Anna Vaccarelli
Istituto di Informatica e Telematica
anna.vaccarelli@iit.cnr.it

STeP

La crittografia

La crittologia

- **Crittologia:** dal greco kryptós lógos che significa "parola nascosta"
- **Crittografia:** è la disciplina che si occupa di individuare algoritmi per trasformare in modo reversibile un messaggio o un documento in modo che il significato sia comprensibile solo per determinate persone
- **Criptoanalisi:** è la disciplina che studia come violare i meccanismi della crittografia
- L'insieme delle due discipline costituisce la crittologia

La crittografia

- Dal greco Kryptos = segreto
  Gràfein = scrivere
- È una scienza antichissima: sono noti molti esempi di "scritture segrete" presso:
  - Assiri e Babilonesi
  - Antico Iraq (sostituzione di nomi con numeri)
  - Thailandia: diverse tecniche di cifratura
    - Sostituzione
    - Divisione delle lettere dell'alfabeto in gruppi
    - Ogni lettera è indicata dal numero di gruppo e dalla posizione nel gruppo

La crittografia

- Dal greco Kryptos = segreto
  Gràfein = scrivere
- È una scienza antichissima: sono noti molti esempi di "scritture segrete" presso Assiri e Babilonesi e Antico Iraq (sostituzione di nomi con numeri)
- Ci sono esempi che risalgono all'epoca di Sparta (IX sec. A.C. -- 400 a.C.)
- Giulio Cesare fu abile inventore di codici di crittografia
- In tempi recenti la crittografia è stata molto usata nello spionaggio tra USA e URSS
- A molti è nota come "protagonista" di film e libri di spionaggio – macchina Enigma

Esempi di ‘scritture segrete‘

- **Scitala lacedemonica**

  (Licurgo IX sec. a.C. – Lisandro 400 a.C.)

  - **Consisteva in un bastone su cui si avvolgeva ad elica un nastro di cuoio; sul nastro si scriveva per colonne parallele all'asse del bastone, e lettera per lettera, il testo segreto**

  - **Tolto il nastro dal bastone il testo vi risultava trasposto in modo regolare ma sufficiente per evitare la lettura senza un secondo bastone uguale al primo**

La macchina Enigma (1)

- Adottata dall'esercito e dalla marina tedesca fino alla seconda guerra mondiale
- La macchina ha al suo interno un certo numero di rotori collegati elettricamente e liberi di ruotare
- Premendo la A un segnale elettrico passa da rotore a rotore fino al rotore finale e quindi torna indietro fino a mostrare una lettera illuminata che è il carattere cifrato
- Non esiste possibilità di stampa, dunque l'operatore deve copiare a mano, carattere per carattere il messaggio cifrato da trasmettere

La macchina Enigma (2)

- La chiave di Enigma è la disposizione iniziale dei rotori; questa chiave veniva cambiata ogni 24 ore secondo una regola prefissata (chiave segreta)
- I tedeschi erano convinti che Enigma fosse inattaccabile
- Negli anni '30 matematici polacchi guidati da Marian Rejewski erano riusciti a ricostruire la struttura dei rotori e a decrittarne i messaggi
- Il servizio crittografico inglese al quale partecipava anche il famoso matematico Alan Turing riuscì a sua volta a forzare Enigma
- Debolezza: Enigma è una macchina simmetrica, nel senso che se la lettera A è cifrata con la G in una certa posizione del testo allora nella stessa posizione la G sarà cifrata con la A

Marian
REJEWSKY
(1905-1980)

Alan
TURING
(1912-1954)

Steganografia

- Steganografia: dal greco greca, "stèganos" = nascosto e "gràfein" = scrivere. E' il sistema di nascondere un messaggio segreto all'interno di un altro, di significato completamete diverso e non sospetto

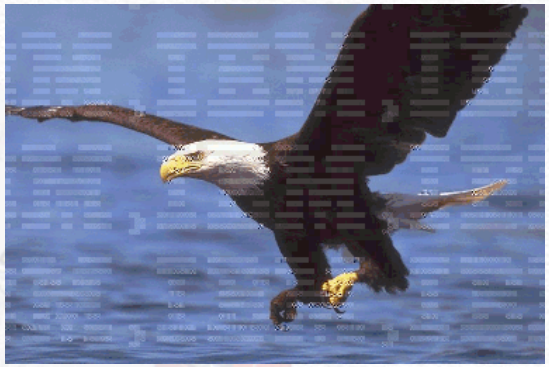
- È spesso confusa con la crittografia, ma sono due tecniche diverse
  - Crittografia: nasconde il contenuto di un messaggio
  - Steganografia: nasconde il messaggio stesso

Steganografia

- Gli antichi romani usavano scrivere fra le linee utilizzando un inchiostro fatto con sostanze naturali come il succo di limone o il latte, che venivano letti esponendo il foglio al calore di una fiamma

Steganografia

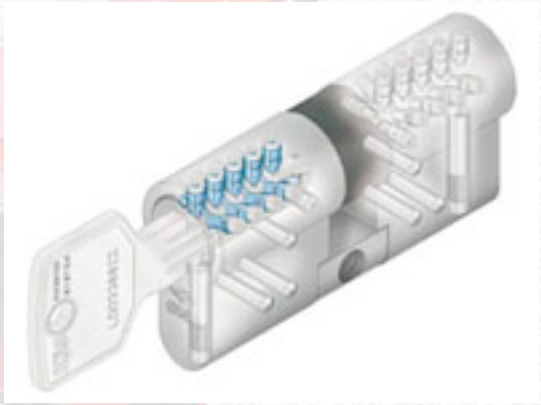
- La steganografia moderna si basa principalmente su due concetti:
  - Un file può contenere, entro certi limiti, delle informazioni nascoste senza perdere funzionalità
  - Sfrutta l'ncapacità dell'occhio umano a percepire piccolissime variazioni di colore e qualità



- Su questo sistema si basa le tecnica per proteggere il copyright in immagini e file audio, più comunemente conosciuto come Digital Watermarking

