La sicurezza nell'uso della rete

15 aprile 2014 - Claudio Bizzarri
Modulo base
claudio@bizzarri.net

Modulo base
La sicurezza nell'uso della rete

- Introduzione
  - internet e Internet
  - obiettivi di un attacco
- Sicurezza degli apparati
  - firewall
  - wireless
  - accesso fisico ad un apparato
  - backup dei dati
- Sicurezza applicativa
  - web application
  - open source e closed source
- Sicurezza comportamentale
  - la navigazione
  - la password
  - la firma digitale
  - la posta elettronica
  - la PEC

Introduzione

Internet e internet

- L'importanza di una I maiuscola
- Internet come bene primario
- In tutti i mondi ci sono lati oscuri...

Internet oggi

BigBag Disruption

“disgregare un mercato consolidato in pochissimo tempo”

il caso Whatsapp

Internet oggi

- Telegrammi-SMS: IM
- Posta, informazioni: mailing list
- Negozi: e-commerce
- Musica: streaming
- Televisione: streaming
- Curriculum e reputazione: social network

Obiettivi di un attacco

- accesso non autorizzato
- sc
- ma
- or
- enti
- intercettazione di messaggi
- modifica di messaggi
- alterazioni delle funzionalità

Obiettivi di un attacco

accesso non autorizzato

scambio di identità

alterazione delle informazioni

cancellazione delle informazioni

alterazione dei permessi degli utenti

intercettazione di messaggi

modifica di messaggi

alterazioni delle funzionalità

Obiettivi di un attacco

accesso non autorizzato

scambio di identità

alterazione delle informazioni

cancellazione delle informazioni

alterazione dei permessi degli utenti

intercettazione di messaggi

modifica di messaggi

alterazioni delle funzionalità

Obiettivi di un attacco

accesso non autorizzato

scambio di identità

alterazione delle informazioni

cancellazione delle informazioni

alterazione dei permessi degli utenti

intercettazione di messaggi

modifica di messaggi

alterazioni delle funzionalità

Obiettivi di un attacco

accesso non autorizzato

scambio di identità

alterazione delle informazioni

cancellazione delle informazioni

alterazione dei permessi degli utenti

intercettazione di messaggi

modifica di messaggi

alterazioni delle funzionalità

Obiettivi di un attacco

accesso non autorizzato

scambio di identità

alterazione delle informazioni

