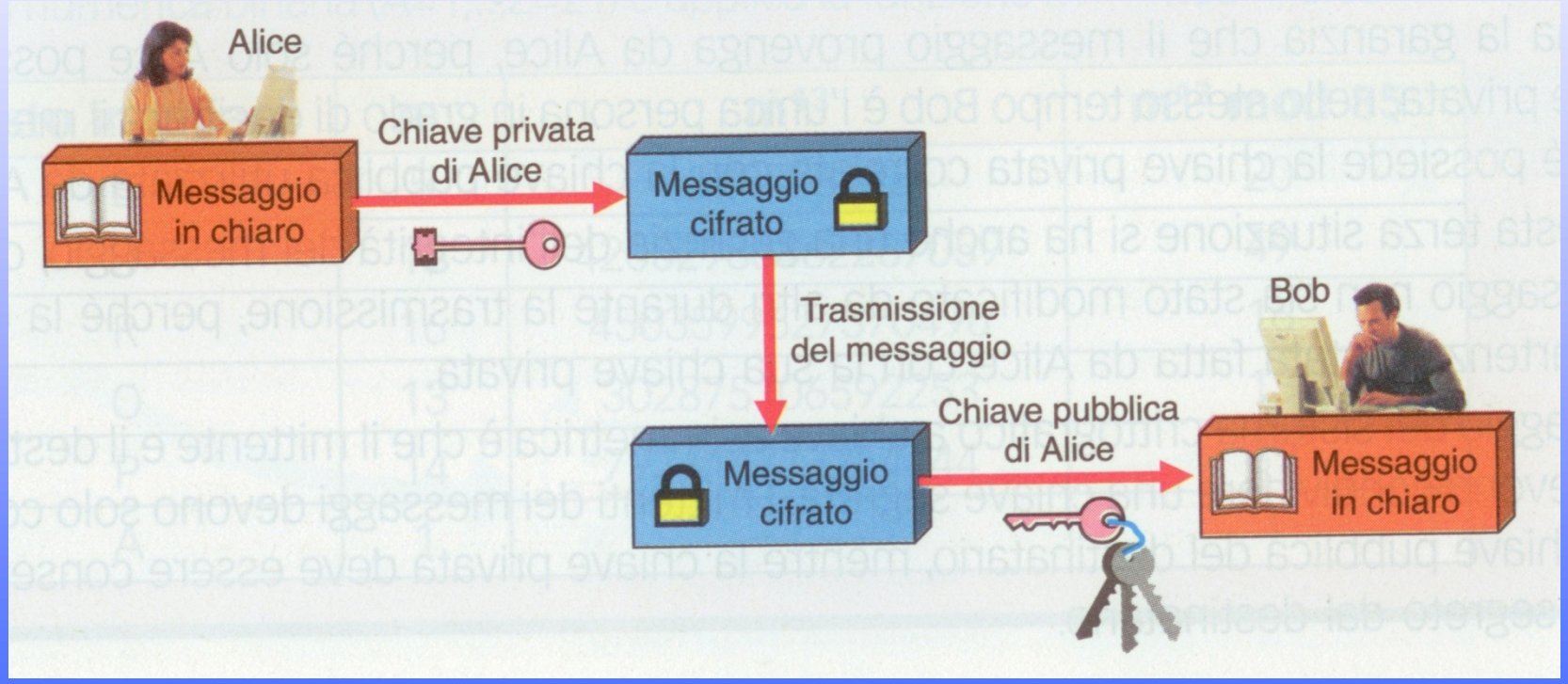
- Ogni utente che ha la necessità di comunicare in modo cifrato richiede le due chiavi ad un ente garante che grazie ad un software specifico le produce.
- L'utente tiene segreta la chiave privata (lui e solo lui), mentre la chiave pubblica la può tranquillamente distribuire.
  Nota: dalla chiave pubblica non è possibile risalire alla chiave privata

Crittografia a chiave asimmetrica
(anche detta a chiave pubblica)

- Diversi modi di utilizzare la chiave pubblica e la chiave privata determinano diversi livelli di sicurezza:
  - **Garanzia dell'identità del mittente**
    (nessuno può inviare messaggi appropriandosi dell'identità altrui anche se tutti possono leggere il messaggio)
    Implicitamente è **garantita l'integrità** del messaggio.
  - **Garanzia della segretezza**
    (solo il destinatario del messaggio può leggere il messaggio ma potrebbe essere stato inviato o modificato da chiunque)
    Non è garantita l'integrità del messaggio.
  - **Garanzia** sia dell'**identità** che della **segretezza** oltre alla **integrità** del messaggio.

