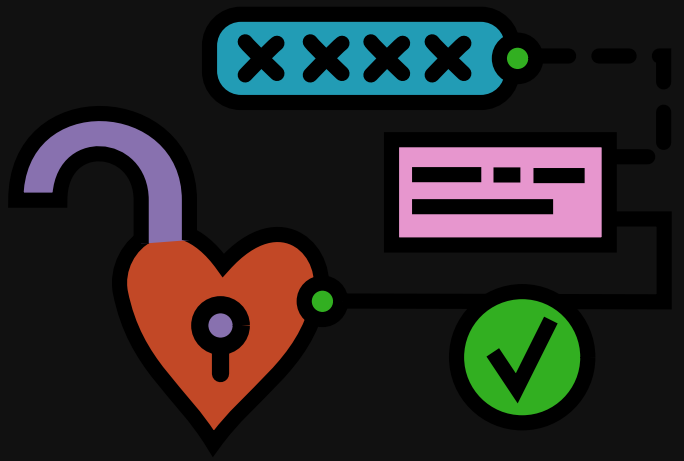
Un amore crittografico



Danilo Abbasciano

Agenda

- crittografia
- funzioni hash
- crittografia simmetrica
- salt
- crittografia asimmetrica
- firma elettronica
- PGP
- GnuPG
- certificati digitali e CA
- crittografia ibrida
- http + TLS = https

cosa è la crittografia

La crittografia è la base della protezione dei dati ed il modo più importante per garantire che le informazioni non possano essere rubate e lette.

crittografia moderna

principio di Kerckhoffs

la sicurezza di un crittosistema non dipende dal tenere segreto l'algoritmo crittografico, ma solo dal tenere segreta la chiave

massima di Shannon

un sistema dovrebbe essere progettato sotto l'assunzione che il nemico acquisirà immediatamente familiarità con esso

cosa può garantire la crittografia?

- **Riservatezza**: Può leggerlo solo il destinatario
- **Integrità**: Il messaggio non è stato alterato
- **Autenticità**: Il destinatario può verificare l'identità del mittente
- **Non ripudio**: L'autore del messaggio non potrà negare di averlo inviato

funzioni hash

una funzione prende in ingresso (input) dei parametri e restituisce un risultato (output)

Possiamo paragonarle alle funzioni matematiche che tutti conosciamo +, -, /, ...

In particolare la funzione **hash** prende un solo parametro in ingresso (come ad esempio la √)

proprietà funzione hash

- **unidirezionale**: Non esiste la funziona inversa

proprietà funzione hash

- unidirezionale
- **univoca**: identifica univocamente un messaggio

proprietà funzione hash

- unidirezionale
- univoca
- **deterministica**: Stesso messaggio stesso valore di hash

proprietà funzione hash

- unidirezionale
- univoca
- deterministica
- **lunghezza fissa dell'output** indipendente dalla lunghezza del messaggio in ingresso

proprietà funzione hash

- unidirezionale
- univoca
- deterministica
- lunghezza fissa dell'output
- **resistenza alla collisione** difficoltà nel creare due messaggi distinti con lo stesso hash

proprietà funzione hash

- unidirezionale
- univoca
- deterministica
- lunghezza fissa dell'output
- resistenza alla collisione
- **veloce** da calcolare

proprietà funzione hash

- **unidirezionale**: Non esiste la funziona inversa
- **univoca**: identifica univocamente un messaggio
- **deterministica**: Stesso messaggio stesso valore di hash
- **lunghezza fissa dell'output** indipendente dalla lunghezza del messaggio in ingresso
- **resistenza alla collisione** difficoltà nel creare due messaggi distinti con lo stesso hash
- **veloce** da calcolare

funzioni hash più comuni

algoritmo	dimensione output (Byte)	sicura
SHA-1	20	NO
MD5	16	NO
SHA256	32	SI
SHA512	64	SI

applicazioni funzione hash

Verifica dell'integrità di un messaggio/file

https://ftp.heanet.ie/mirrors/linuxmint.com/stable/21/

Index of /mirrors/linuxmint.com/stable/21

Name	Last modified	Size	Description
Parent Directory		-	
linuxmint-21-cinnamon-64bit.iso	2022-07-26 16:25	2.3G	
linuxmint-21-mate-64bit.iso	2022-07-26 18:10	2.3G	
linuxmint-21-xfce-64bit.iso	2022-07-26 19:57	2.2G	
sha256sum.txt	2022-07-29 12:24	286	
sha256sum.txt.gpg	2022-07-29 12:26	833	

```
f524114e4a10fb04ec428af5e8faf7998b18271ea72fbb4b63efe0338957c0f3
02a80ca98f82838e14bb02753bd73ee0da996c9cda3f027ae1c0ffb4612c8133
3ad001dc15cb661c6652ce1d20ecdc85a939fa0b4b9325af5d0c65379cc3b17e
```

applicazioni funzione hash

Verifica delle password

/etc/shadow

```
root:$y$j9T$bnWq/75L7bHk0xedMO1wc.$Ob6dLjepy.YFJz7rXyJHqbuyCCvuK
test:$y$j9T$T..Bgz0qQNR.LBX3jwUzd0$Avt8FhdlV6x2PWNQxC910.mcNkloK
```