cancellazione delle informazioni

alterazione dei permessi degli utenti

intercettazione di messaggi

modifica di messaggi

alterazioni delle funzionalità

Obiettivi di un attacco

accesso non autorizzato

scambio di identità

alterazione delle informazioni

cancellazione delle informazioni

alterazione dei permessi degli utenti

intercettazione di messaggi

modifica di messaggi

alterazioni delle funzionalità

Obiettivi di un attacco

accesso non autorizzato

scambio di identità

alterazione delle informazioni

cancellazione delle informazioni

alterazione dei permessi degli utenti

intercettazione di messaggi

modifica di messaggi

alterazioni delle funzionalità

Obiettivi di un attacco

accesso non autorizzato

scambio di identità

alterazione delle informazioni

cancellazione delle informazioni

alterazione dei permessi degli utenti

intercettazione di messaggi

modifica di messaggi

alterazioni delle funzionalità

Obiettivi di un attacco

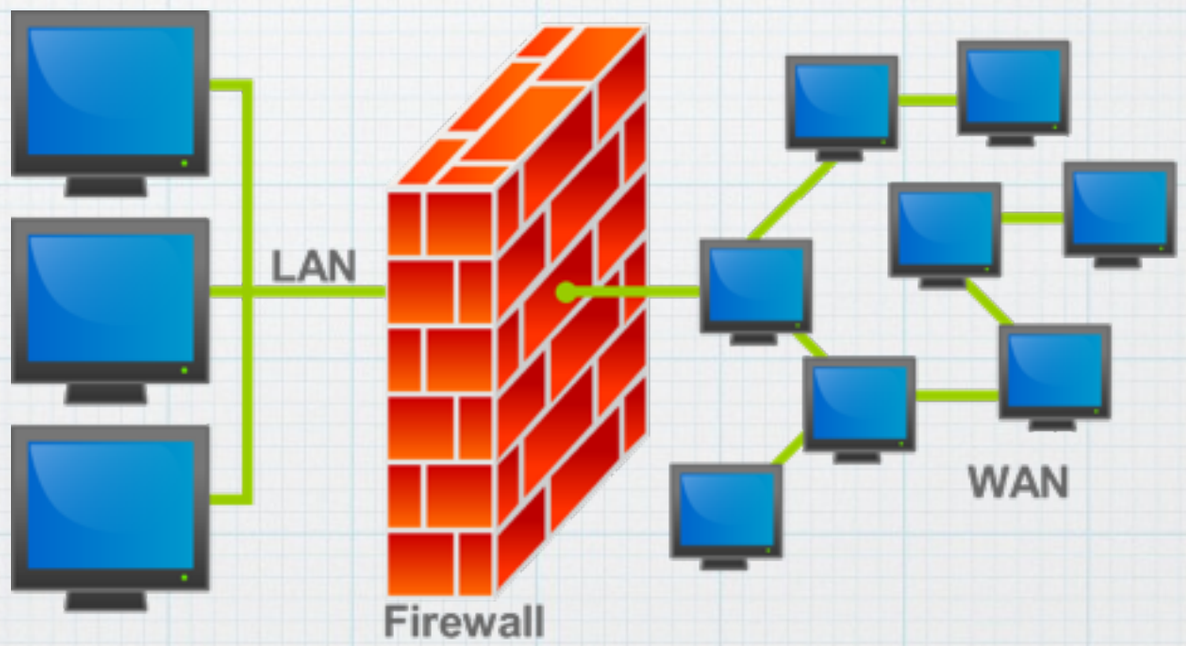
Informazioni
=
soldi

La sicurezza degli apparati

Firewall

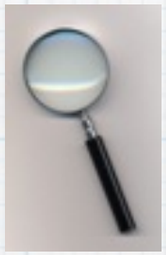
Firewall

Il firewall si posiziona fra la rete locale (LAN) e il mondo esterno (WAN)



Firewall

Le funzioni di un firewall sono:



- monitoraggio
- autorizzazione

- modifica

Firewall

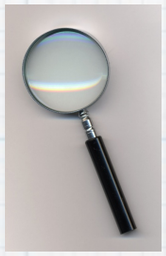
Le funzioni di un firewall so

- monitoraggio

- autorizzazione
- modifica

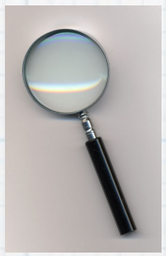
Firewall

Le funzioni di un firewall s

- monitoraggio 
- autorizzazione
- modifica 

Firewall

Le funzioni di un firewall sono:



- monitoraggio
- autorizzazion

- **modifica**

Firewall

è un programma

è un filtro intelligente

è un meccanismo di prevenzione

NON è un antivirus/antimalware/antispyware

NON è una protezione universale

NON è un apparecchio magico

Firewall

Considerazioni:

- il firewall è solo uno strumento, se usato male (o non usato) non ha alcuna utilità
- la configurazione e la manutenzione è più importante dell'apparecchio in sé

Wireless

- open: nessuna sicurezza
- WEP: vulnerabile
- WPA+TKIP
- WPA+TKIP/AES
- WPA+AES
- WPA2+AES

Il meccanismo WPS introduce una falla in alcuni sistemi, andrebbe sempre disabilitato. La sicurezza dipende anche dal tipo di apparato installato.