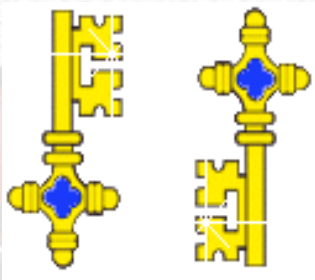
La crittografia moderna

- **Cifratura:** trasformazione di un testo in chiaro in un testo cifrato
- **Decifratura:** trasformazione di un testo cifrato in un testo in chiaro
- Trasformazione basata in genere su:
  - Chiave
  - Algoritmo (procedimento ben definito e pubblico)
- La sicurezza si basa su:
  - Segretezza della chiave
  - Robustezza dell'algoritmo



Cifratura e decifratura

Algoritmi a chiavi simmetriche

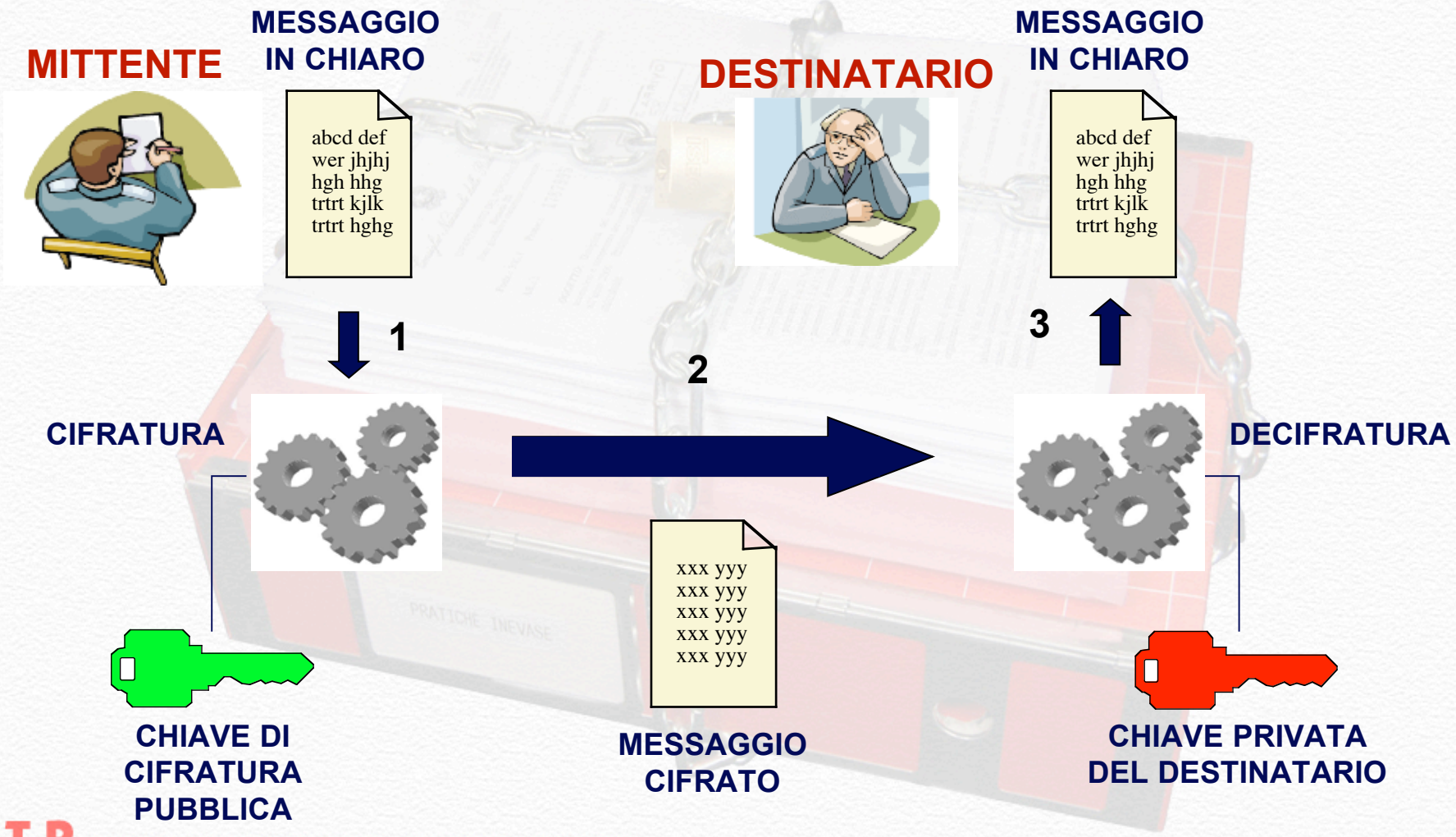


- Stessa chiave per cifratura e decifratura (DES – 64 / 128 bit)
- Segretezza della chiave
- Vantaggi:
  - Algoritmi “veloci” per cifrare e decifrare
- Svantaggi:
  - Preliminare scambio della chiave segreta
  - Per una comunità di n utenti sono necessarie ~ n^2 chiavi

