

# Certificati digitali e hashing

## Sicurezza informatica

v 2.2 ~ mar 2021



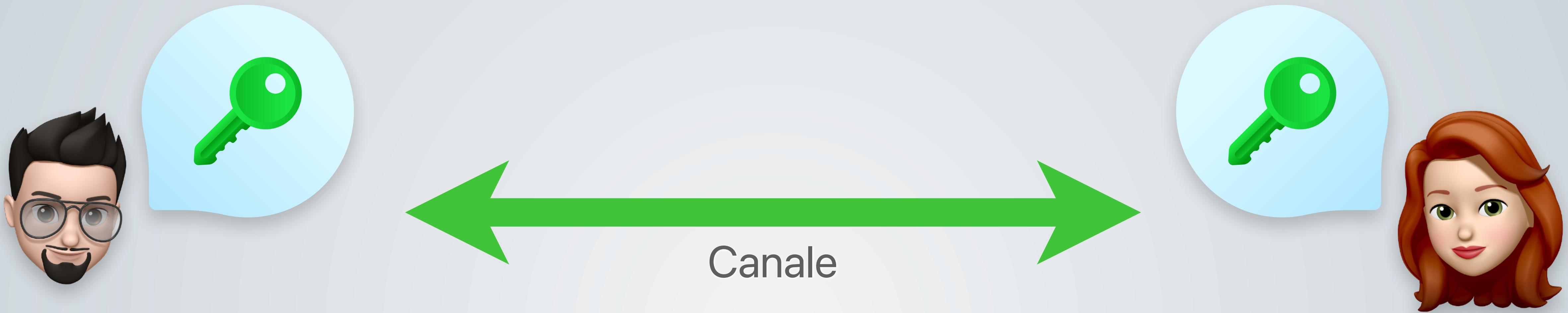
Prof. Marco Farina

[marco.farina@its-ictpiemonte.it](mailto:marco.farina@its-ictpiemonte.it)

[t.me/marcofarina](https://t.me/marcofarina)

in collaborazione con:

# Risolvere il Man-in-the-middle



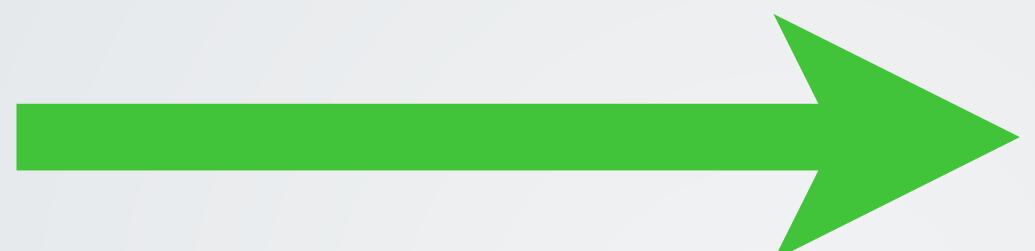
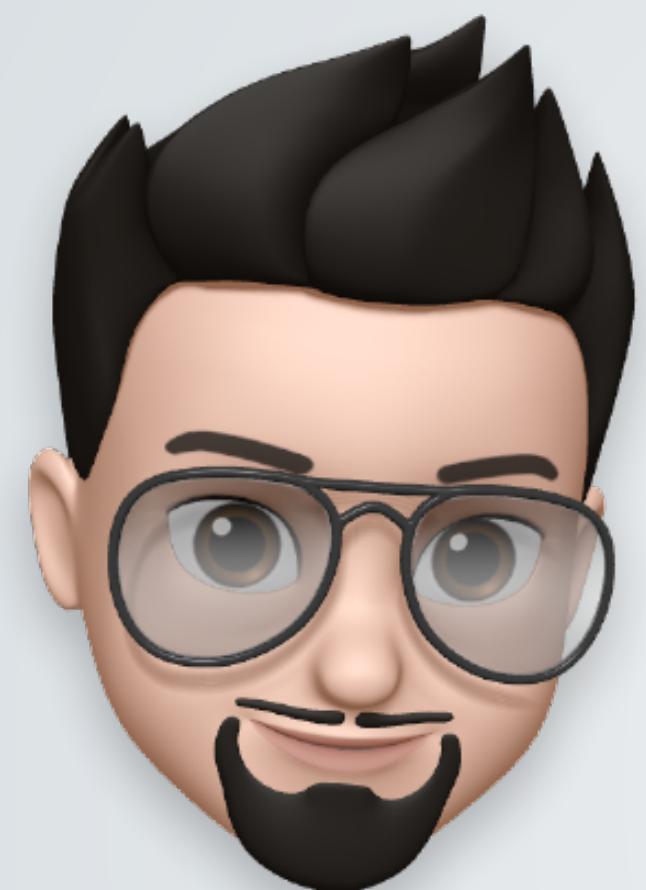
Come possiamo verificare che nessuno si sia messo in mezzo alla comunicazione?