Accesso fisico ad un apparato

* L'accesso fisico ai dati è il metodo più efficace
* Porte LAN, porte USB, e porte fisiche vanno sempre controllate
* La zona server (se esiste) va protetta

Backup dei dati

- Non SE ma QUANDO smetterà di funzionare
- I dati importanti vanno mantenuti in tre copie
- Le procedure di ripristino vanno verificate spesso
- La protezione dei backup è fondamentale tanto quanto quella dei server normali

(fine prima parte)

Sicurezza applicativa

Web application

I dati circolano in rete: HTTPS

I dati sono memorizzati in rete: reputazione

Scrivere una web application sicura è difficile: autore

Creare una replica di una web application è semplice: inganno

Web application

I dati circolano in rete: HTTPS

I dati sono memorizzati in rete: reputazione

Scrivere una web application sicura è difficile: autore

Creare una replica di una web application è semplice: inganno

Web application

I dati circolano in rete: HTTPS

I dati sono memorizzati in rete: reputazione

Scrivere una web application sicura è difficile: autore

Creare una replica di una web application è semplice: inganno

Web application

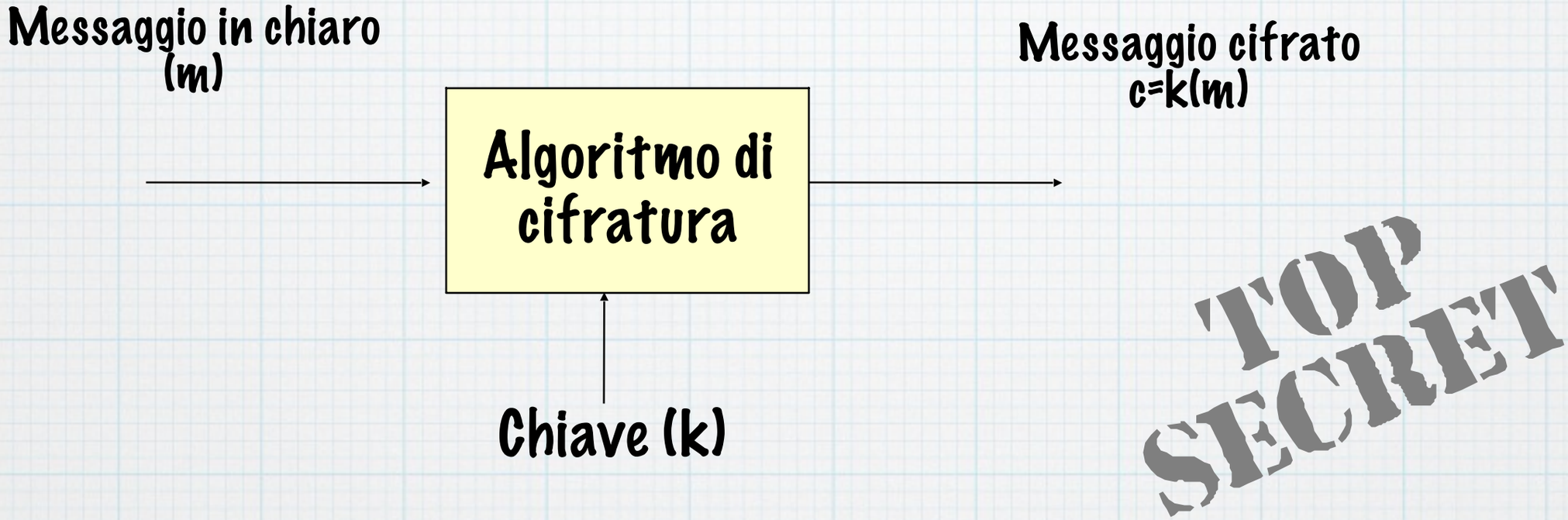
I dati circolano in rete: HTTPS

I dati sono memorizzati in rete: reputazione

Scrivere una web application sicura è difficile: autore

Creare una replica di una web application è semplice: inganno

Principi di Crittografia



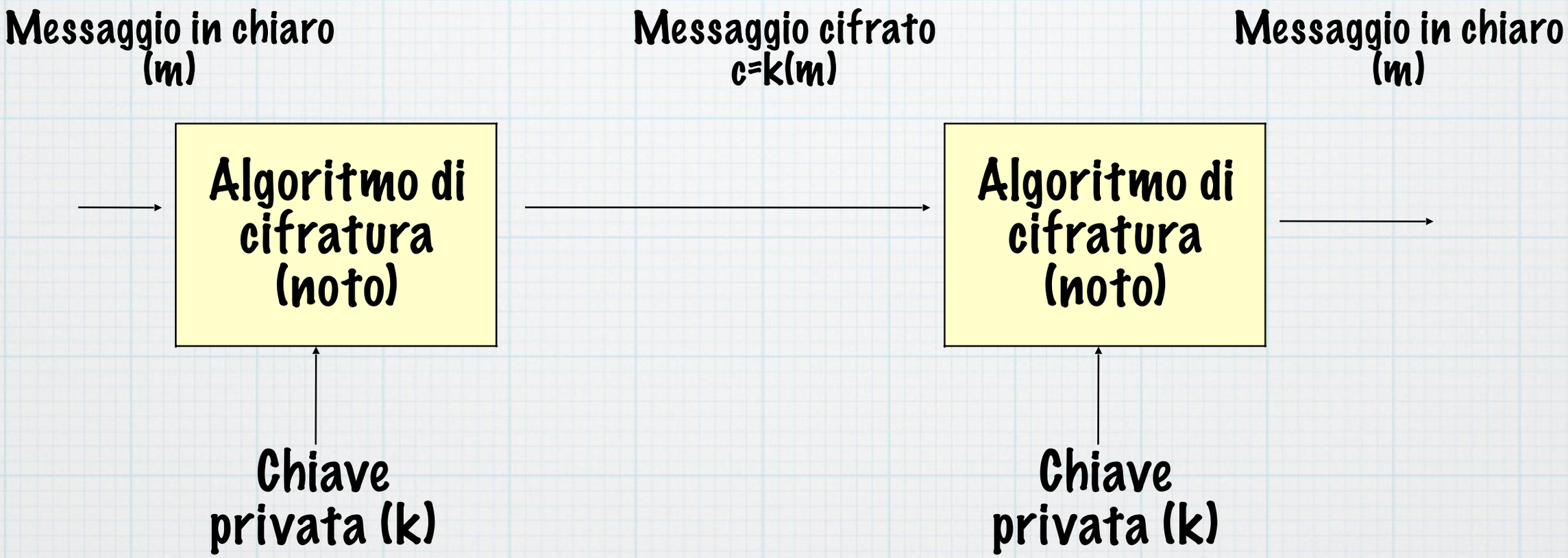
Possibili algoritmi di cifratura:

elevamento a potenza del messaggio in chiaro, dove la chiave è inclusa nella potenza

shift ciclico del messaggio in chiaro di un numero di posizioni dipendente dalla chiave