Crittografia a chiave asimmetrica
(anche detta a chiave pubblica)

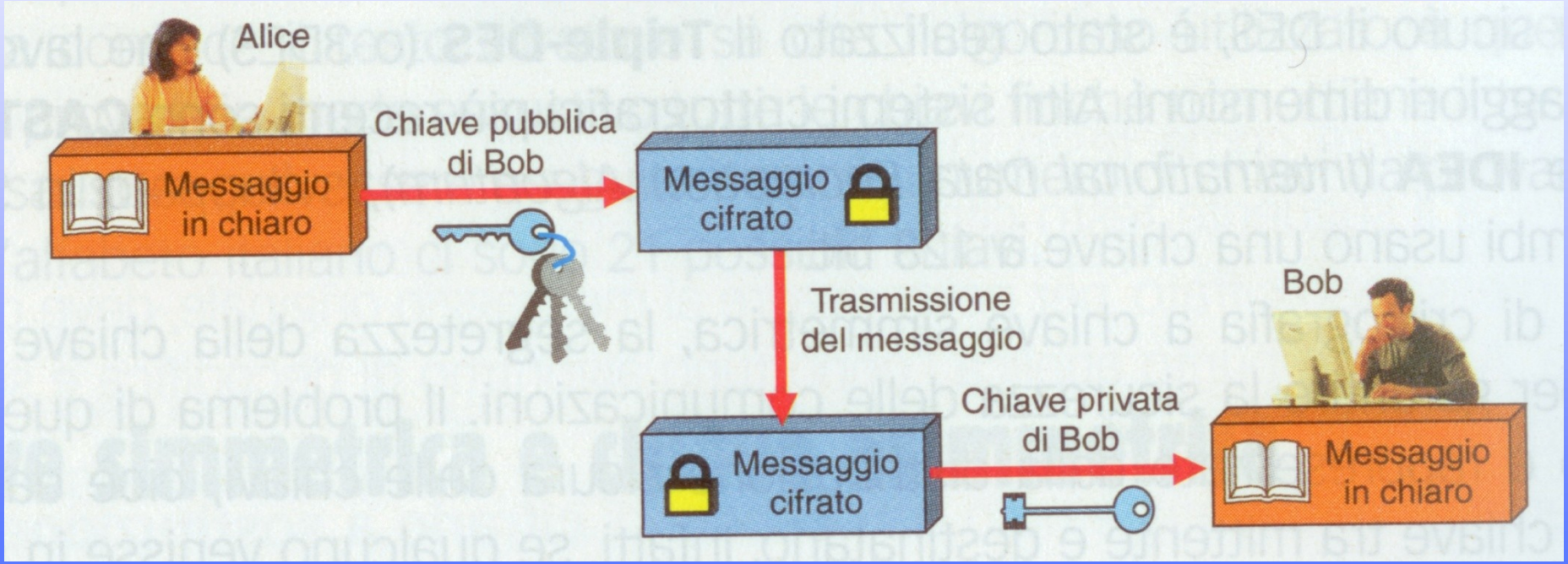
- **Garanzia dell'identità del mittente**
  (nessuno può inviare messaggi appropriandosi dell'identità altrui anche se tutti possono leggere il messaggio)



Alice non ha la certezza che l'unico a leggere il messaggio è Bob
Bob è sicuro che il messaggio proviene da Alice
(Implicitamente **è garantita anche l'integrità** del messaggio)

Crittografia a chiave asimmetrica
(anche detta a chiave pubblica)