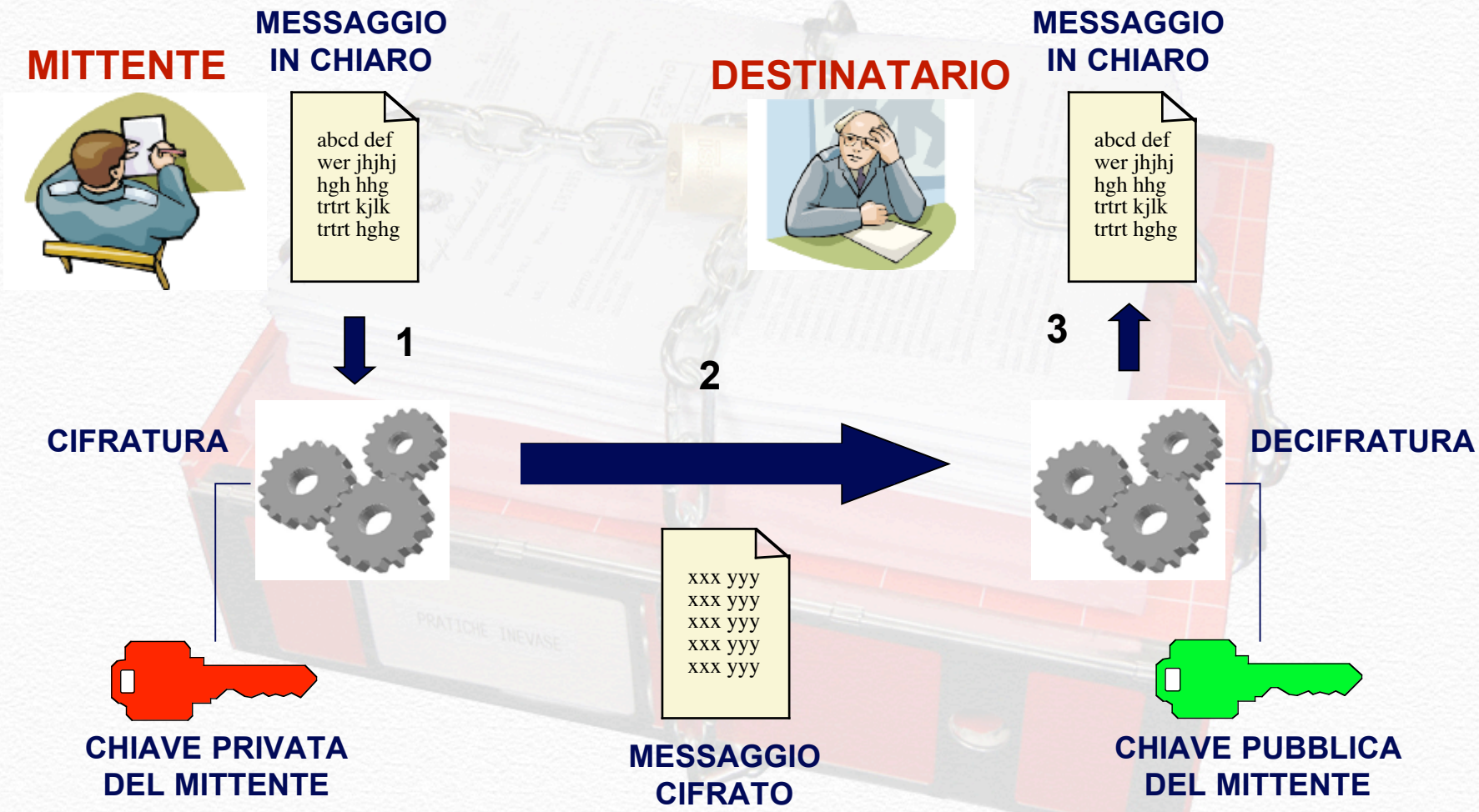
Algoritmi a chiavi asimmetriche

- 2 chiavi diverse: cifratura e decifratura (RSA/DSA - 1024/2048 bit)
- Ogni corrispondente:
  - Chiave privata: segreto da custodire
  - Chiave pubblica: informazione da diffondere
- Ogni chiave può essere usata indifferentemente per cifrare o decifrare
- Vantaggi: flessibilità (riservatezza, autenticità, integrità)
- Svantaggi: algoritmi “lenti”

Riservatezza di un messaggio



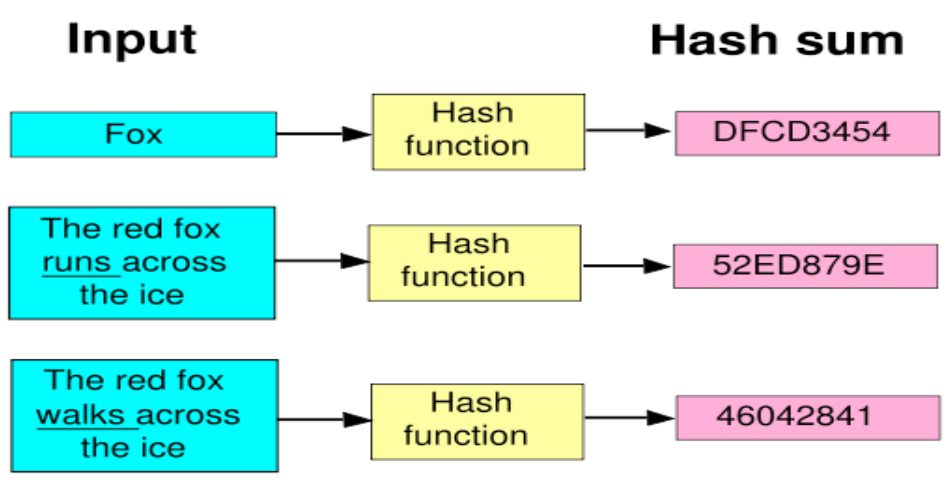
Autenticità e integrità



Autenticità e riservatezza

Funzioni di Hash

- H è tale che data una stringa in ingresso x di qualunque lunghezza, H genera una stringa in uscita di lunghezza fissata h=H(x) (digest)
- Hanno le seguenti proprietà:
  - H(x) è relativamente facile da ottenere dato un qualunque x
  - H(x) è una trasformazione "a senso unico" (one-way), cioè dato h=H(x) è computazionalmente molto impegnativo ricavare x