scrambling del messaggio in chiaro con algoritmi dipendenti dalla chiave

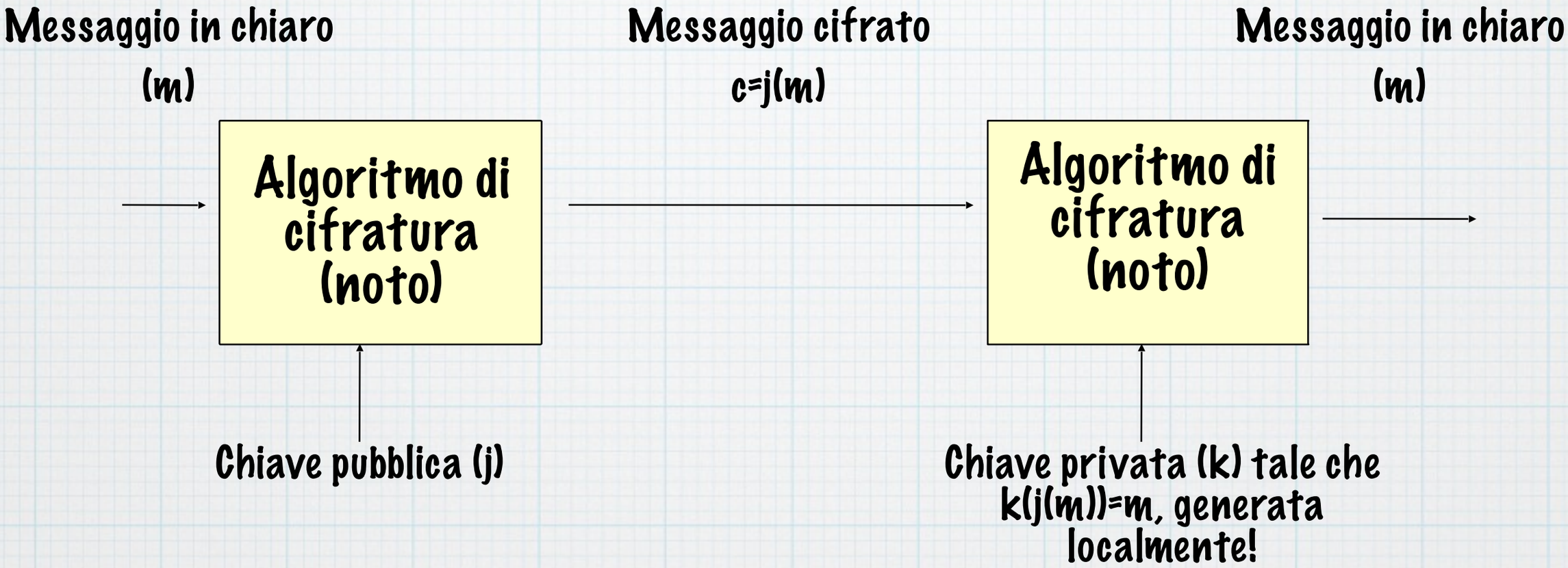
Cifratura a Chiave Simmetrica



Semplice, veloce