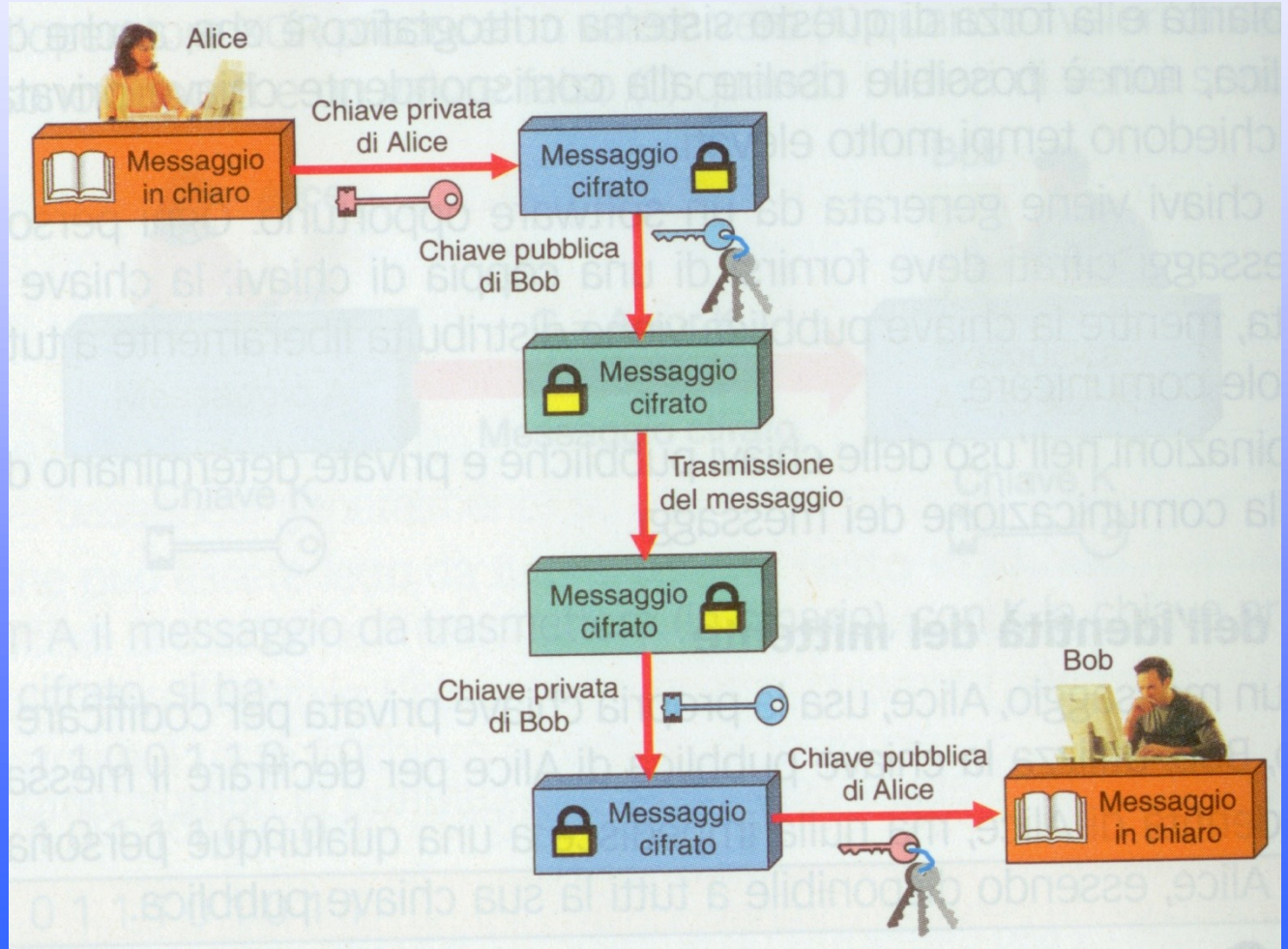
- **Garanzia della segretezza**
  (solo il destinatario del messaggio può leggere il messaggio ma potrebbe essere stato inviato da chiunque)



Alice è sicura che il suo messaggio può essere letto solo da Bob
Bob non ha la certezza che Alice gli abbia effettivamente mandato il messaggio
(**Non è garantita l'integrità** del messaggio)

Crittografia a chiave asimmetrica
(anche detta a chiave pubblica)

- Garanzia sia dell'**identità** che della **segretezza** implicitamente anche della **integrità**



Firma digitale

- Metodo che consente ad una persona di apporre un segno distintivo ad un documento inviato
- Un destinatario può verificare che il documento ricevuto è stato effettivamente spedito da una persona e che non è stato modificato da terzi
- Viene garantita:
  - **Autenticità (garanzia dell'identità del mittente)**
  - **Integrità (è possibile verificare se il documento firmato è stato manomesso)**

- La firma digitale viene realizzata utilizzando la tecnica a chiave asimmetrica anche se in questo contesto l'uso della chiave privata e pubblica assume un ruolo diverso rispetto a quello visto per la crittografia.