La firma digitale …

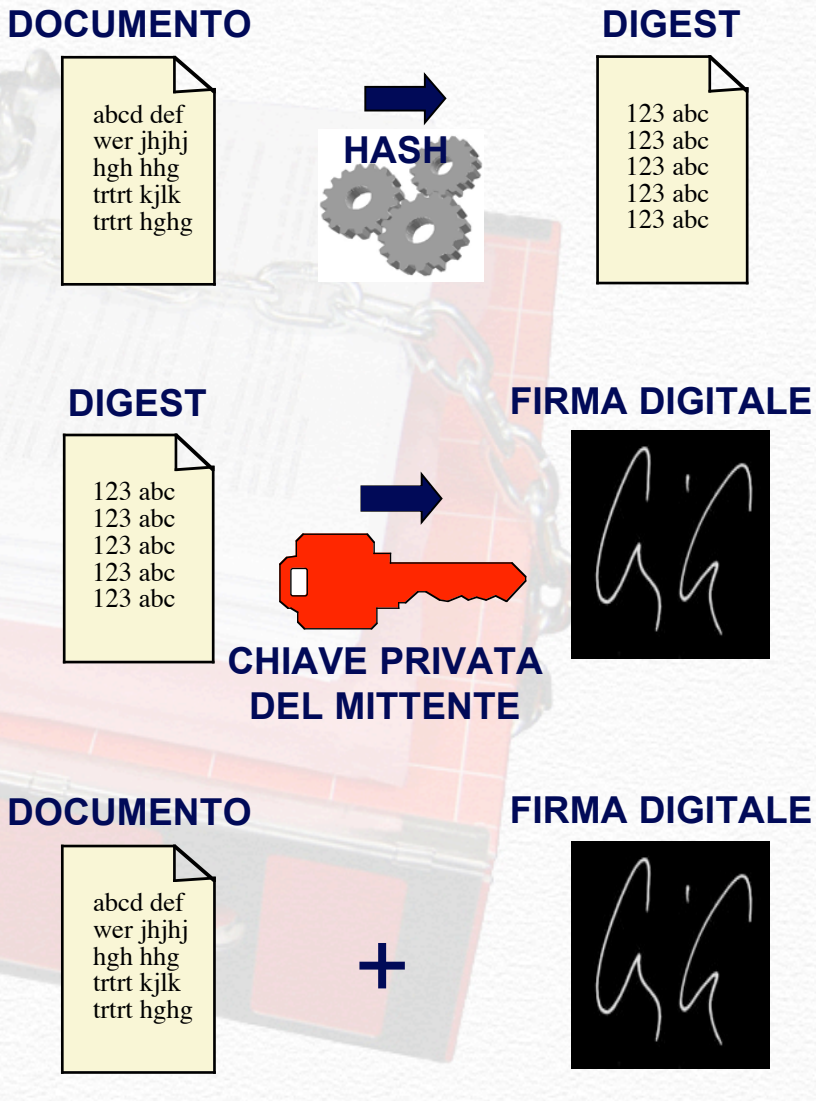
- È una procedura informatica basata sugli algoritmi di crittografia a chiavi asimmetriche

Requisiti

- La firma digitale deve poter essere facilmente prodotta dal legittimo firmatario
- Nessun utente deve poter riprodurre la firma di altri
- Chiunque deve poter facilmente verificare una firma

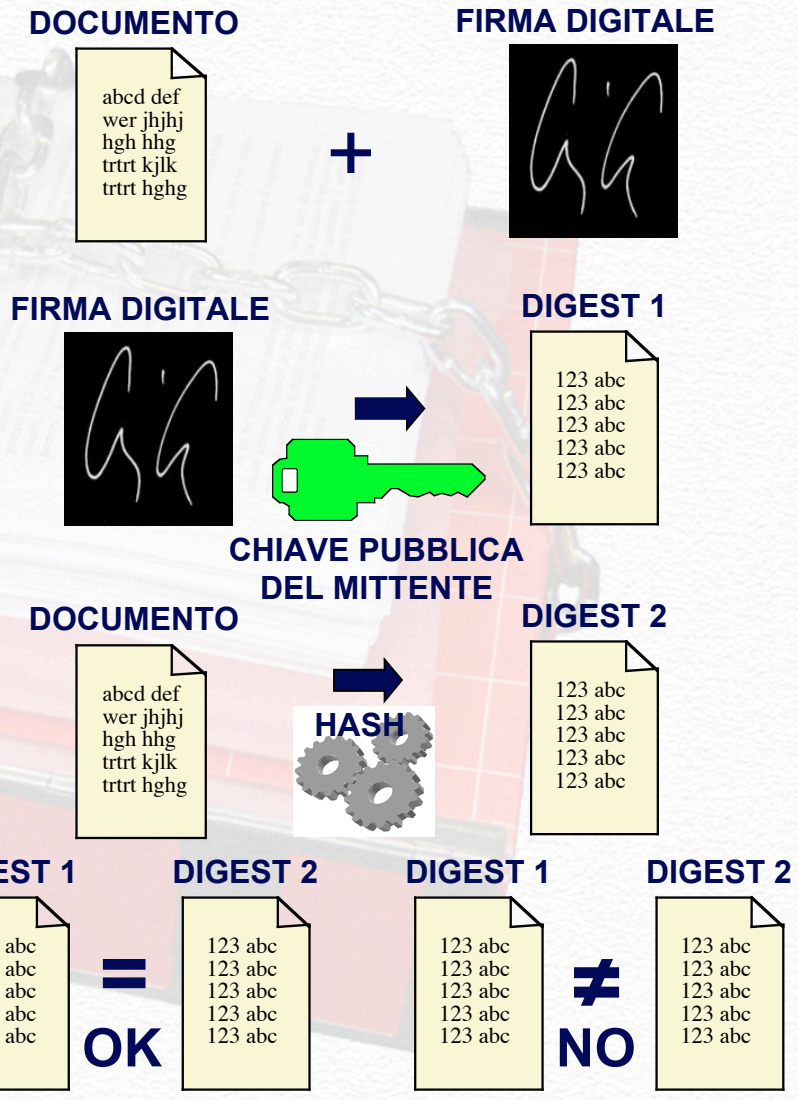
Generazione della firma

- Calcolare il **DIGEST** del documento
- **CIFRARE** il digest con la chiave privata del mittente (si ottiene così la firma digitale)
- Aggiungere al documento originale la firma digitale ottenuta al passo precedente e inviare la coppia (Messaggio, Firma)



Verifica della firma

- Separare il messaggio dalla firma
- Decifrare la firma usando la chiave pubblica del mittente
- Applicare al documento la funzione di Hash cioè calcolare il digest
- Verificare che i due risultati coincidano
  - SI: accetto il documento
  - NO: rifiuto il documento poiché è stato manomesso



La firma digitale

- Generata dal mittente utilizzando la sua chiave privata
  - Autenticità
- Verificata dal destinatario
  - Confronto tra il digest ricevuto e quello da lui generato
  - Integrità ed autenticità
- Se è necessaria la riservatezza: cifratura con
  - Chiave pubblica del destinatario
  - Chiave simmetrica stabilita tramite scambio di messaggi riservati

Garanzie

- Autenticità del mittente
- Integrità del messaggio durante il percorso mittente/destinatario
- NON garantisce la riservatezza

CERTIFICATI DIGITALI E CERTIFICATION AUTHORITY

STATE of WASHINGTON

SECRETARY of STATE

I, RALPH MUNRO, Secretary of State of the State of Washington and custodian of its seal,

hereby issue this

RECOGNITION OF REPOSITORY

to

VeriSign, Inc.

