Università degli Studi di Cagliari
Corso di Laurea in Ingegneria Elettronica

ELEMENTI DI INFORMATICA

http://agilegroup.eu

A.A. 2015/16

Docente: **Michele Marchesi**

SICUREZZA INFORMATICA

Sommario

- **Sicurezza informatica**
  - **definizioni**
  - **malware, virus, worms, trojans, anti-virus**
  - **attacchi informatici**
- **Crittografia**
  - **storia**
  - **algoritmi di cifratura simmetrica e asimmetrica**
  - **applicazioni: protocolli, firma digitale, criptovalute**

Sicurezza informatica

- **Riguarda l'utilizzo sicuro dei calcolatori e delle reti**
- **Sicurezza rispetto a:**
  - **intrusioni nel proprio computer**
  - **accesso a dati riservati**
  - **perdita di dati**
  - **distruzione di servizi**
  - **furti di identità**

Concetti di base

- **utenti**: persone opportunamente identificate
- **risorse**: entità a cui alcuni utenti hanno l'abilitazione ad accedere:
  - **hardware**
  - **software**
  - **reti**
  - **dati**

Caratteristiche della sicurezza

- **Disponibilità:**
  - le varie risorse devono essere sempre reperibili e accessibili agli utenti
- **Riservatezza:**
  - le varie risorse devono essere accessibili solo agli utenti autorizzati e preservate da accessi impropri
- **Integrità:**
  - i dati e i programmi devono essere identici agli originali, e modificabili solo dagli utenti autorizzati
  - i dati e i programmi devono essere protetti da perdite dovute a guasti

Terminologia

- **Rischio**: una situazione in cui un'organizzazione risulta esposta a danni, diretti o indiretti, alle proprie risorse
  - Ad es.: accesso non autorizzato al proprio conto corrente bancario
  - cancellazione/alterazione di informazioni importanti
- **Minaccia**: un elemento esterno, di solito umano, che rappresenta una minaccia per le risorse
  - Ad es.: una spia che cerca di accedere a dati strategici
- **Vulnerabilità**: una carenza di protezione del sistema
  - Ad es.: errori nelle applicazioni software
  - errori di installazione della rete
- **Attacco**: la minaccia sfrutta una vulnerabilità del sistema per trasformare un rischio in un danno reale

Tipi di attacchi informatici

- **Malware**: programmi inseriti in modo fraudolento sui computer, per causare danni più o meno gravi
  - in ogni caso, consumano risorse (disco, memoria, CPU, banda di rete) in modo abusivo
- **Social engineering**: "attacchi" effettuati direttamente sulle persone, per carpire dati informatici
- **Phishing**: truffe online per acquisire dati sensibili
- **Attacchi sulla rete**: per disabilitare servizi o carpire informazioni

Malware – Virus

- Sono parti di codice che si diffondono copiandosi all'interno di altri programmi (di vario tipo), o sul settore di “boot” del disco
- Sono eseguiti ogni volta che il file infetto viene aperto
- Se eseguiti, cercano sul computer altri programmi da infettare, e si diffondono su questi – possono anche eseguire altre azioni, più o meno dannose
- Si trasmettono da un computer a un altro tramite lo spostamento di file infetti ad opera degli utenti
- Possono infettare file del sistema operativo
- Possono usare tecniche “furtive” (stealth) o di mutazione per evitare di essere riconosciuti

Malware – Worm

- Malware che si replica, di solito sfruttando Internet
- E' un programma completo che si installa nella macchina ospite, ed è eseguito quando parte il S.O.
- Spesso ha un *payload*, codice per effettuare azioni specifiche, dannose o di reperimento informazioni
- Sono la base per la creazione di:
  - **backdoor**: per dare accesso al computer ad altri
  - **zombie o bot**: computer controllati da fuori, che possono essere attivati insieme per eseguire attacchi
- Esempio: Conficker, che ha infettato 15 milioni di PC in 200 paesi nel 2009, sfruttando una falla di Windows

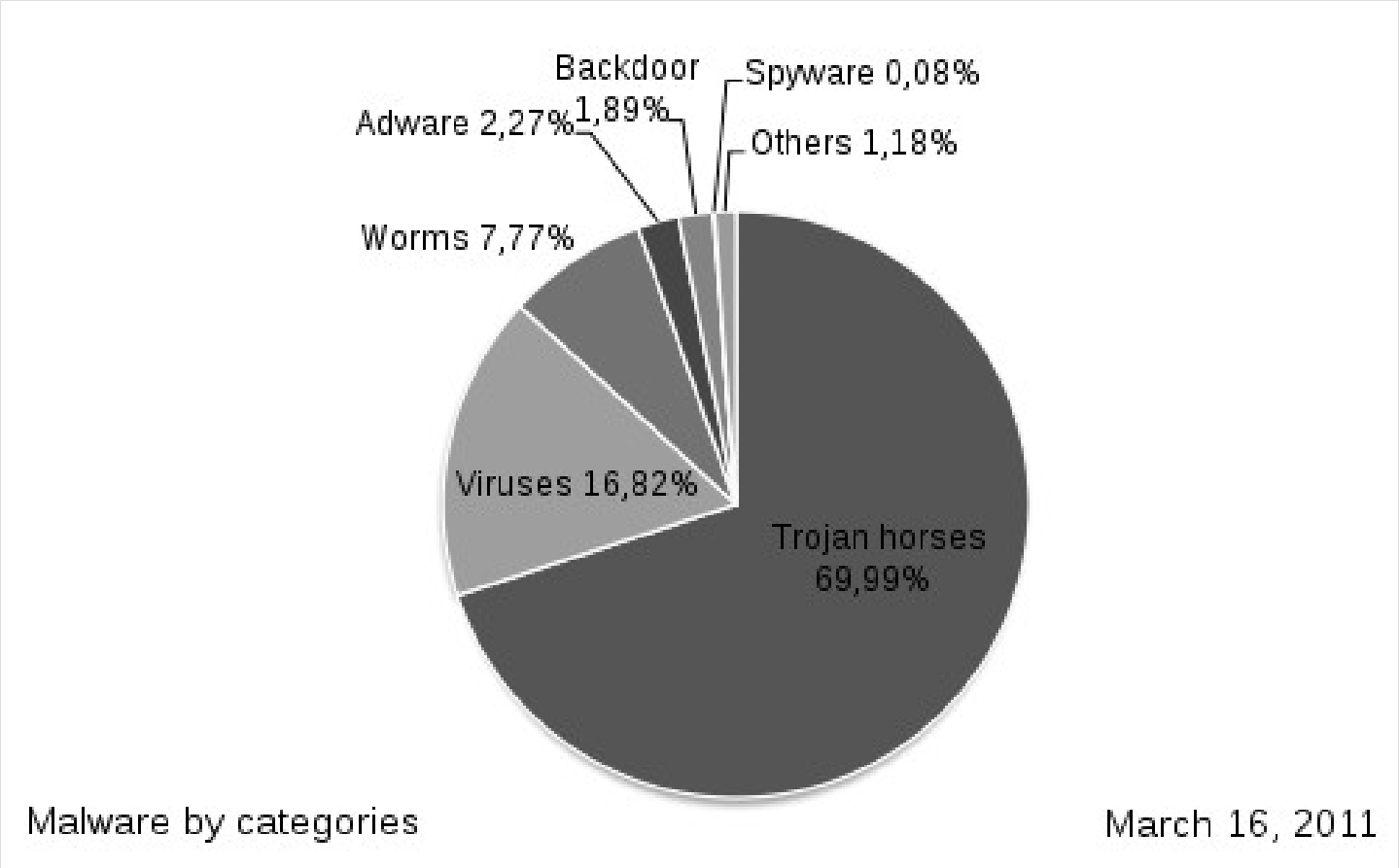
Malware – Cavallo di Troia (Trojan horse)

- E' un programma completo per dare pieno controllo del PC da parte di un altro PC collegato alla rete
- E' spesso inserito tramite attacchi di “social engineering”: mail che invitano a eseguire un allegato, giochi scaricabili gratuitamente, falsi antivirus, ecc.
- E' usato per:
  - carpire informazioni come password, dati di accesso a banche e carte di credito e inviarli a terze parti
  - effettuare invii di messaggi di mail (spam)
  - trasformare il PC attaccato in bot, per attacchi informatici