Firma digitale

- Dato un Documento da firmare, viene prima di tutto generata un'"impronta" (fingerprint) cioè una sequenza di bit (128 o 160 bit) che rappresenta un sorta di riassunto del documento (digest)

- Per la produzione del "**digest**" viene utilizzata una funzione specifica detta "**funzione di hash**" che a partire da documenti diversi produce sempre un'impronta diversa

- Il "digest" viene criptato con l'utilizzo della chiave privata del mittente e costituisce la "**firma digitale del documento**"

- Il documento "in chiaro" unito alla "firma digitale" viene inviato al destinatario (documento con firma digitale).

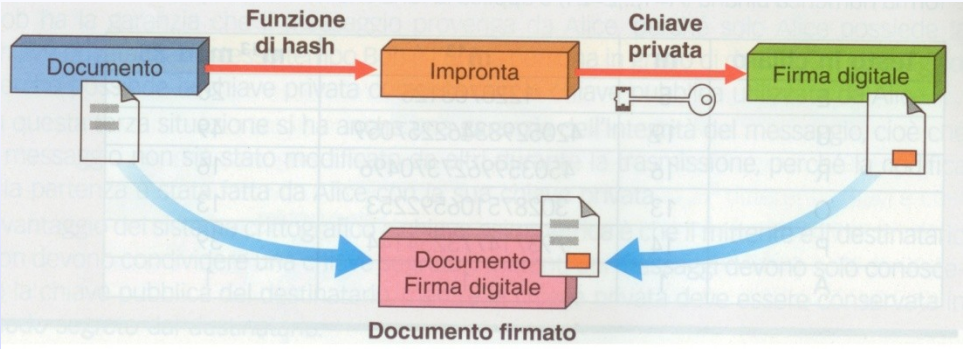
Firma digitale

- Chiunque può ricevere il documento firmato e verificarne l'autenticità e l'integrità

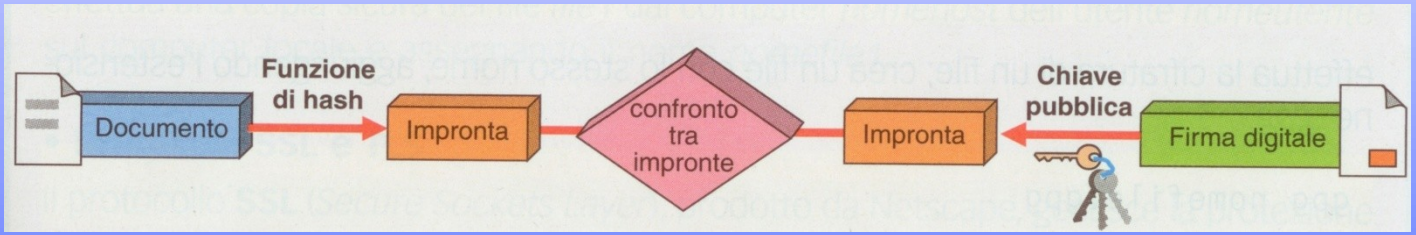
- Il destinatario:
  - Utilizzando la parte del "documento firmato" che costituisce il "documento in chiaro" e con l'utilizzo della "funzione di hash" riproduce l'impronta.
  - Utilizzando la firma digitale la decodifica servendosi della chiave pubblica del firmatario, riproducendo così l'impronta
  - Effettua un confronto: se il confronto fra le due impronte ottenute da esito positivo, avrà la certezza dell'autenticità e dell'integrità del documento ricevuto.

Firma digitale

Mittente



Destinatario



- La coppia di chiavi deve essere rilasciata da un "**ente di certificazione**" che garantisce l'identità del possessore
- Spesso vengono utilizzate le "Smart-Card" per la conservazione della chiave privata.
- In prospettiva le Carte di Identità conterranno la chiave privata di ogni cittadino.