I FURTHER CERTIFY that the records on file in this office show that the above named repository was recognized under the laws of the State of Washington on January 21, 2000.

I FURTHER CERTIFY that the recognition of repository hereby issued is valid for a period of one (1) calendar year, unless revoked or suspended prior to that date, and is subject to any classifications reflected on the records of this office.

Date: January 21, 2000

Given under my hand and the Seal of the State of Washington at Olympia, the State Capital

RALPH MUNRO

Ralph Munro, Secretary of State

La “Certification Authority”

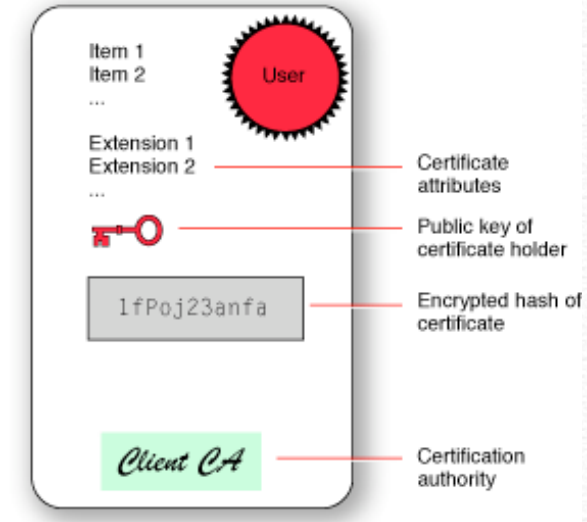
- Chi garantisce che la chiave pubblica trascritta su un registro pubblico ed abbinata a Bob sia stata rilasciata proprio a Bob?
- E' necessaria una terza parte fidata: il "soggetto certificatore" o “Certification Authority (CA)”
- La Certification Authority certifica il legame chiave pubblica/identità

Il certificato digitale

- **Un documento di identità:**
  - **Associa l'identità di una persona (nome, cognome, data di nascita…) al suo aspetto fisico (foto)**
  - **È emesso da una autorità riconosciuta**