Malware – Adware e Spyware

- Spesso collegati a vulnerabilità dei Web browser, o dei sistemi operativi su cui i browser girano.
  - Si scaricano accedendo a siti Web. Di solito, non si auto-replicano.
- **Adware**: software che genera messaggi pubblicitari
- Può essere voluto:
  - si usa un'applicazione o un servizio Web gratuitamente, in cambio della ricezione di messaggi pubblicitari
- **Spyware**: software che raccoglie informazioni sui siti visitati, e le invia a punti di raccolta
  - può anche raccogliere informazioni più sensibili

Diffusione dei tipi di Malware



Anti virus

- Sono così chiamati i programmi per difendere i computer dal malware (virus, trojan, worm, adware, spyware...)
- Effettuano analisi della memoria (per individuare processi virali o sospetti), del settore di boot, dei dischi, delle e-mail ricevute
- Necessari per i sistemi operativi più attaccati, sia per diffusione che per intrinsica vulnerabilità (Windows)
- Per ora praticamente non necessari per S.O. derivati da Unix (Linux e Mac OS)
- Si aggiornano periodicamente dal proprio sito, per proteggere anche dal malware uscito dopo l'acquisto

Social engineering

- Studio e/o manipolazione del comportamento di una persona per venire a conoscenza di informazioni utili per attaccare il suo computer. Ad es.:
  - *shoulder surfing* (osservare la digitazione della password) da dietro, o installando telecamere nascoste
  - esame dei cestini della carta straccia, per trovare info
- **Pishing**: invio di mail contraffatte, con richieste di aiuto o che promettono vincite, per ottenere dati sensibili o anche pagamenti
- CD o penne USB sono “abbandonate”: chi li trova e li inserisce nel PC installa del malware
- Falsi centralini telefonici di banche e simili

Attacchi alla rete Internet

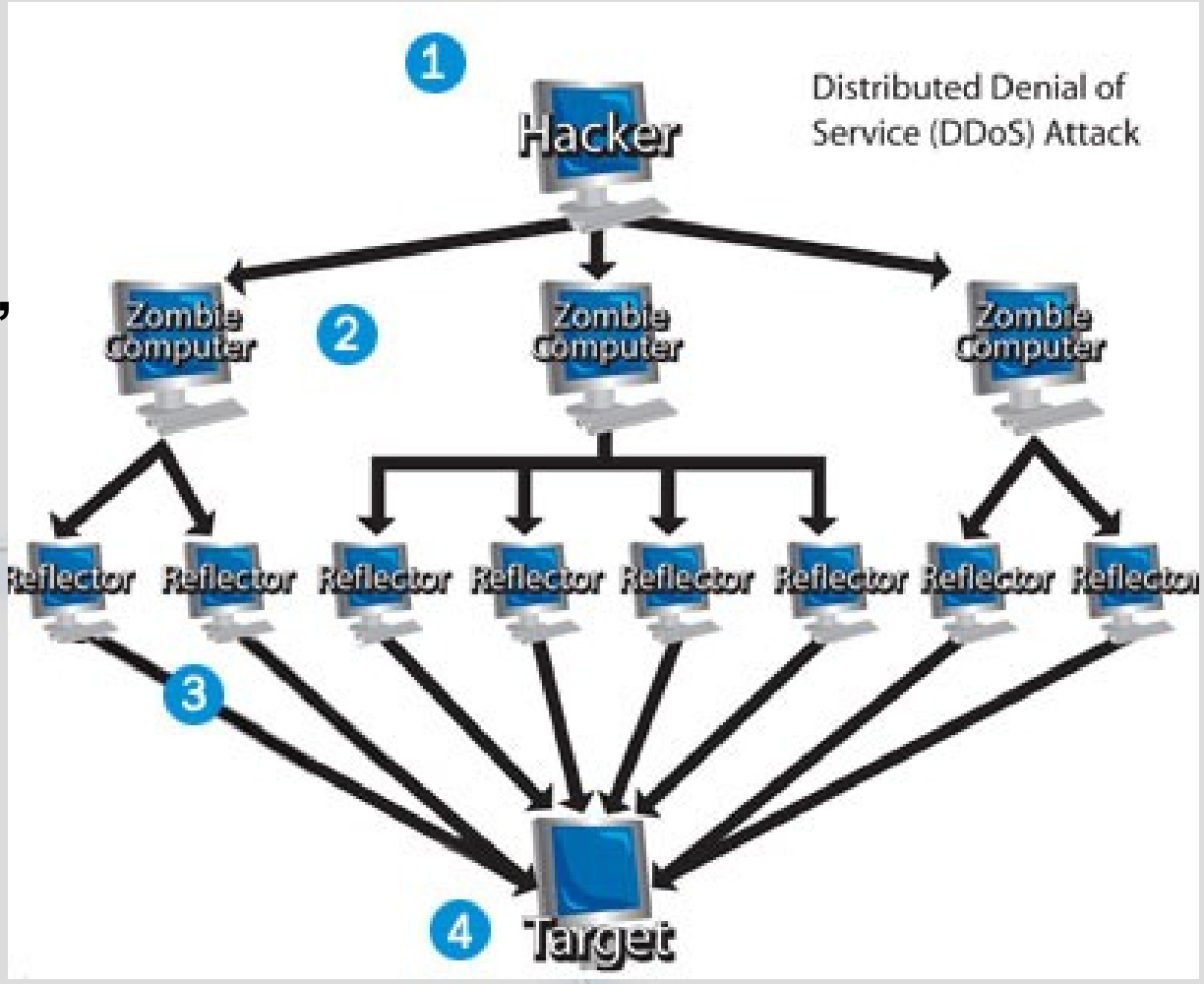
- Con la diffusione di Internet, si sono aperte anche opportunità di attacchi informatici verso specifici siti, o verso la rete stessa, per carpire informazioni o infliggere danni
- Attacchi passivi: si carpiscono informazioni che viaggiano in rete
- Attacchi attivi:
  - Denial of service
  - Spoofing
  - Attacchi ai computer (buffer/heap overflow)
  - ...

Denial of Service (DoS)

- Attacco per rendere indisponibile un servizio su Web
- Di solito, un sito Web oppure una porzione della rete
- Si inonda di false richieste (pacchetti IP) un server fino a sovraccaricarlo
- Per effettuare un attacco DoS occorrono:
  - moltissimi computer (tipicamente una botnet)
  - o pochi computer molto potenti e con larga banda
- Attacchi anche tramite reti peer-to-peer: i server dicono a tutti i nodi di collegarsi a quello da attaccare
- Attacchi di 2 livello per attivare difese note, e comunque escludere l'obiettivo dalla rete

Attacco DoS con “riflettori”

Gli “zombie” non attaccano direttamente l'obiettivo, ma PC intermedi (riflettori), inducendoli a inviare pacchetti a questo



Altri attacchi a livello TCP/IP

- **Sniffing**: lettura passiva dei pacchetti che transitano in una rete, per raccogliere informazioni. Può essere legittimo, o volto a intercettare password e altre informazioni sensibili
- **Spoofing**: si falsifica la propria identità (spoof), a vari possibili livelli OSI. Nell'IP spoofing si falsifica l'indirizzo IP del mittente per fare in modo che questi finga di essere un altro sistema.
- **Man in the middle**: spoofing "bifronte": l'attaccante si mette in mezzo alla comunicazione tra due computer, in modo che questi non si accorgano dell'intrusione. Si possono così leggere e modificare i dati scambiati.
- **Hijacking**: si prende il controllo non autorizzato di un canale di comunicazione
  - ad es. il **malware**, trasmesso tramite un virus, modifica la pagina iniziale di un browser web

Crittografia

- Deriva dalle parole greche kryptós (nascosto) e graphía (scrittura)
- La crittografia è un insieme di tecniche per mascherare dei dati, in modo da poterli trasmettere senza che chi li intercetti li possa leggere
- Serve a garantire la *riservatezza* dei dati
- Ha avuto un'enorme spinta con le comunicazioni elettroniche e con Internet
- Saper codificare (cifrare) e decodificare (decifrare) informazioni è utile anche per altri scopi (firma elettronica, garanzia di identità, ecc.)