Tutto si incentra sulla sicurezza e sulla riservatezza della chiave!

Cifratura a Chiave Asimmetrica



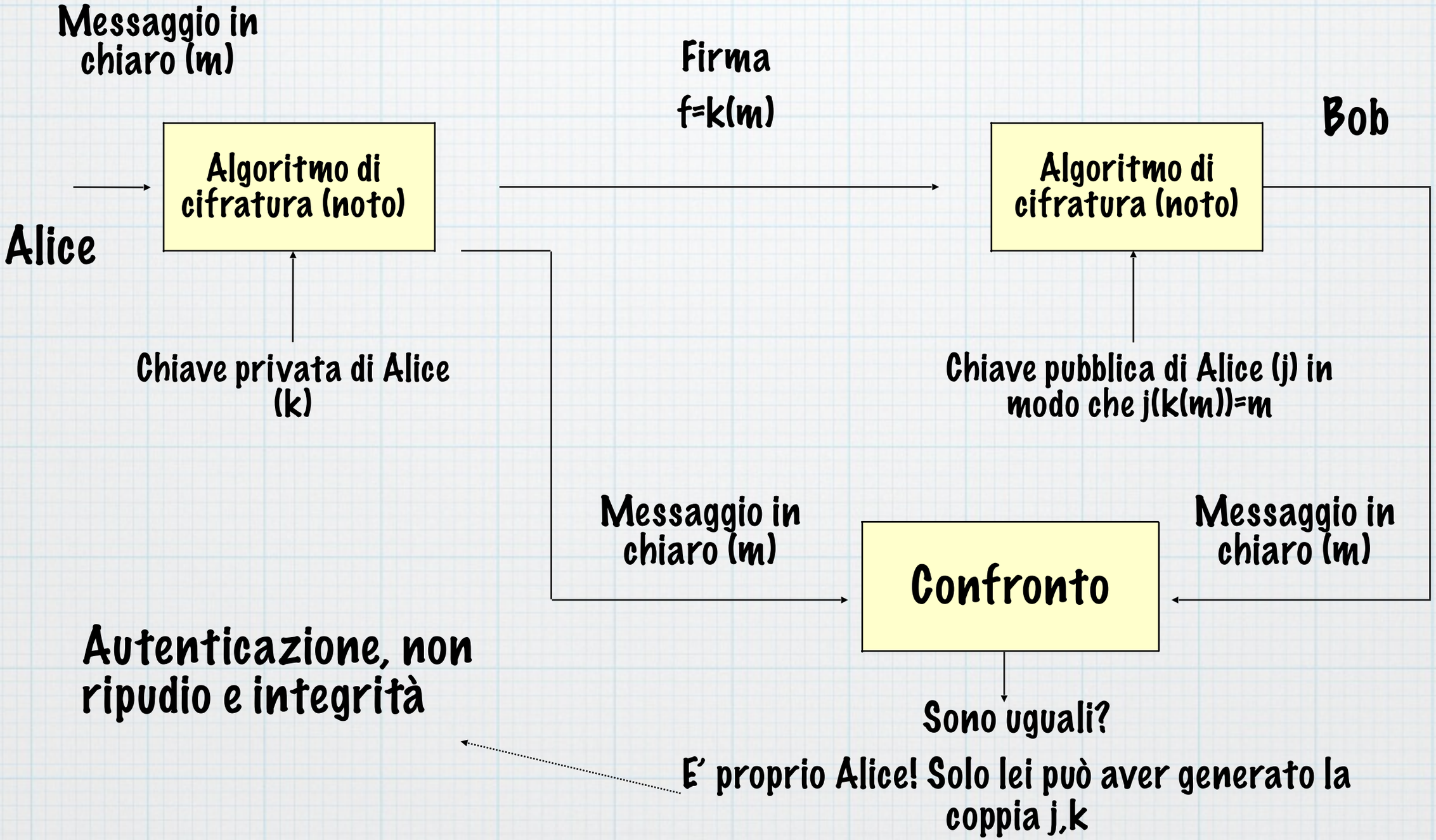
In realtà vale anche j(k(m))=m!! (firma elettronica, slide successiva)