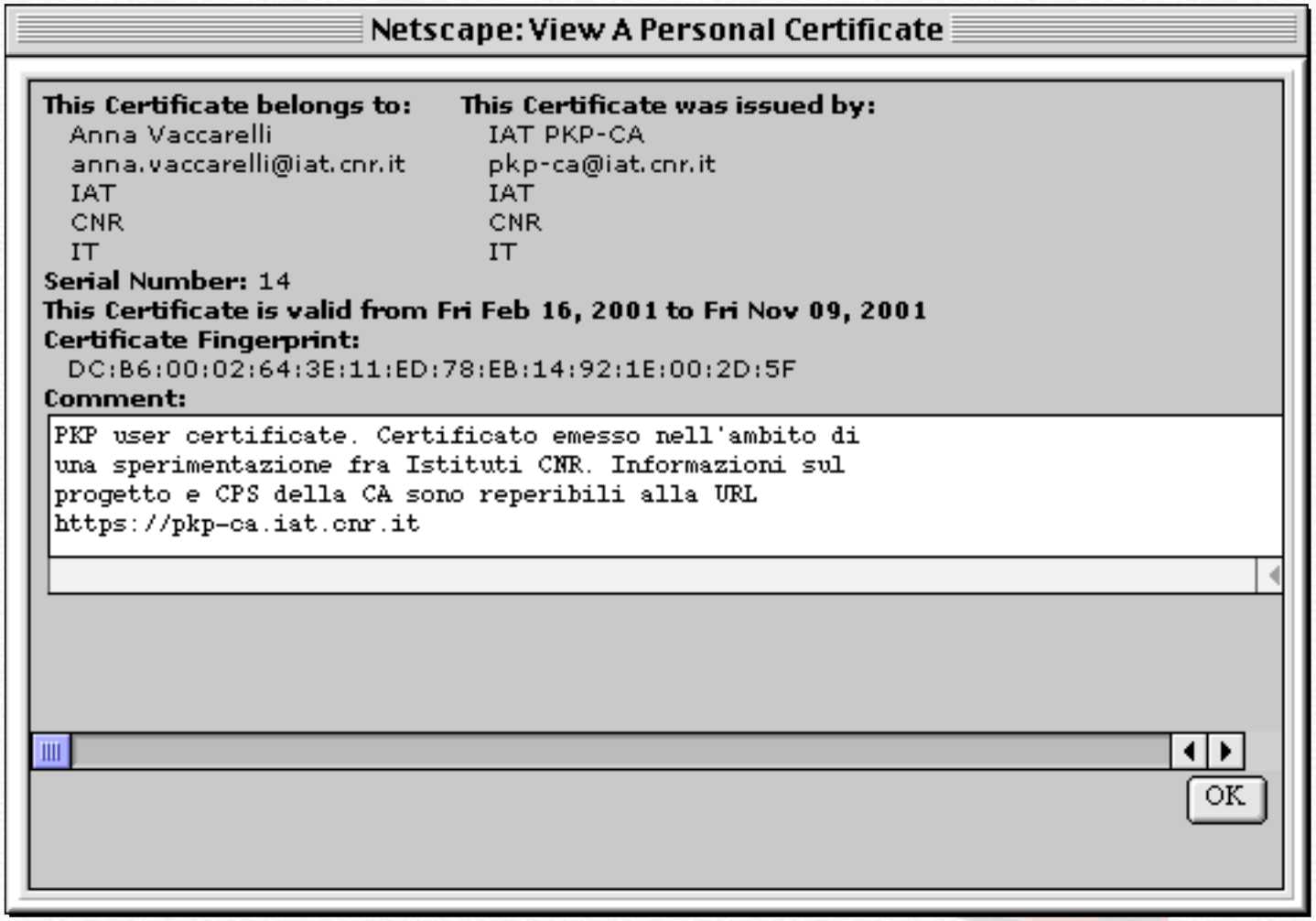
Il certificato digitale

- E’ un documento elettronico
- Associa l’identità di una persona ad una chiave pubblica
- Emesso, secondo standard internazionali (X.509 raccomandato dall'ITU-T (International Telecommunication Union - settore Telecomunicazioni), da una CA riconosciuta
- Firmato digitalmente con chiave privata della CA



L'Istituto Informatica e Telematica

Il certificato X.509



Compiti di una CA

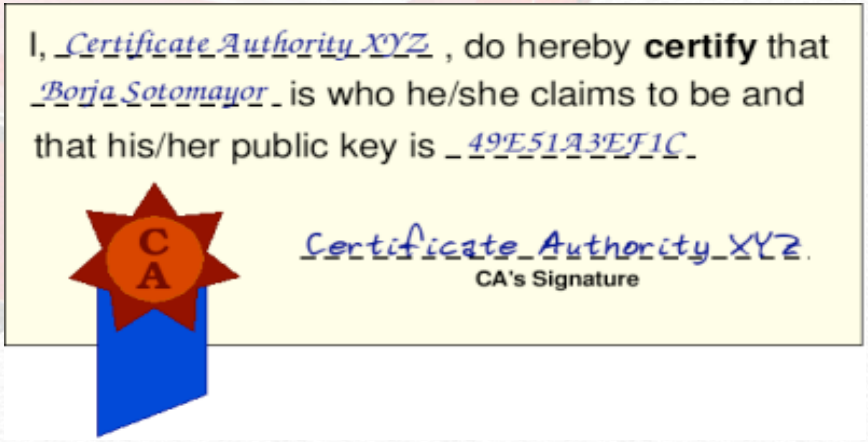
- Identificare con certezza la persona che fa richiesta della certificazione della chiave pubblica
- Rilasciare e rendere pubblico il certificato
- Garantire l'accesso telematico al registro delle chiavi pubbliche
- Informare i richiedenti sulla procedura di certificazione e sulle tecniche per accedervi
- Dichiarare la propria politica di sicurezza

Compiti di una CA

- Attenersi alle norme sul trattamento di dati personali (non rendersi depositario delle chiavi private)
- Procedere alla revoca o alla sospensione dei certificati in caso di richiesta dell'interessato o essendo a conoscenza di abusi o falsificazioni, ecc.
- Rendere pubblica la revoca o la sospensione delle chiavi (CRL)
- Assicurare la corretta manutenzione del sistema di certificazione

Come ottenere un Certificato Digitale

- La CA provvede ad autenticare il richiedente, di solito richiedendo di recarsi di persona ad uno sportello di LRA (Local Registration Authority) collegato con la CA
- Verificata l'identità, la CA emette il certificato, lo invia al richiedente tramite posta elettronica ed inserisce la chiave certificata nel registro delle chiavi pubbliche
- Procedure di richiesta e gestione dei certificati sono gestite da Infrastrutture a Chiave Pubblica (PKI - Public Key Infrastructure)