Sistema crittografico

Il testo in chiaro viene elaborato dal sistema crittografico che produce il testo cifrato, e viceversa

Un po' di storia

- I primi sistemi crittografici noti risalgono all'antichità:
  - L'**Atbash** degli antichi Ebrei, sembra anche usato nella Bibbia
  - Si sostituisce l'alfabeto con lo stesso scritto alla rovescia:
    ABCDEFGHILMNOPQRSTUVZ
    ZVUTSRQPONMLIHGFEDCBA
  - Così: “Ciao mamma” diventa “Uozi mzmmz”
  - In Geremia 25, 26 si parla di “Sesàch” (ש-ש-כ) per intendere “Babel” (ב-ב-ל) cioè per non nominare Babilonia: תשרקצפעסנמל כי טחז ו הדגבא
    אבגדה ו זחטיכלמנסעפצקרשת

La Scitala lacedemonica

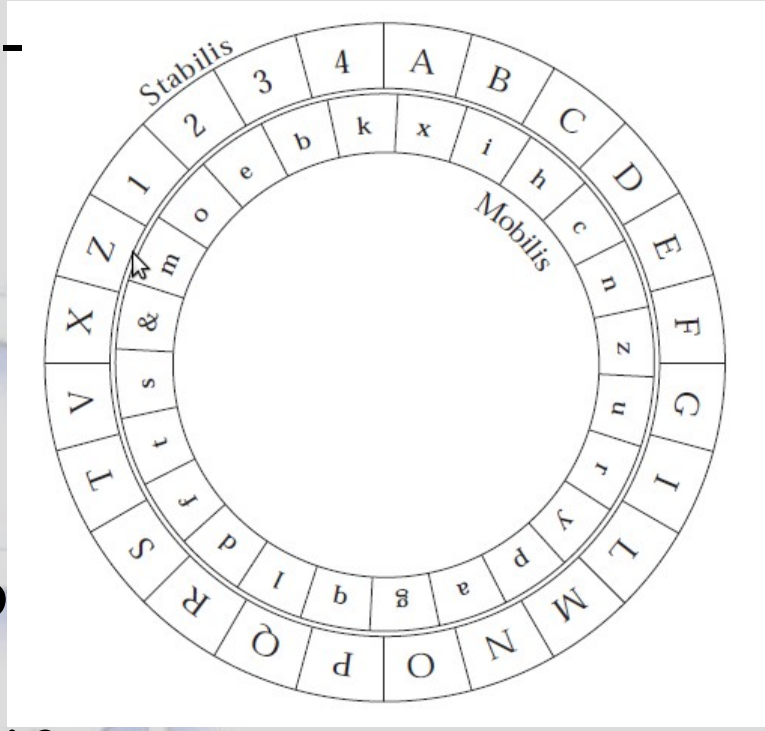
- Usata dagli spartani
- Si scrive il messaggio su una striscia di cuoio arrotolata su un bastone di diametro dato.
- Per decodificarlo, occorre un altro bastone dello stesso diametro
- La chiave è il diametro del bastone

Il cifrario di Cesare

- Usato effettivamente da Giulio Cesare
- E' un *cifrario a sostituzione monoalfabetica*
- Simile all'Atbash, solo che ogni lettera è sostituita da quella che la segue di *k* posizioni nell'alfabeto, ruotando dopo la Z
- La chiave è proprio *k*
- Esempio *(k* = 3*)*:
  `ABC|DEFGHILMNOPQRSTUVZ`
  `UVZ|ABCDEFGHILMNOPQRST`
  - Ora “Ciao mamma” diventa “Zful Huhhu”
- Se la chiave vale 13 (in alfabeto inglese con 26 lettere) si chiama ROT13 (*rotate by 13 places*)
  - così si usa lo stesso algoritmo sia per cifrare che per decifrare

Il disco cifrante di L.B. Alberti

- Introdotto nel primo trattato di crittografia, *De Componendis Cifris*, nel 1466 (largamente ignorato dai crittografi sino al 1900)
- Due dischi concentrici rotanti, in modo da poter variare facilmente la chiave
- Il disco interno ha l'alfabeto scritto in modo casuale
- La chiave varia man mano che si cifra
- Si decifra col procedimento opposto
- Metodo *polialfabetico* praticamente indecifrabile con metodi a mano



Robustezza della codifica

- Qualità di un algoritmo crittografico:
  - qualità della matematica sottostante
  - lunghezza della chiave
- Attacco a **forza bruta**
  - provare tutte le possibili combinazioni della chiave
  - ogni algoritmo è vulnerabile a questo attacco, tranne il *cifrario di Vernam*, in cui la chiave è lunga quanto il testo in chiaro, ed è usabile una sola volta; è però un metodo teorico e non utilizzabile in pratica!
  - chiave sufficientemente lunga → richiede troppo tempo
  - se una chiave ha ***n*** bit mediamente servono $\mathbf{2^{n-1}}$ tentativi
- **Rompere** (*to break*) un sistema crittografico
  - forzarlo in meno tempo rispetto alla forza bruta

Algoritmi pubblici o segreti?

- In passato, si credeva che mantenere segreto l'algoritmo di cifratura/decifratura ne aumentasse la sicurezza
- Ciò ha portato a fallimenti colossali:
  - Cifratura del GSM: decodificabile in 2” nel '99
  - Codifica DVD: decifrabile col sw. DeCSS
- In realtà, gli algoritmi di cifratura buoni sono sempre *pubblici*
- In tal modo, si possono studiare, pubblicarne le debolezze ed eventualmente migliorarli o scartarli
- La forza è nella lunghezza della chiave

Es. attacco a forza bruta sull'algoritmo DES

- DES: uno dei primi sistemi di cifratura simmetrica (1976)
- Aveva una chiave troppo corta: 56 bit (anche per motivi legati ai servizi segreti USA)
- Tempo impiegato per decodificare una chiave:
  - 1997: 2000 ore con supercalcolatore
  - 1998: 56 ore con supercalcolatore
  - 1999: 22 ore con supercalcolatore
  - 2008: 150 ore con una macchina da 10.000 $