**Verifica manuale**

**Certificazione**

(tra due lezioni...)

# Certificazione delle informazioni pubbliche



Chiave  
pubblica e  
info



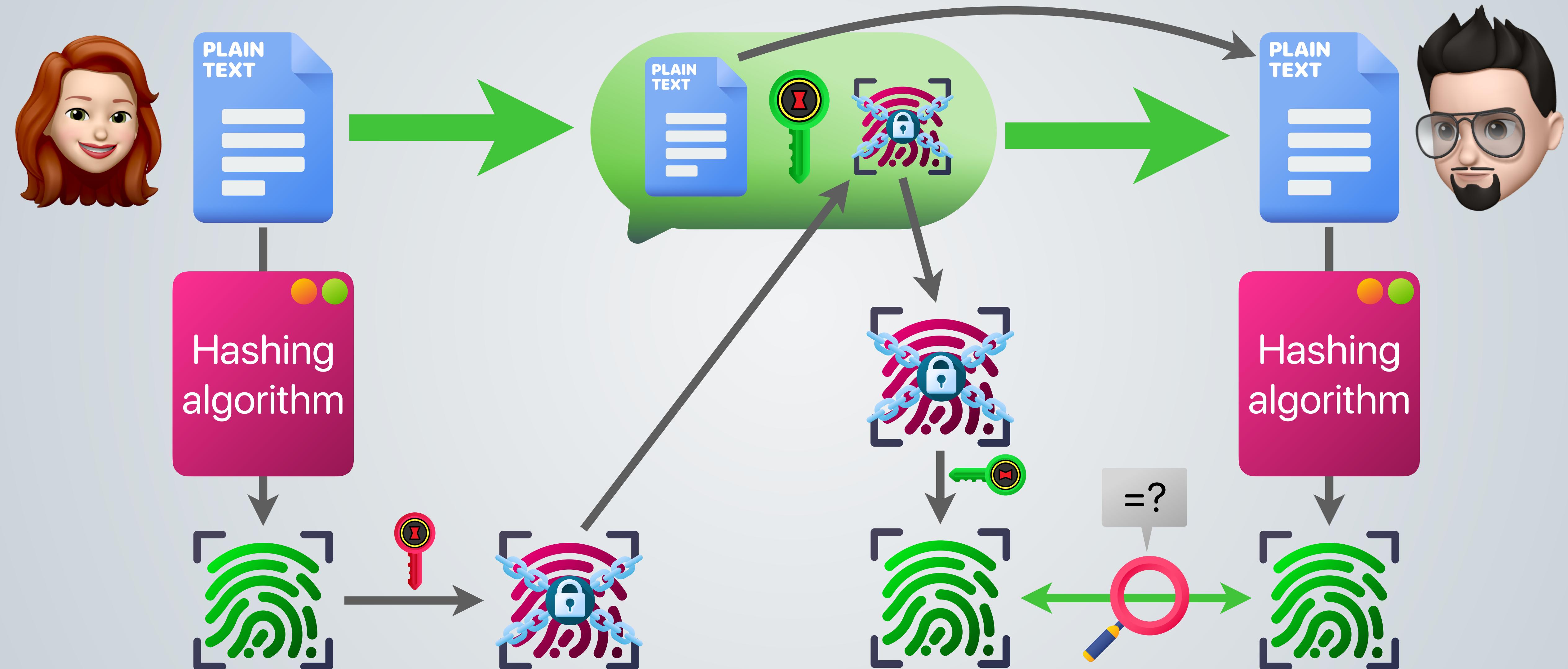
L'informazione pubblica può essere falsificata, quindi:

- viene distribuita all'interno di un certificato;
- il certificato è firmato digitalmente e non può essere contraffatto.