Database

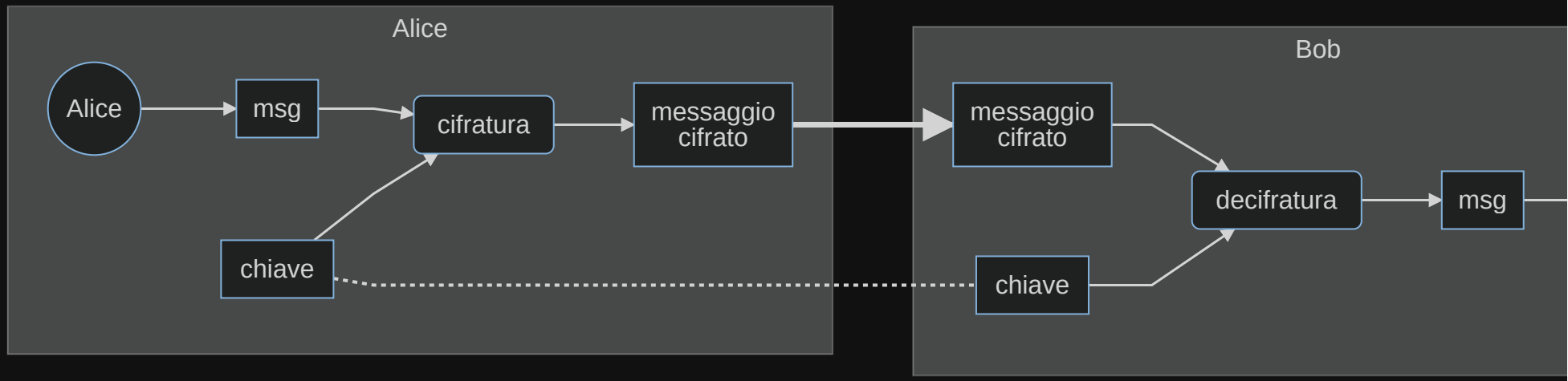
```
+------+-----------------------------------------------------
| NAME | PASSWORD
+------+-----------------------------------------------------
| io   | 1ec27867278516475080 85f26c5bff07159b8db7a8569be847afc58
+------+-----------------------------------------------------
```