Crittografia simmetrica

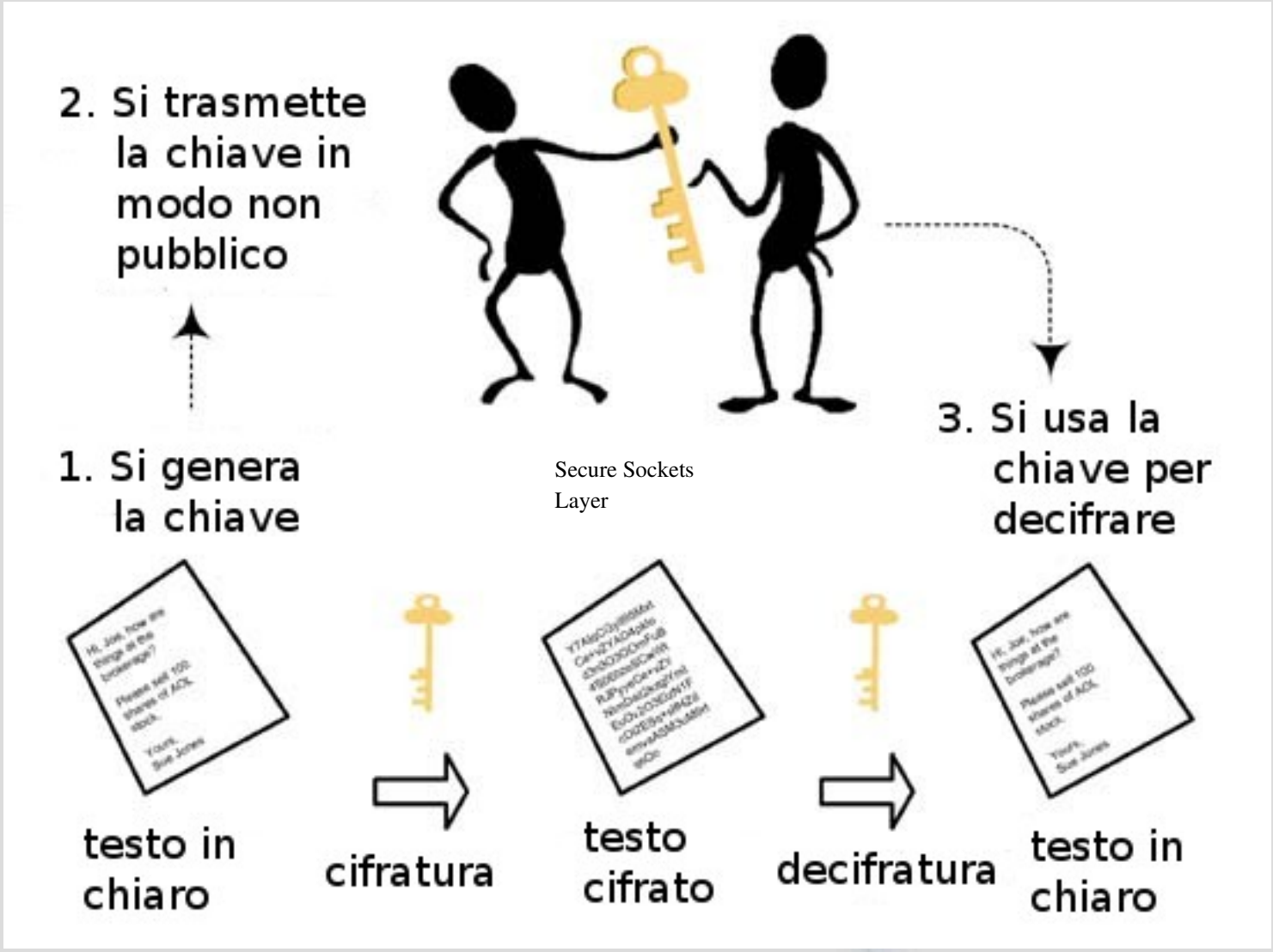
- C'è un'unica chiave *k* per codificare e decodificare
- Oppure, la chiave per decodificare, *d,* è facilmente calcolabile a partire da *k* (ad es. cifrario di Cesare)
- E' molto veloce ed efficiente
- Occorre però che la chiave sia notificata a parte, o su un canale sicuro!
- Esempi: DES, Triple DES, AES, Blowfish, Twofish
- E' tanto più sicura quanto più lunga è la chiave
  - deve essere almeno 80 bit, meglio 128 o 256
  - Es. 20 caratteri (scelti tra gli 80 più facili) sono circa $20 * \log_2 80 \cong 126$ bit – *evitare parole del vocabolario!*

Cifratura simmetrica

1. Sia il documento da cifrare, T, e la chiave k
2. La chiave k deve essere trasmessa al ricevente in modo sicuro
3. Il mittente usa l'algoritmo E, che usa k, per codificare T producendo il documento cifrato C: $C = E(k,T)$
4. Il documento C può essere trasmesso su una rete insicura, perché non decodificabile senza conoscere k
5. Il destinatario decifra C usando l'algoritmo di decodifica D, che rigenera il documento originale T: $T = D(k,C) = D[k,E(k,T)]$

- Il documento T può essere un vero documento testuale, o qualunque *file* (sequenza di bit)

Cifratura simmetrica



Crittografia asimmetrica

- Le chiavi di codifica *k* e di decodifica *d* sono diverse
- Conoscere *k* non permette di decodificare il documento: è necessario conoscere *d*
- *k* può quindi essere resa *pubblica* dal ricevente, e chiunque può inviargli messaggi codificati con *k*, non decifrabili da terzi
- *d* si chiama chiave *privata*
- Esempi: Diffie-Hellman, RSA, DSS
- Tanto più sicuro quanto più lunghe sono le chiavi
- Ha un costo computazionale molto maggiore della crittografia simmetrica

Cifratura asimmetrica

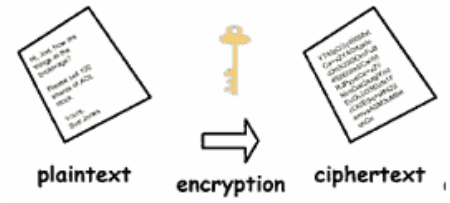
1. Sia il documento da cifrare, T
2. Il ricevente genera le due chiavi associate: *k* per cifrare e *d* per decifrare
3. Il ricevente trasmette al mittente la chiave *k*, anche in modo insicuro (chiave pubblica)
4. Il mittente usa l'algoritmo *A*, che usa *k,* per codificare T producendo il documento cifrato C: $C = A(k,T)$
5. Il documento C può essere trasmesso su una rete insicura, perché non decodificabile senza conoscere *d*
6. Il destinatario decifra C usando l'algoritmo di decodifica *B*, che rigenera il documento originale T: $T = B(d,C) = B[d, A(k,T)]$

Cifratura asimmetrica

1. Il ricevente genera le due chiavi k e d

2. Il ricevente dà la chiave pubblica k a tutti i possibili mittenti

3. Il mittente codifica il documento con la chiave pubblica



4. Il documento cifrato è trasmesso su rete insicura

5. Il ricevente decodifica il messaggio usando la chiave privata d

I protocolli TLS (Transport Layer Security) e SSL (Secure Sockets Layer)

- Sono standard per trasmettere dati su Internet in modo “sicuro”
- Si basano su crittografia asimmetrica (per l'autenticazione iniziale e la trasmissione della chiave simmetrica) e simmetrica (per la trasmissione vera e propria)
- Il server si autentica con una chiave pubblica certificata (emessa da un'Autorià di certificazione)
- Anche il client può certificarsi, se necessario
- Supportano molti algoritmi di codifica simmetrica
- SSL è del 1996, TLS 1.0 del '99, TLS 1.3 del 2008
- TLS può declassarsi all'uso di SSL 3.0

Il processo TLS/SSL ("Handshake")

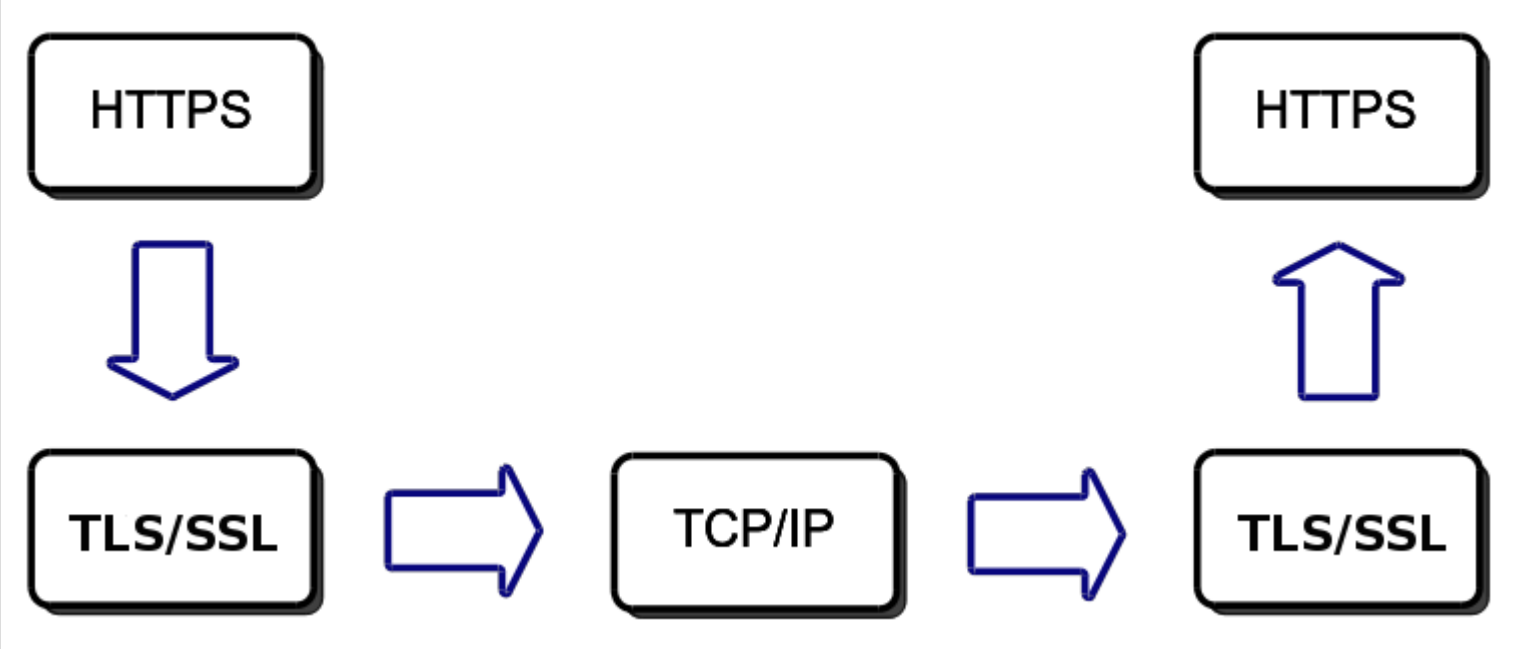
1. Il cliente invia un messaggio iniziale che elenca i propri algoritmi crittografici
2. Il server risponde con la scelta di uno degli algoritmi
3. Il server invia il proprio certificato TLS/SSL, che include la propria chiave pubblica k_s
4. Il cliente controlla che il certificato sia valido e invia il proprio certificato, se richiesto
5. Il cliente invia un numero random, k (la chiave per la trasmissione), codificato con la chiave pubblica del server k_s
6. Il server decodifica la chiave k con la propria chiave privata – ora cliente e server condividono la chiave k