Molto lenta! Elevamento a potenza: 1024 bit, qualche decina di kb al secondo!!!

Più sicura su reti pubbliche, ideale per Internet!

Sicurezza: non esistono algoritmi conosciuti per la fattorizzazione veloce di un numero

Firma Elettronica



Cifratura Simmetrica/ Asimmetrica

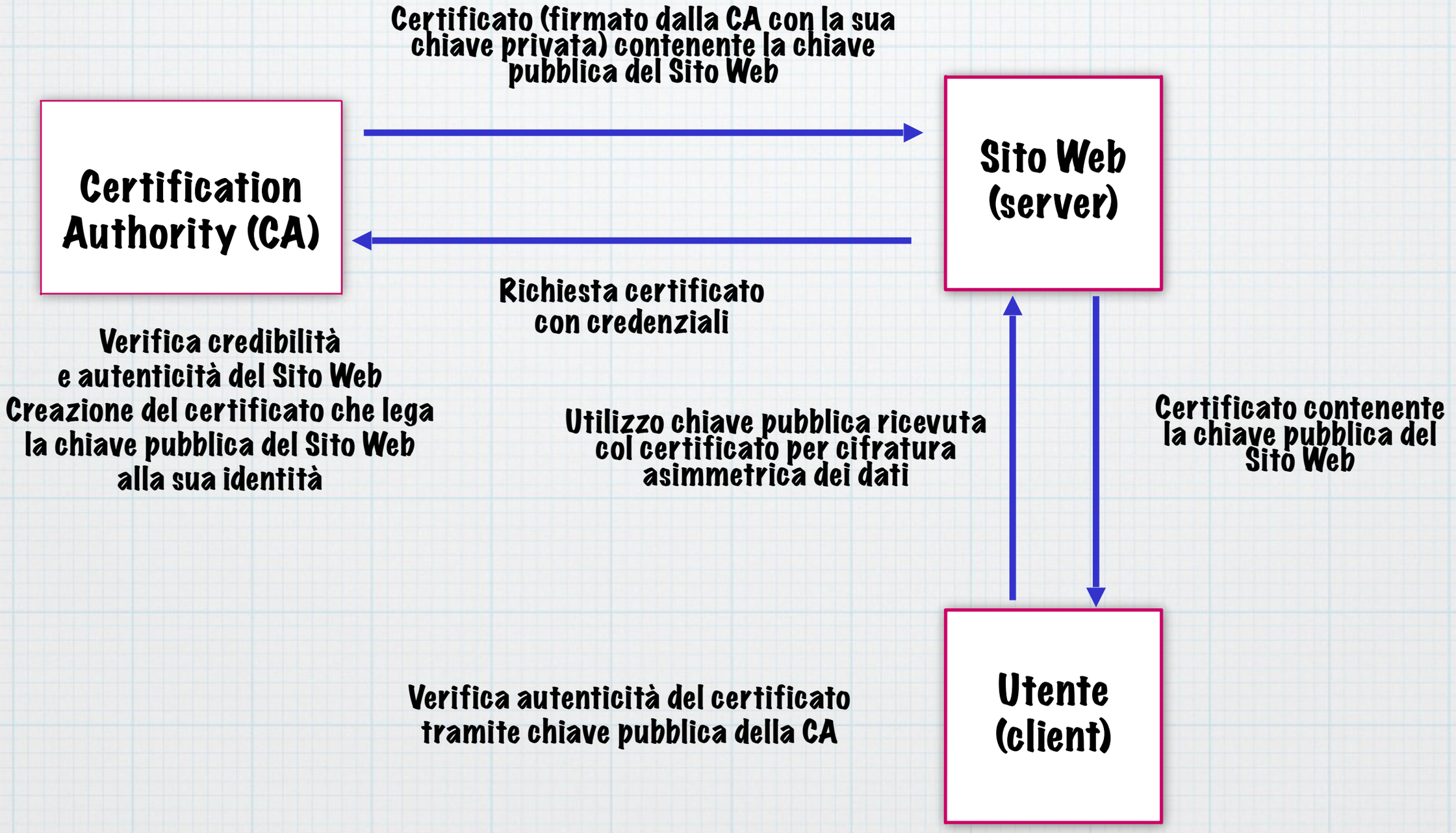
Cifratura simmetrica: veloce ma poco sicura su reti pubbliche per lo scambio della chiave

Cifratura asimmetrica: lenta ma sicura su reti pubbliche

Fase iniziale: scambio della chiave privata (di sessione) con cifratura asimmetrica (RSA)

Fase operativa di trasmissione dati: la chiave di sessione è stata consegnata con sicurezza, si può cifrare in modo simmetrico (DES) con la chiave di sessione, più veloce!

Certificato Digitale - CA



Open source e closed source

Open source e closed source

- Il software è originalmente associato al concetto di scienza
- La scienza deve circolare liberamente
- Il sorgente dei programmi deve essere libero

GNU is Not UNIX

- Sempre negli anni 80 nasce un movimento per riportare il software al concetto originario di conoscenza, guidato da **Richard M. Stallman**, fondatore della Free Software Foundation (FSF) e del Progetto GNU
- Stallman mette a punto la licenza GNU General Public License (GPL)
- Lo scopo dichiarato è quello di riportare il software (UNIX ma non solo) allo stato "libero"

La GPL

In sostanza, la GPL mira a garantire a chiunque possieda del software sotto di essa il diritto e la libertà di usarlo, copiarlo, modificarlo e ridistribuirne le versioni modificate, a patto di acconsentire a renderne disponibili i codici sorgenti e di non aggiungere restrizioni di qualsiasi tipo a tali versioni

Il problema del Kernel

- Nel 1990 il sistema GNU era praticamente completo, tranne un piccolo particolare: il kernel...
- Stallman e gli altri attendevano il rilascio di Mach, un microkernel sviluppato dalla Canergie-Mellon University e dalla University of Utah
- Nell'attesa accade qualcosa di veramente nuovo: nasce Linux

Linus Torvald

« Sto programmando un sistema operativo (gratuito e solo per hobby, non vuole essere grande e professionale come GNU) per cloni di AT 386(486). È in preparazione da aprile, e sta iniziando a funzionare. Mi piacerebbe sapere cosa vi piace e non vi piace in Minix, siccome il mio Sistema Operativo gli assomiglia in parte (fra le altre cose, lo stesso layout fisico del filesystem, per ragioni pratiche).