applicazioni funzione hash

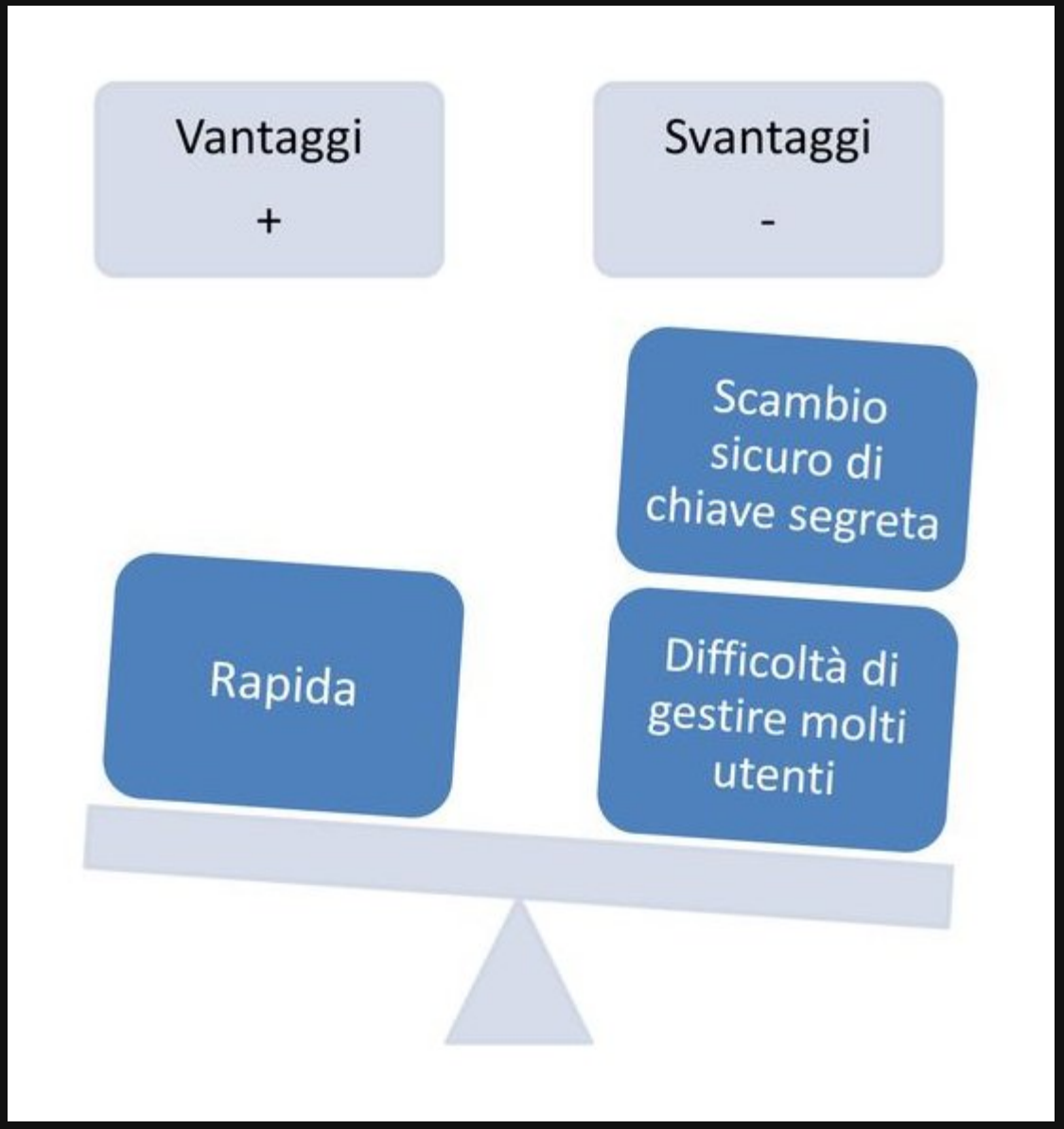
Identificare file o dati

crittografia simmetrica (o chiave privata)

la chiave di cifratura è uguale alla chiave di decifratura



crittografia simmetrica (o chiave privata)



Alice → Bob

chiave simmetrica

Rainbow table

una tabella precalcolata per memorizzare gli output di una funzione hash, in genere per decifrare gli hash delle password.

Un malintenzionato può utilizzare le rainbow table precalcolate per recuperare le password in chiaro.

crittografia simmetrica con salt

Una difesa comune contro questo attacco consiste nel calcolare gli hash utilizzando l'aggiunta di un "salt" alla password prima di eseguirne l'hashing.