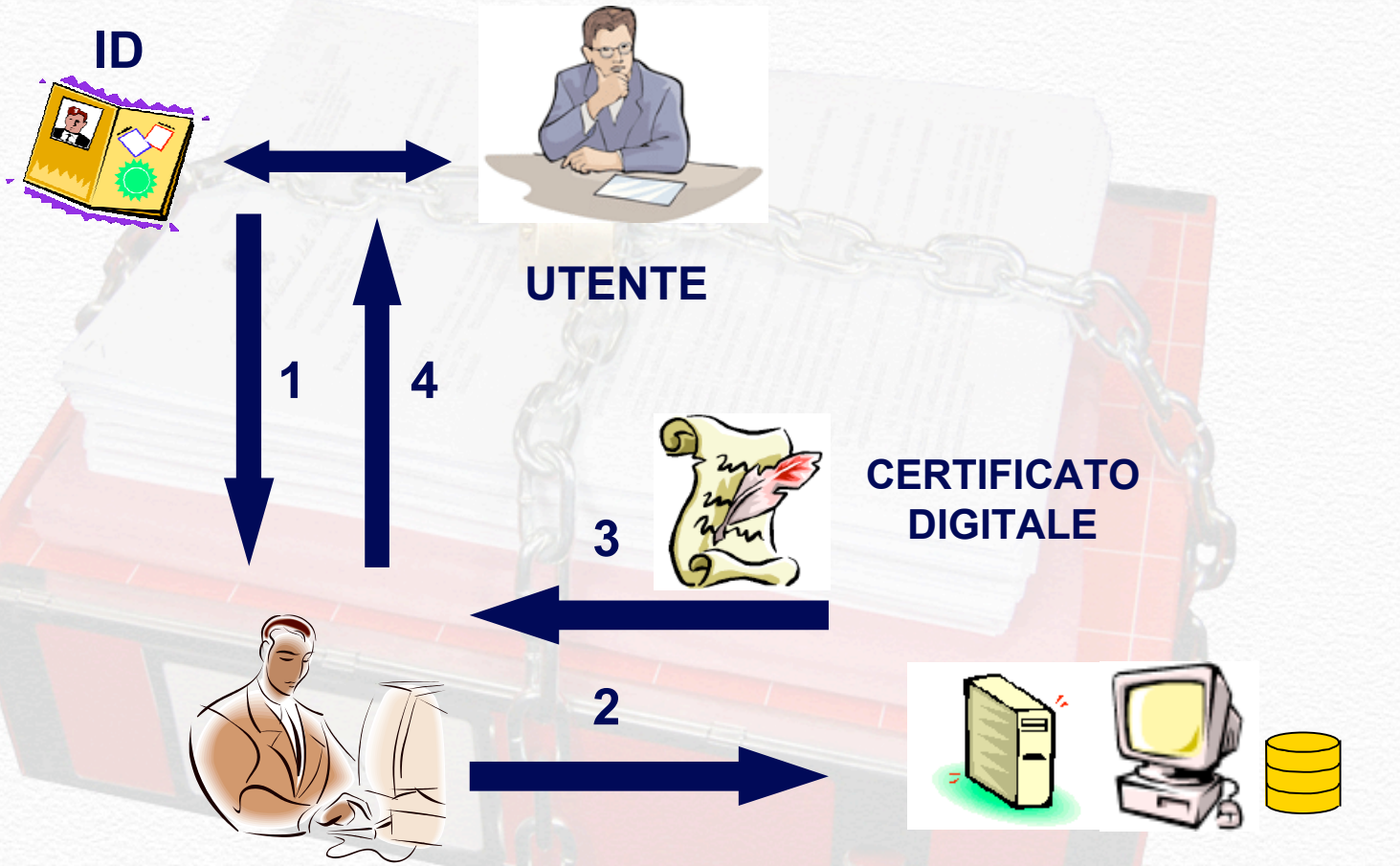


La Public Key Infratructure (PKI)

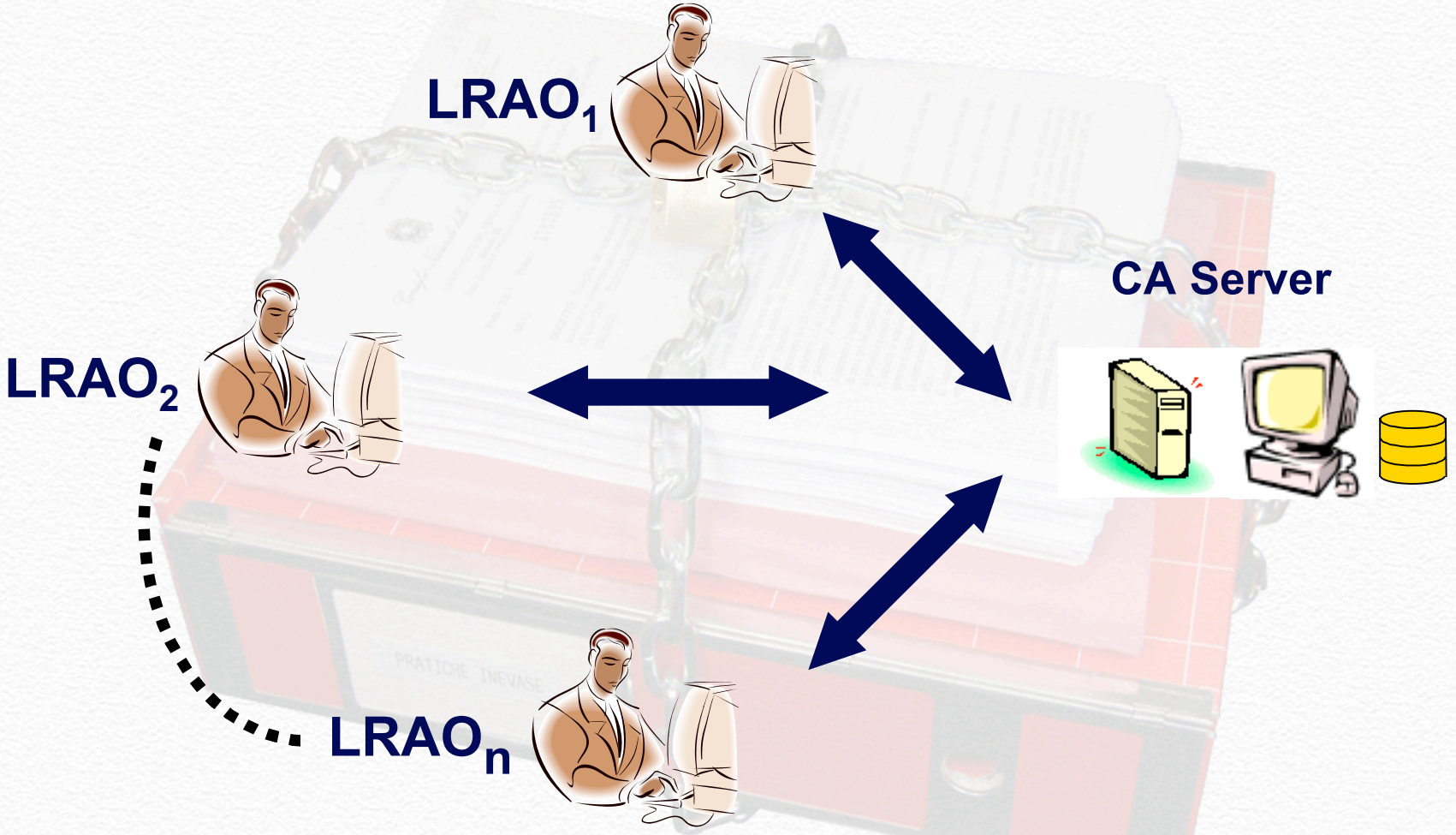
La Public Key Infrastructure (PKI)

- La struttura minima di una PKI è costituita da una CA e un Local Registration Authority (LRA)
- LRA è uno “sportello” con un operatore (LRAO) che effettua il riconoscimento personale del richiedente. A seguito del riconoscimento effettuato da LRAO, la CA emette il certificato
- Ogni CA può avere più di un LRA