Il processo TLS/SSL (trasmissione)

7. Sia il cliente che il server si scambiano messaggi che notificano che le successive trasmissioni saranno codificate
8. Tutti i dati scambiati sono crittografati con l'algoritmo simmetrico prescelto e la chiave *k*
9. Alla fine della trasmissione, la chiave *k* è scartata

- La fase di handshake di solito dura meno di un secondo
- La codifica simmetrica è veloce, ma la trasmissione è ovviamente più lenta di una trasmissione in chiaro
- TLS/SSL sono usati dal protocollo HTTPS e per le VPN (Virtual Private Network)

HTTPS e TLS/SSL



Firma digitale

- Usa la cifratura asimmetrica con lo scopo di garantire:
  - **Autenticità**: un documento è stato "firmato" da una data persona
  - **Non ripudio**: il firmatario non può ripudiare la firma
  - **Integrità**: il documento non è stato alterato dopo la firma
- Richiede un'autorità di certificazione che garantisca sulla validità della firma
- Usa le chiavi della cifratura "al contrario":
  - la chiave di codifica *k* è mantenuta privata
  - la chiave di decodifica *d* è pubblica (per "leggere" e autenticare le firme)

Firma digitale

- **Autenticità**: è garantita dal fatto che il proprietario è riconosciuto, e gli è assegnata una coppia di chiavi *k, d* che solo lui può avere
- **Integrità**: dal documento originale viene generata un'*impronta digitale* hash, *h*, che viene crittografata con la chiave segreta *k*
  - qualunque modifica al documento porterebbe a generare un'impronta diversa da *h*
- **Non ripudio**: il firmatario non può ripudiare la firma, perché solo la sua chiave *k* può aver generato la codifica corretta dell'impronta *h*

Rilascio della firma digitale

- Rilasciata da Autorità (InfoCamere, Unione Notai, Poste Italiane, …) che archiviano i codici e garantiscono sulla validità
- Rilasciata previo riconoscimento fisico certo dell'utente
- Si rilascia una “smart card” o una chiave USB univocamente associate all'utente, e il software per la firma vera e propria
- La smart cart contiene la chiave *k* (privata) per codificare
- La chiave *d* per la verifica della firma è pubblica, e può essere richiesta all'Autorità

Firma digitale

Meccanismo di “hashing”

- Usato per la verifica di integrità
- Una funzione *hash* è una funzione $H(x) : \mathbb{N} \rightarrow [0, M]$
- $H()$ associa a un documento x (insieme di bit, e dunque considerabile come un numero naturale $\mathbb{N}$) a un numero naturale scelto in un intervallo dato (M è compreso tra 2^{128} e 2^{256}; $M = 2^{160}$ nel caso della firma digitale)
- Una buona funzione hash genera numeri molto diversi anche in presenza di variazioni minime dell'argomento
- E' praticamente impossibile alterare un documento, in modo che il nuovo abbia lo stesso valore hash dell'originale

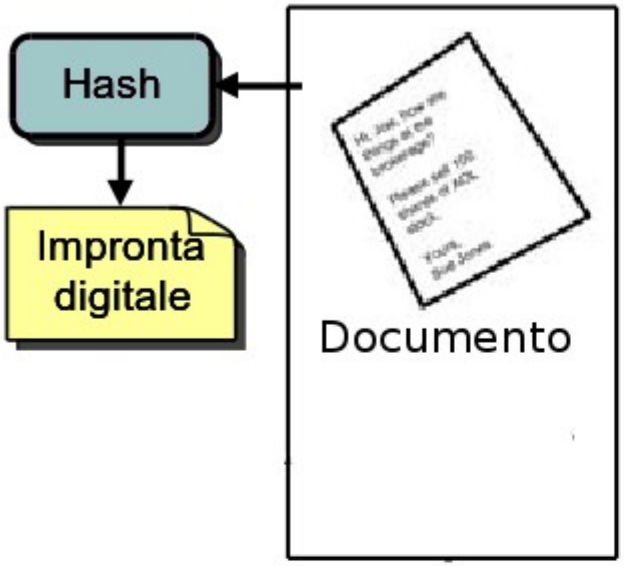
Meccanismo della firma digitale

1. Dato un file da firmare *x*, si usa la coppia di chiavi asimmetriche *k* e *d*
2. *S*i applica al file *x* una funzione hash standard (fornita con la firma), che genera un valore dell'*impronta digitale* $h = H(x)$
3. Si codifica *h* (non *x*!) con la chiave *k*, mantenuta segreta dal firmatario: $c = A(k,h)$. *c* è detta *firma digitale*
4. Si costruisce il file firmato (.p7m) "impacchettando" *x* , *c* e l'informazione sul firmatario e l'Autorità che ha rilasciato la firma

Verifica del file firmato

1. Dato il file firmato, si richiede all'Autorità (via Internet) la chiave pubblica di decodifica, *d,* del file firmato
2. Si decodifica la firma *c,* ottenendo l'impronta digitale originale *h*
3. Si applica la funzione hash al documento x' (che è incluso nel documento firmato), ottenendo $h' = H(x')$
4. Se $h = h'$ ho la certezza che $x' = x$, cioè che il file è integro, e che è stato firmato dall'utente originale