Ho convertito la shell bash (v.1.08) e GCC (v.1.40), e sembrano funzionare. Ciò denota che otterrò qualcosa di funzionante in pochi mesi e mi piacerebbe sapere quali funzionalità vuole la maggior parte della gente. Ogni suggerimento è ben accetto, anche se non posso promettervi che lo implementerò. »

25 agosto 1991

Lo sviluppo del kernel

- La maggiore innovazione di Linux è stato il metodo di sviluppo

The Cathedral and the Bazaar (Raymond)

- Cattedrale: pochi esperti scrivono il codice isolati dal mondo. Le comunicazioni sono verticali.
- Bazaar: gli sviluppatori interagiscono fra loro, non ci sono limiti, chiunque può modificare qualunque cosa.

Linux nel 2014...

- Oggi esistono centinaia di distribuzioni, dalle più diffuse (Mint, Ubuntu, Debian, ecc.) alle più specifiche (Sabayon, Gentoo, ecc.)
- Android (kernel Linux) è ormai il più diffuso sistema operativo al mondo

Open Source - Applicativi

- GCC e tutta la famiglia di compilatori
- LibreOffice
- MySQL (MariaDB) - PostgreSQL
- ecc.

Open Source - Formati

- Il formato dei dati è importante
- Chi controlla il formato controlla intere economie

Sicurezza comportamentale

Sicurezza comportamentale

Il componente più cri… ma
informatic… normalu… o fra
…stiera e …

Sicurezza comportamentale

la navigazione

la password

la firma digitale

la posta elettronica

la PEC

HTTP e HTTPS
attenzione a Javascript e popup
S.O. e Browser aggiornati SEMPRE
il principio è "mai fidarsi"

Sicurezza comportamentale

la navigazione

la password

la firma digitale

la posta elettronica

la PEC

Paradigma della sicurezza:
qualcosa che si conosce
più qualcosa che si ha

Autenticazione a due vie
Scegliere una combinazione di
lettere, numeri ed errori

ESEMPIO:

croso131Sicureza

Sicurezza comportamentale

la navigazione

la password

la firma digitale

la posta elettronica

la PEC

Autenticità

Non ripudio

Integrità

Sicurezza comportamentale

la navigazione

la password

la firma digitale

la posta elettronica

la PEC

EMAIL = messaggio
sotto al tergicristallo
SPAM
SCAM
Link nelle email

Sicurezza comportamentale

la navigazione

la password

la firma digitale

la posta elettronica

la PEC

Risposta italiana

NON è uno standard internazionale

Portabilità non garantita

Poteva esser fatta meglio

Dobbiamo gestirla per forza

Sono paranoico...

...ma lo sarò "abbastanza"?

Conclusioni

Obiettivi di un attacco

accesso non autorizzato

scambio di identità

alterazione delle informazioni

cancellazione delle informazioni

alterazione dei permessi degli utenti

intercettazione di messaggi

modifica di messaggi

alterazioni delle funzionalità

Obiettivi di un attacco

accesso non autorizzato

scambio di identità

alterazione delle informazioni

cancellazione delle informazioni

alterazione dei permessi degli utenti

intercettazione di messaggi

modifica di messaggi

alterazioni delle funzionalità

Crittografia
(firma elettron

Obiettivi di un attacco

accesso non autorizzato

scambio di identità

alterazione delle informazioni

cancellazione delle informazioni

alterazione dei permessi degli utenti

intercettazione di messaggi

modifica di messaggi

alterazioni delle funzionalità

Backup e uso di web application

Obiettivi di un attacco

accesso non autorizzato

scambio di identità

alterazione delle informazioni

cancellazione delle informazioni

alterazione dei permessi degli utenti

intercettazione di messaggi

modifica di messaggi

alterazioni delle funzionalità

Grazie per l'attenzione!
Domande?

claudio@bizzarri.net