Bob → Alice

chiave simmetrica con salt

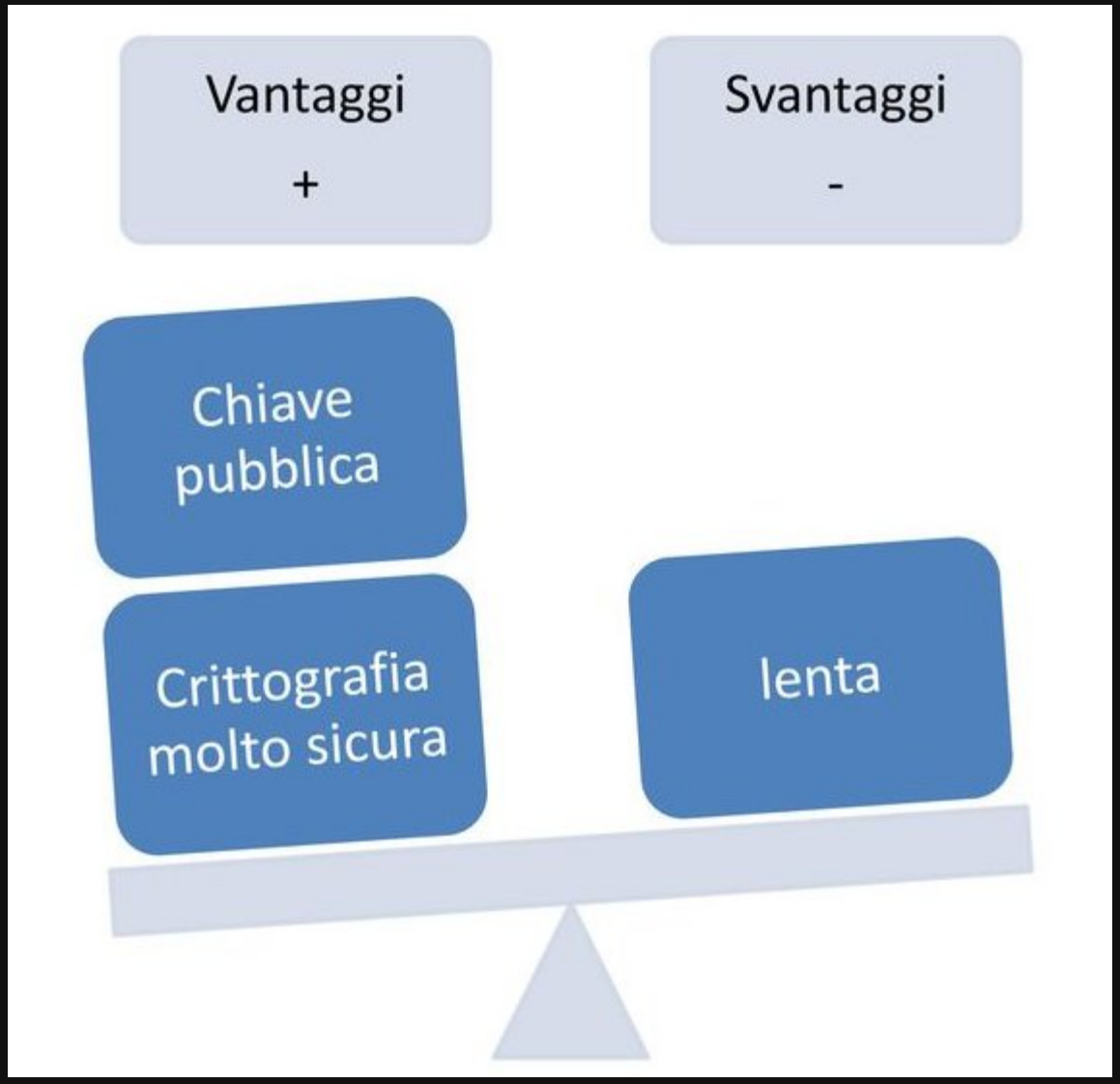
crittografia asimmetrica

(chiave pubblica e privata)

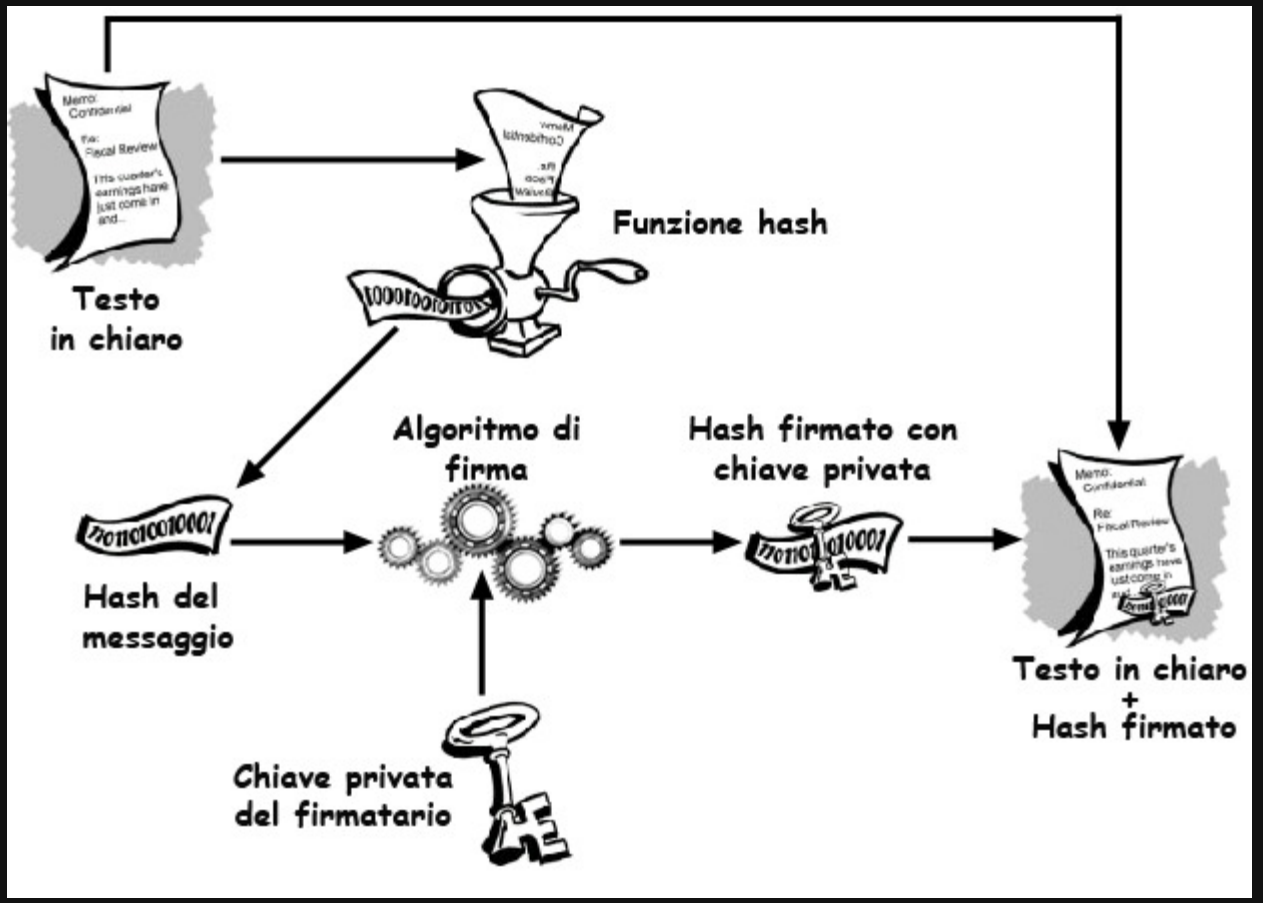
Ogni attore coinvolto ha una coppia di chiavi:

- **chiave pubblica**: deve essere distribuita
- **chiave privata**: appunto personale, segreta

crittografia asimmetrica



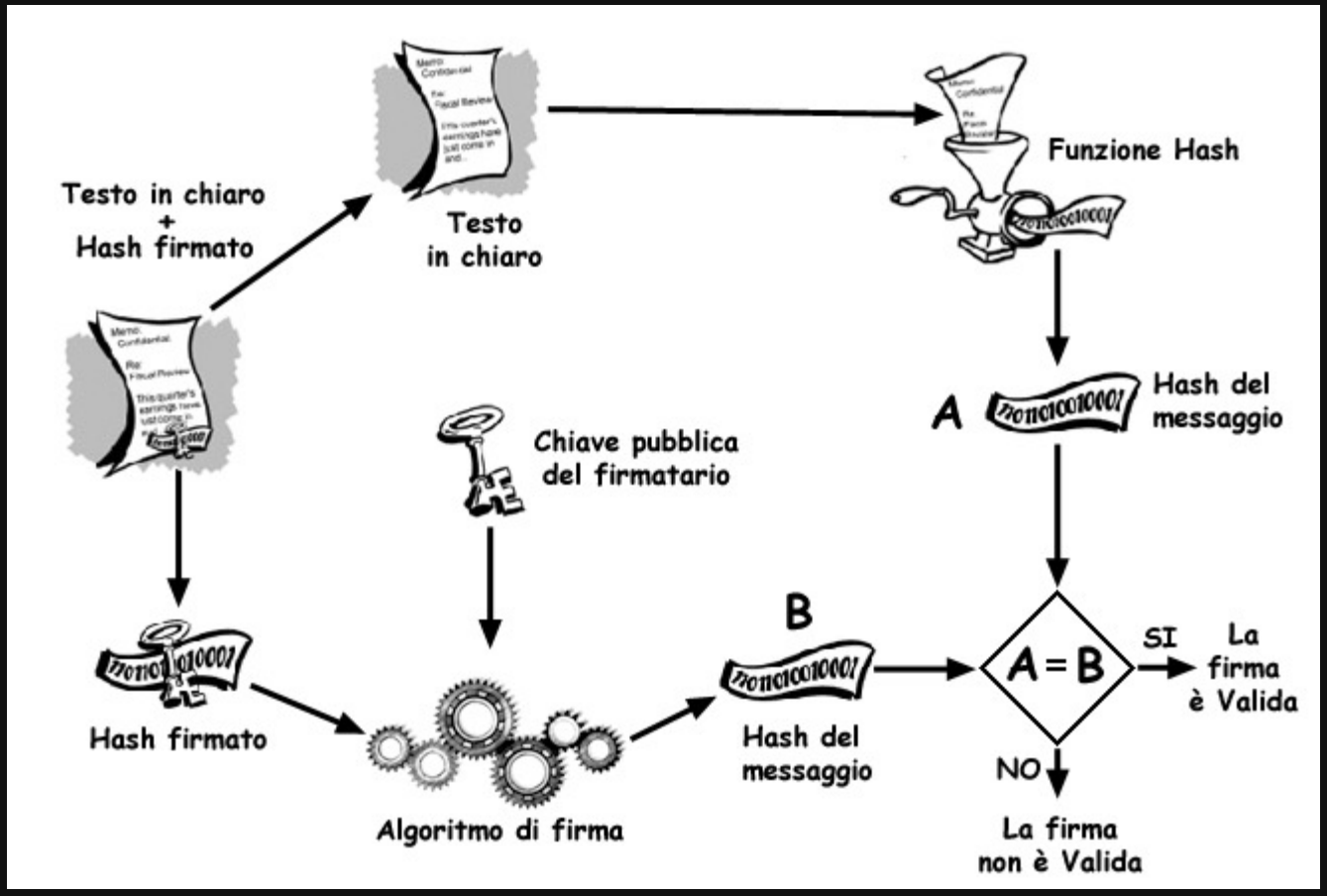
crittografia asimmetrica - firma elettronica



Alice → Bob

chiave assimmetrica (firma elettronica)