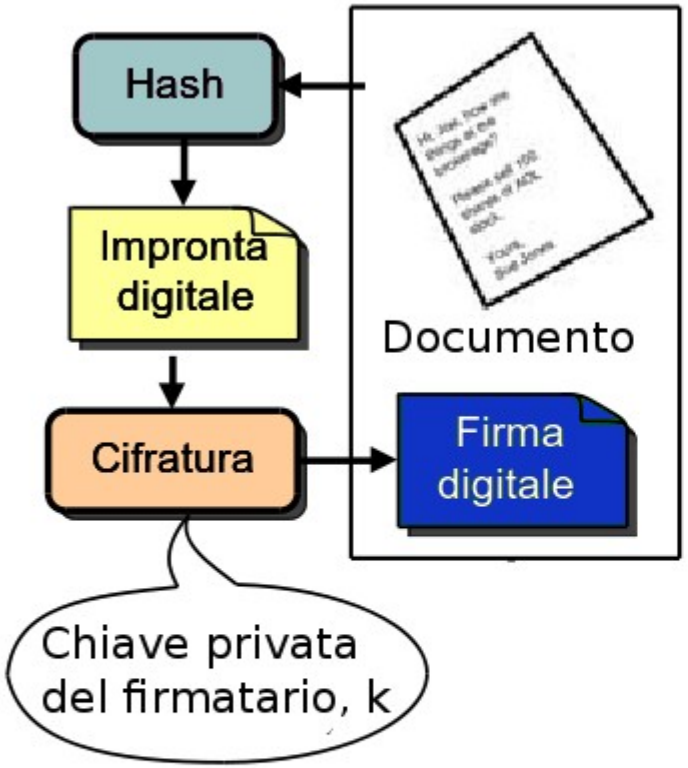
Meccanismo della firma digitale



Firmatario

Destinatario

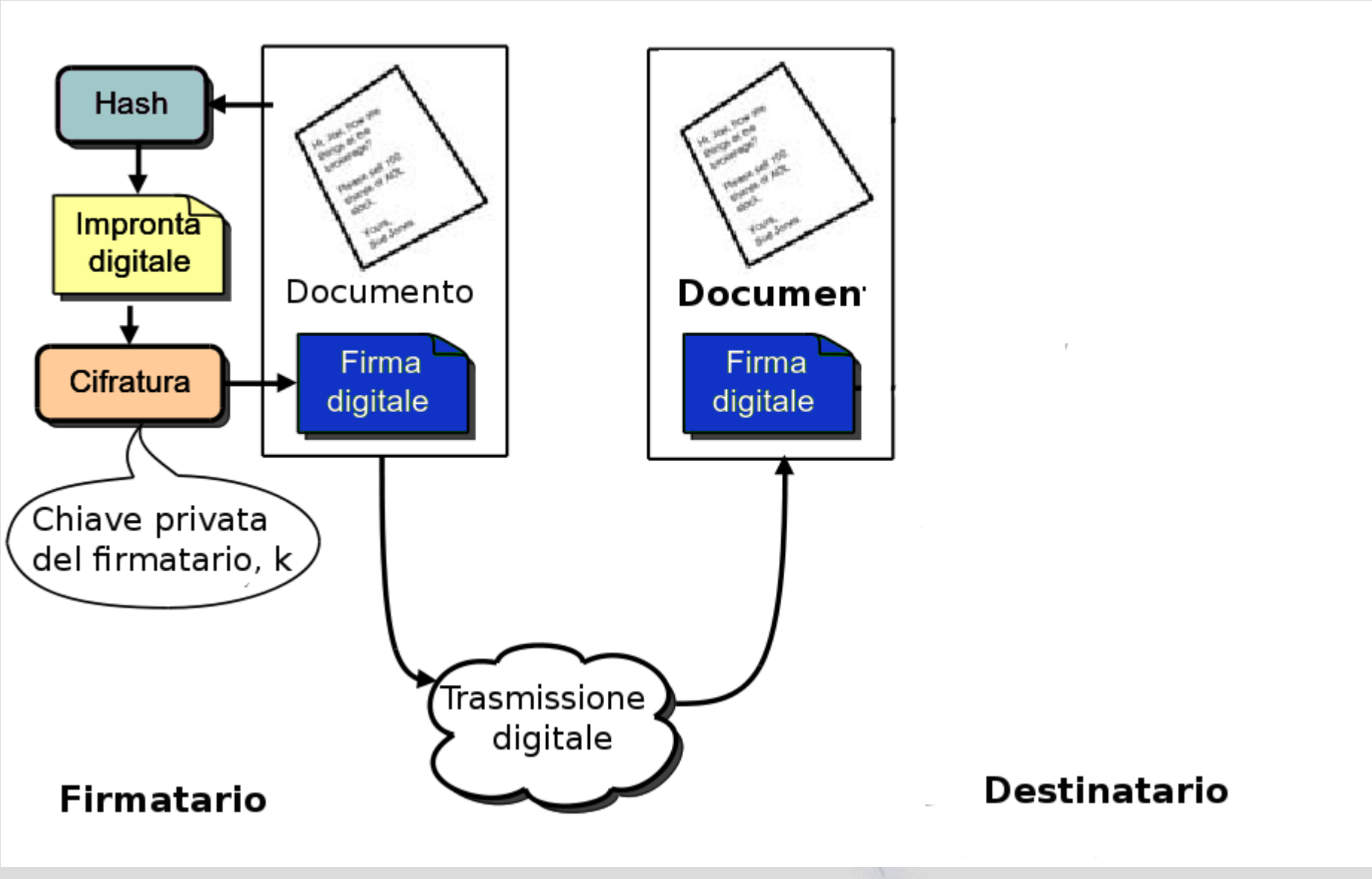
Meccanismo della firma digitale



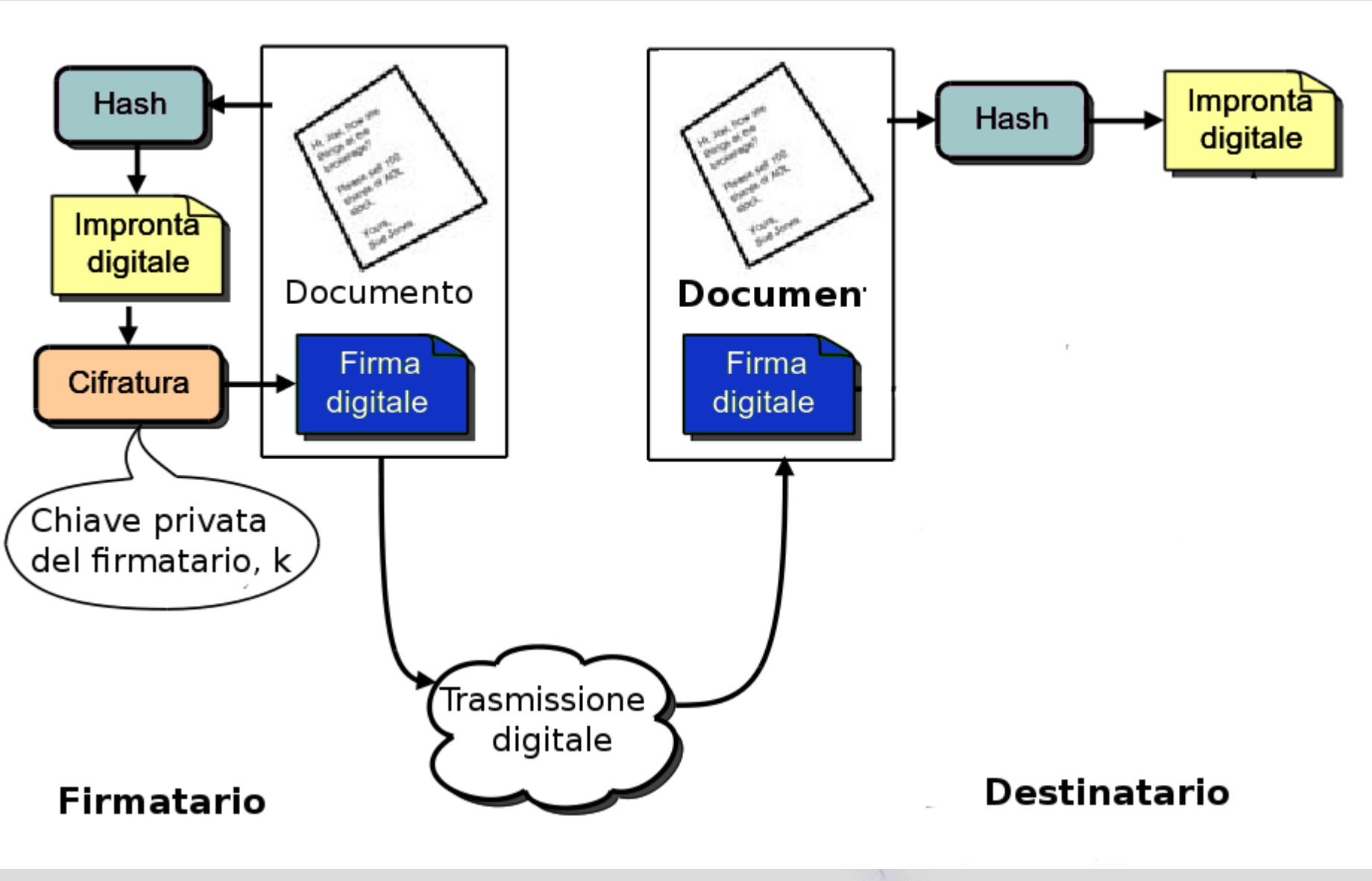
Firmatario

Destinatario

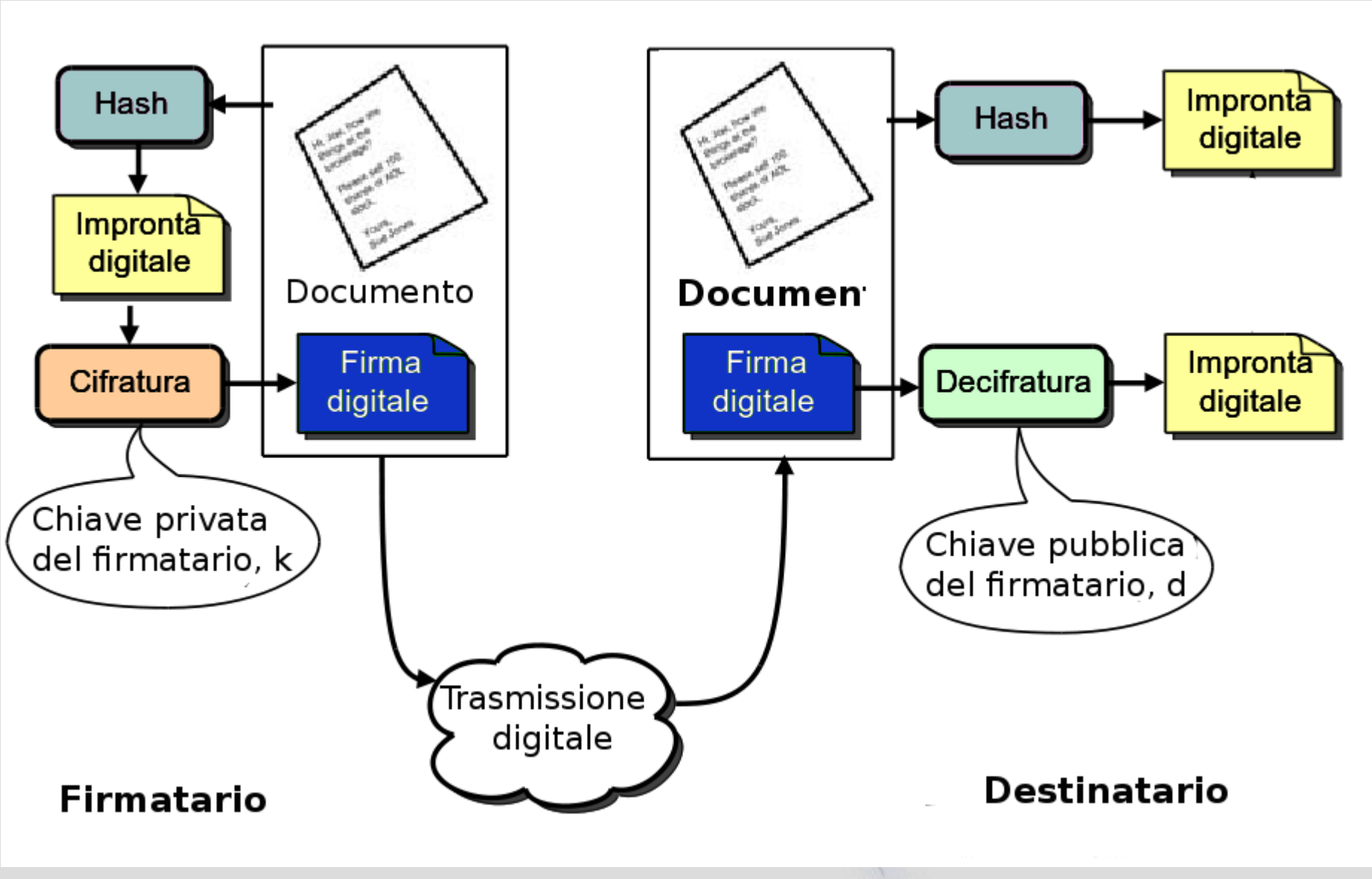
Meccanismo della firma digitale



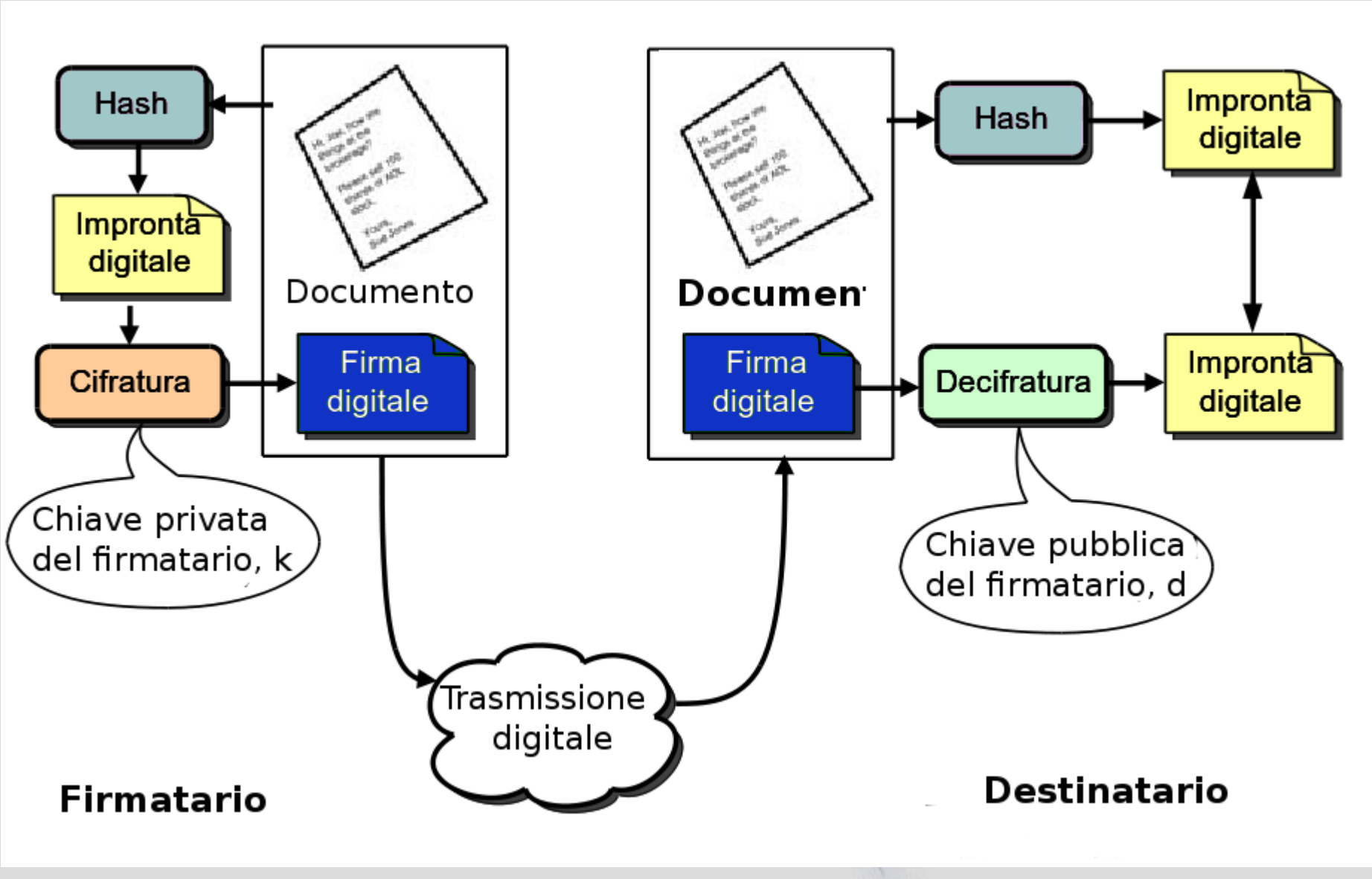
Meccanismo della firma digitale



Meccanismo della firma digitale



Meccanismo della firma digitale



Firma digitale e firma autografa

	Firma autografa	Firma digitale
Creazione	manuale	mediante algoritmo
Apposizione	sul documento: la firma modifica il documento e ne è parte integrante	come allegato al documento originale: il documento firmato è costituito dalla coppia (documento, firma)
Verifica	confronto con una firma autenticata: metodo facile ma insicuro	mediante algoritmo e chiave di verifica pubblicamente noti: metodo sicuro
Falsificazione	facilmente falsificabile, ma il falso è riconoscibile.	solo carpendo la chiave privata; il falso non è riconoscibile
Ripudio	la firma deve essere autenticata da un notaio per impedire il ripudio.	solo tramite querela di falso, con prova a carico del firmatario
Documento copia	diverso e distinguibile	indistinguibile: ogni copia è un originale
Validità temporale	illimitata	limitata
Automazione dei processi	non possibile	possibile