Schema di base di una PKI

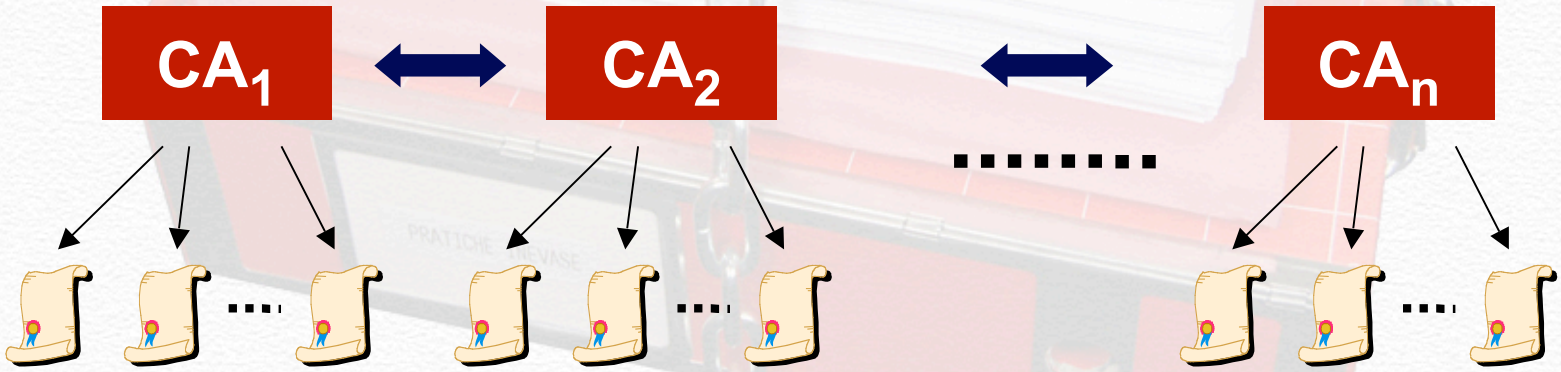


Schema di PKI con più LRA



La Public Key Infrastructure (PKI)

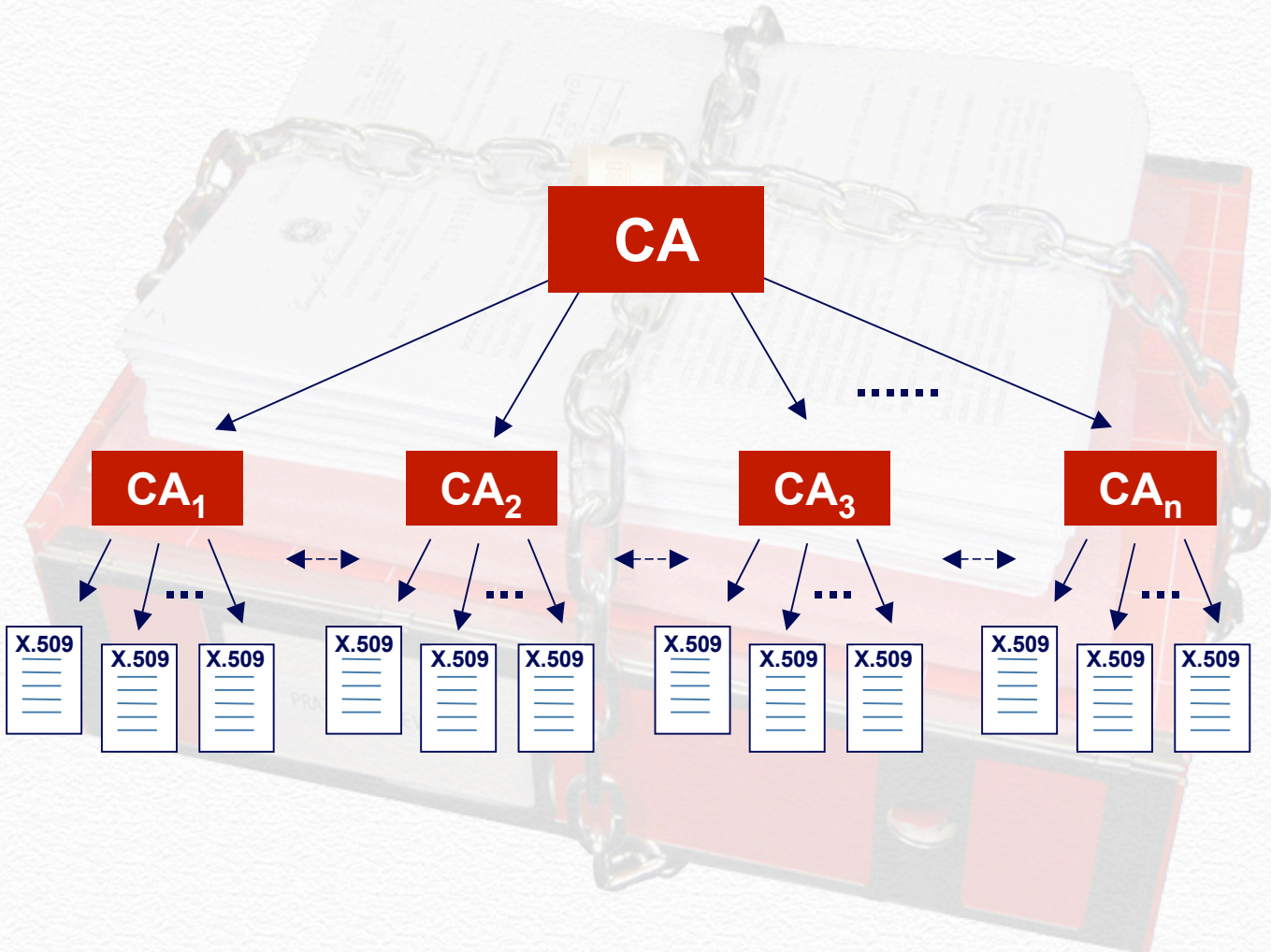
- Le CA possono certificarsi a vicenda, in modo da stabilire una “catena di fiducia”



La Public Key Infrastructure (PKI)

- Molto spesso la struttura della catena di fiducia è ad albero, in cui la CA principale (Root CA) certifica le chiavi di CA subordinate. A loro volta esse possono certificarne altre (fino a certificare la chiave pubblica del singolo utente).

Schema gerarchico di PKI



La crittografia

...E ci sarebbe ancora molto da dire

Ma (per fortuna?) non c'è tempo...