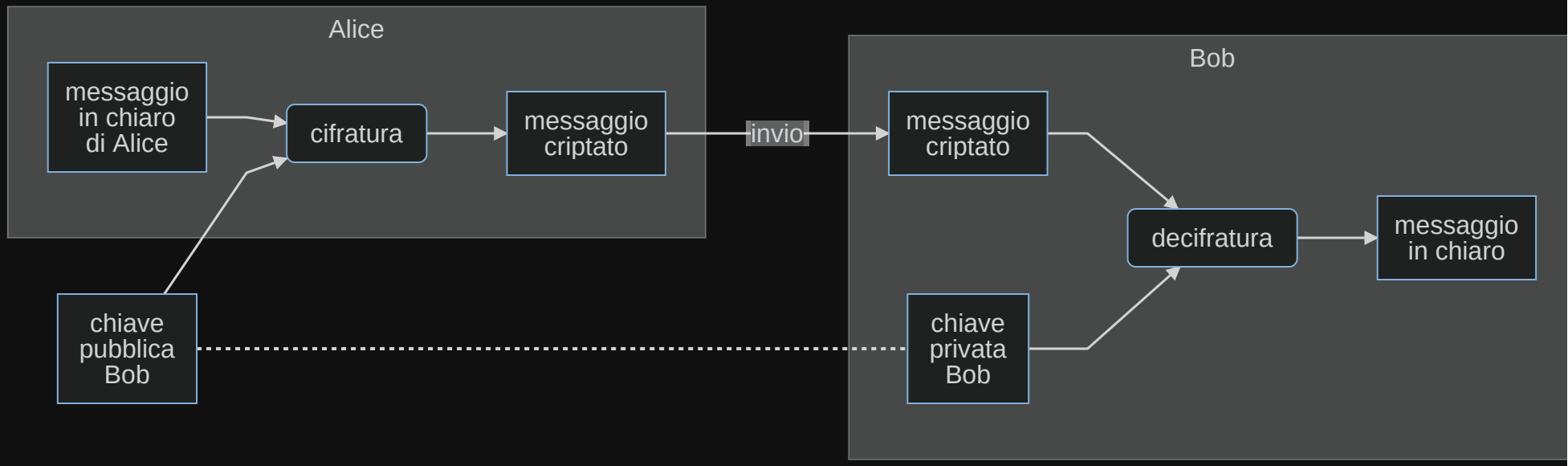
crittografia asimmetrica - verifica firma elettronica



Bob

chiave assimmetrica (verifica firma elettronica)

crittografia asimmetrica



Bob → Alice

demo crittografia asimmetrica (openssl)

PGP (Pretty Good Privacy)

Uno dei software che è divenuto molto famoso nell'ultimo decennio è il PGP (Pretty Good Privacy), sviluppato da *Phil Zimmermann* nel 1991.

Usato per la posta elettronica e la protezione dei file di uso personale che consente di firmare una e-mail lasciando il testo in chiaro, oppure cifrarla senza firmarla, o fare entrambe le cose.

GnuPG (GNU Privacy Guard)

GnuPG è un sistema crittografico che permette la cifratura/decifratura e autenticazione di messaggi. La cifratura/decifratura si basa su un sistema "ibrido" simile a quello usato da PGP con l'utilizzo combinato di algoritmi simmetrici e asimmetrici, ma non preclude la possibilità di cifrare/decifrare anche solo con algoritmi simmetrici.

Alice → Bob

GPG: cifratura e firma digitale

Bob → Alice

GPG e thunderbird

certificati digitali

Certificato digitale è documento che contiene:

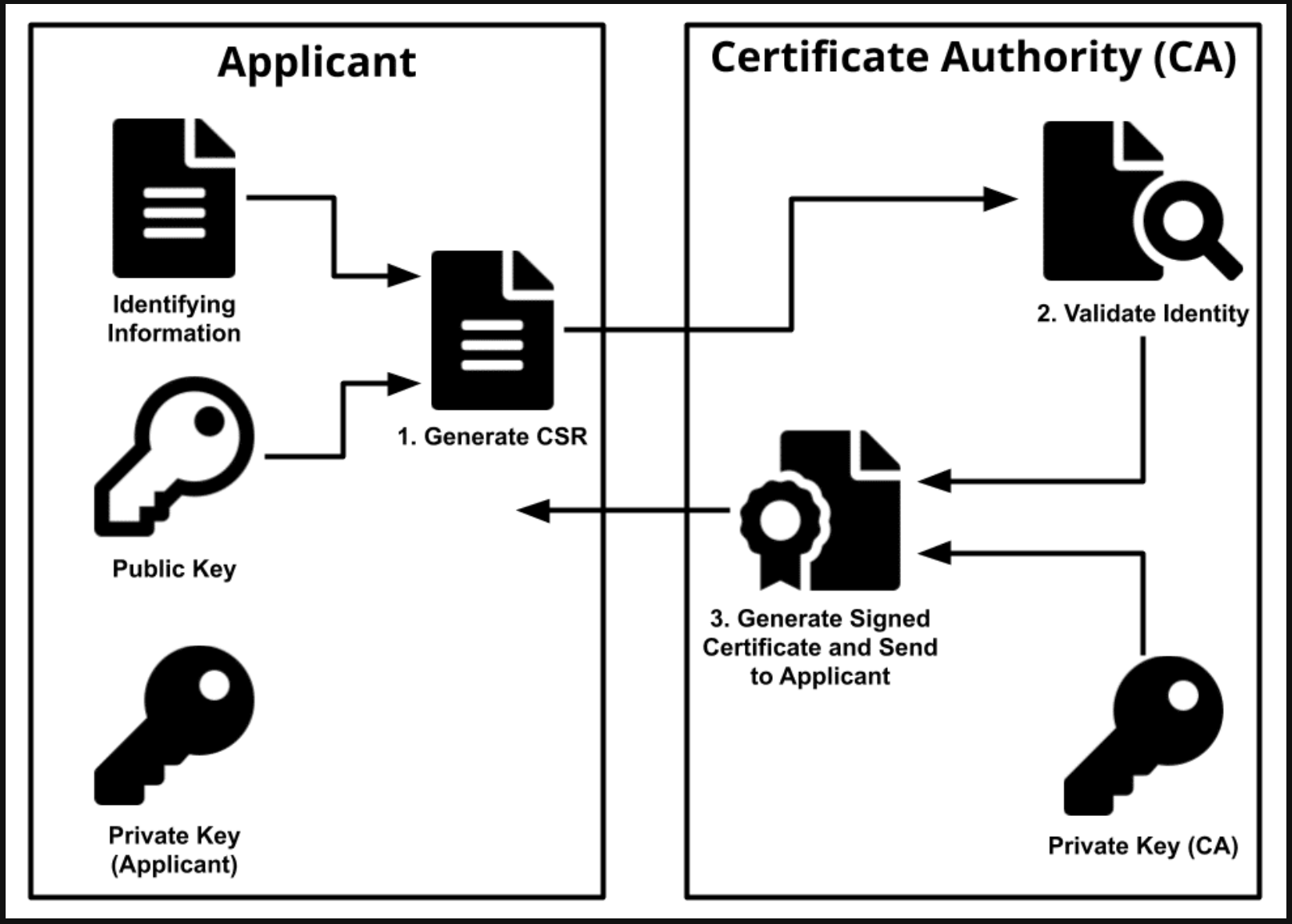
- la chiave pubblica
- dati del propretario
- firma digitale che ne garantisce la validità da parte di una CA (Certification Authority)