Protezione dei dati: tre problemi

- **Identificazione**
  Chi sei?
  - l'utente fornisce il proprio codice identificativo (username, mail, codice fiscale...)
- **Autenticazione**
  Come puoi provare che la tua identità è vera?
  - domanda difficile: vedi dopo
- **Autorizzazione**
  Sei autorizzato a effettuare questa operazione?
  - esistono meccanismi basati su liste per il controllo degli accessi (**ACL**) che danno i vari livelli di autorizzazione (NO, LETTURA, SCRITTURA, AMMINISTRAZ., ...)

Meccanismi di autenticazione

- **Quello che si sa**
  - password
  - domande di recupero password (il film preferito...)
- **Quello che si ha**
  - smart card
  - chiave USB
- **Quello che si è (biometria)**
  - impronte digitali
  - voce
  - iride
  - ...

Vulnerabilità delle password

- Possono essere intercettate:
  - quando sono trasmesse sulla rete
  - se sono scritte su carta
- Possono essere condivise da più utenti
- Password guessing:
  - **Attacco a forza bruta**: si cerca di individuare la password provando tutte le possibili combinazioni
  - **Attacco basato su dizionari**: si cerca di individuare la password cercando le parole più probabili (dizionario)
    - esistono in rete liste delle 1000 password più usate, parole italiane e inglesi, frasi comuni, ecc.

Robustezza di una password

- Dipende dalla sua lunghezza (**keyspace**)
  - è robusta se il tempo necessario per indovinarla è maggiore della durata della password
  - una buona password deve avere almeno 15-20 caratteri
- Diminuisce con il tempo
  - la potenza di calcolo degli elaboratori aumenta costantemente:
    - si riduce il tempo necessario per il password guessing
  - aumenta la probabilità che qualcuno la riesca a spiare
- One-time password
  - Generata ogni pochi minuti da un'apposito dispositivo
  - Comune per operazioni bancarie e con carta di credito

Le criptovalute

- Una delle ultime novità della crittografia e dell'informatica
- La più popolare è il ***Bitcoin*** **(**sigla: **BTC o XBT)**
- Sono monete (denaro) digitale:
  - Decentralizzate (nessuna autorità centrale)
  - Anonime
  - Deflazionarie (limitate in quantità)
  - Fruibili tramite Internet

Che cos'è il denaro?

- **Un mezzo di scambio:**
  - Per scambiare i beni superando il baratto
  - Le valute ufficiali devono essere accettate per legge
- **Un'unità di conto:**
  - Riconoscibile, usabile, divisibile, trasferibile, di difficile contraffazione
- **Una riserva di valore:**
  - Stabile e durevole
  - Rara
  - “Concentrata” in poco spazio

Una criptovaluta è un valore al portatore

- Il proprietario è il possessore
- Non ci sono registrazioni sul proprietario: anonima
- Digitale
- Difficile o impossibile da rimpiazzare se persa o rubata (*come il denaro tradizionale!*)
- Basata sulla crittografia digitale:
  - Affidabilità basata sulle proprietà matematiche della crittografia (asimmetrica) e delle impronte hash
  - NON su proprietà chimico-fisiche (es. oro)
  - NON su stato legale coercitivo (valute)

L'idea

- La moneta è una registrazione in un registro pubblico (*Block Chain*), condiviso su Internet da migliaia di nodi e gestito in modo *peer to peer*
- La registrazione ha un indirizzo pubblico (derivato da una chiave crittografica pubblica)
- Il proprietario possiede la chiave privata associata
- Solo usando tale chiave privata si può trasferire (***una sola volta!***) la moneta verso un altro indirizzo pubblico
- Tale trasferimento (*transazione*) è validato e registrato nella Block Chain (BC)

La transazione

- Tutte le richieste di trasferimento di moneta, “firmate” tramite le chiavi private, sono inviate alla rete *peer to peer* e aggregate in *blocchi*
- Ogni transazione (trasferimento di moneta) è verificata per essere accettata:
  - L'indirizzo pubblico di origine deve corrispondere a moneta ***esistente*** e ***non già spesa***
  - La transazione deve essere ***firmata*** dalla chiave privata corrispondente all'indirizzo
- Tutte le transazioni validate sono inserite in un *blocco* e tale blocco è aggiunto alla BC

Il blocco e il mining

- La verifica delle transazioni in un blocco ha un costo computazionale, che va remunerato
- L'idea è che chiunque possa validare blocchi; chi valida blocchi si chiama *miner – minatore* (di BTC)
- La validazione è resa computazionalmente difficile, in modo che non possa essere effettuata prima di qualche minuto
- Il primo miner che riesce a validare il blocco corrente, lo inserisce nella BC e guadagna una quantità fissata di moneta
- Tutti gli altri miner smettono di computare, e passano al blocco successivo

Dati di un blocco

- Un block header contiene i seguenti dati (Block Chain dei Bitcoin):
  - Data e ora
  - Nr. di transazioni
  - Nonce (un numero intero a 32 bit)
  - Hash del blocco
  - Hash del blocco precedente
  - La lista di tutte le transazioni
- L'hash del blocco deve iniziare con un numero dato di zeri (problema di difficile computazione), che si ottiene per tentativi variando il *nonce*.

Bitcoin: la criptovaluta più diffusa

- Il Bitcoin fu introdotto nel 2008
- Il primo blocco (Genesis Block) fu generato a gennaio 2009
- Sino al 11/2012 ogni blocco validato dava 50 BTC
- Ogni circa 4 anni, tale quantità è dimezzata (ora sono 25)
- Il numero di BTC in circolazione resterà limitato a circa 21 milioni (moneta deflazionaria)
- Nel 2011 il valore del BTC iniziò ad essere > 1 US$
- Nel dicembre 2013 il picco a 1220 US$
- Ora viaggia sui 200-250 US$

Il prezzo del Bitcoin

Bitcoin: la criptovaluta più diffusa

- Gli *Exchange* sono siti in cui si possono comprare o vendere BTC in cambio di denaro tradizionale
- Molti siti vendono beni o servizi in cambio di BTC
- La rete dei miner è molto vasta
  - Quasi tutti appartengono a *pool* (gruppi di miner associati)
- Potenza di calcolo (hash rate) complessiva dei miner nel 2015: centinaia di volte maggiore della somma della potenza dei primi 500 supercomputer noti

Bitcoin: hash rate

Dove si conservano in Bitcoin?

- In portafogli (*wallet*) nel proprio computer
  - Sono programmi che conservano le chiavi pubbliche e private, e sono in grado di accedere alla BC e effettuare/ricevere versamenti
- In "conti correnti" presso gli exchange (rischioso!)
- In cassaforte:
  - Chiavi pubblica e privata stampate su carta, tramite codici leggibili elettronicamente, e plastificate

Maggiori informazioni

- Bitcoin.org : sito della fondazione Bitcoin
- blockchain.info : exchange e informazioni statistiche
- blockexplorer.com : visualizzatore dei blocchi e delle transazioni
- www.coindesk.com : sito di notizie
- www.bitcoinita.it : sito di notizie in italiano
- localbitcoins.com : sito per comprare e vendere BTC anche tramite transazioni locali faccia a faccia
- therocktrading.com : exchange maltese gestito da italiani