certificati digitali e CA (Certification Authority)

Certification Autority è un ente di certificazione:

- ha una coppia di chiavi che usa per validare i certificati
- registro pubblico dei certificati digitali emessi e tuttora validi

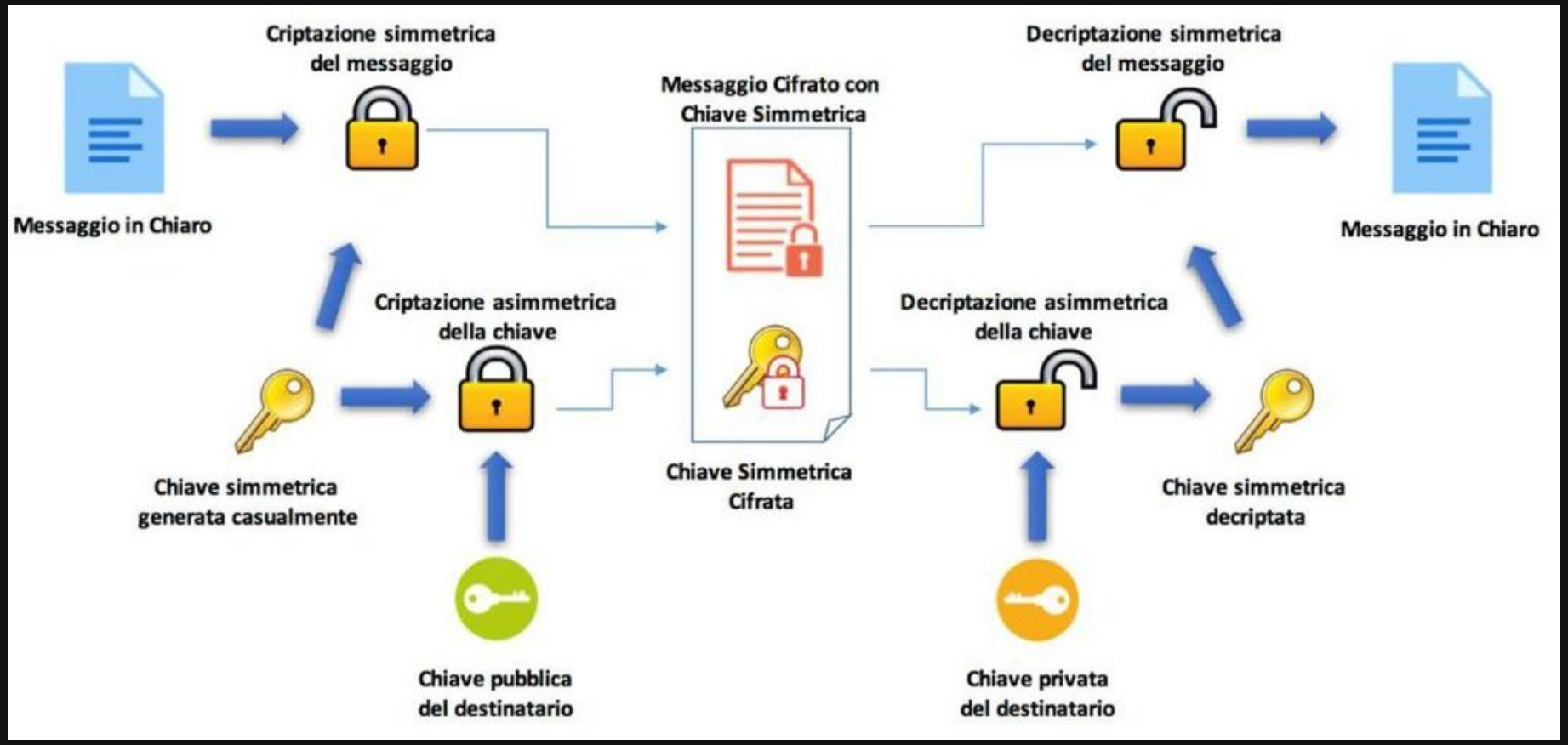
generazione certificato digitale



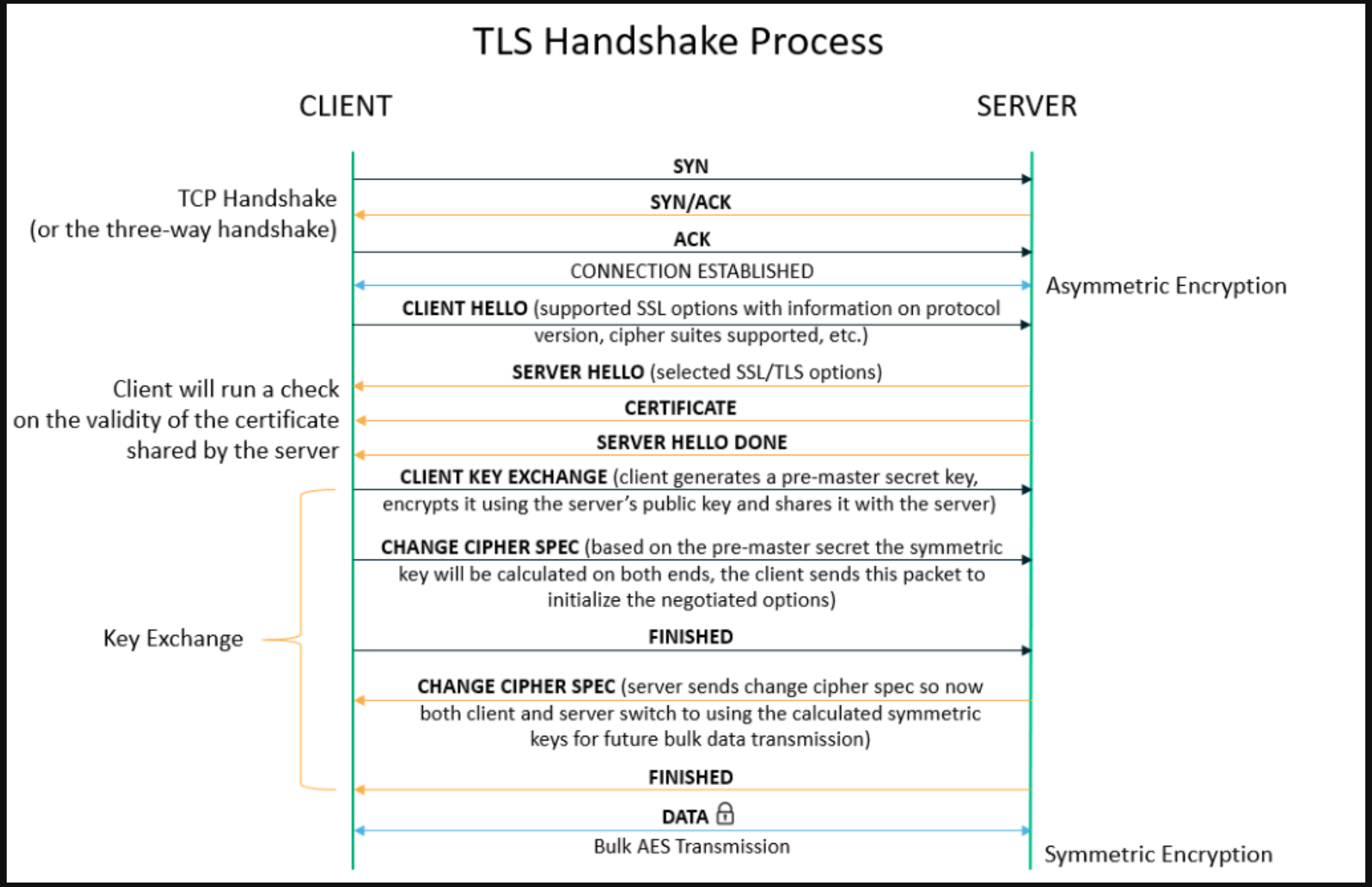
Alice

generazione certificato digitale

crittografia ibrida



comunicazioni sicure su Internet: https



... e vissero per sempre felici e criptati

danilo@piumalab.org

https://github.com/piuma/talk-amore-crittografico