La firma digitale

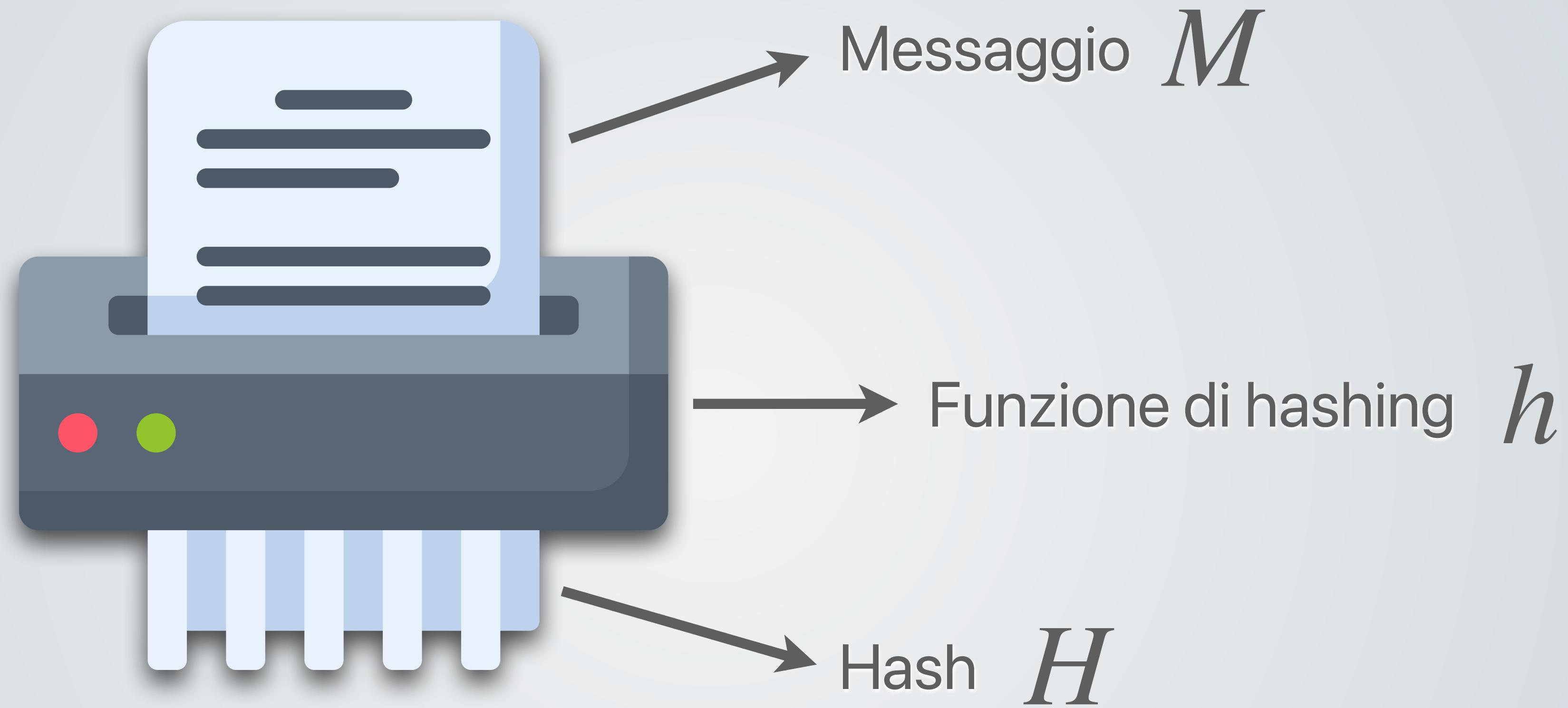
# La firma digitale





# Algoritmi di hashing

# Le funzioni di hashing



$$H = h(M)$$

# Le funzioni di hashing



L'hash è una **funzione non invertibile** che mappa una stringa di lunghezza arbitraria in una stringa di lunghezza predefinita.

1. A partire dall'hash non è possibile risalire alla stringa originale.

# Le funzioni di hashing



L'hash è una funzione non invertibile che mappa una stringa di **lunghezza arbitraria** in una stringa di lunghezza predefinita.

1. A partire dall'hash non è possibile risalire alla stringa originale.
2. L'input può essere di qualunque dimensione.

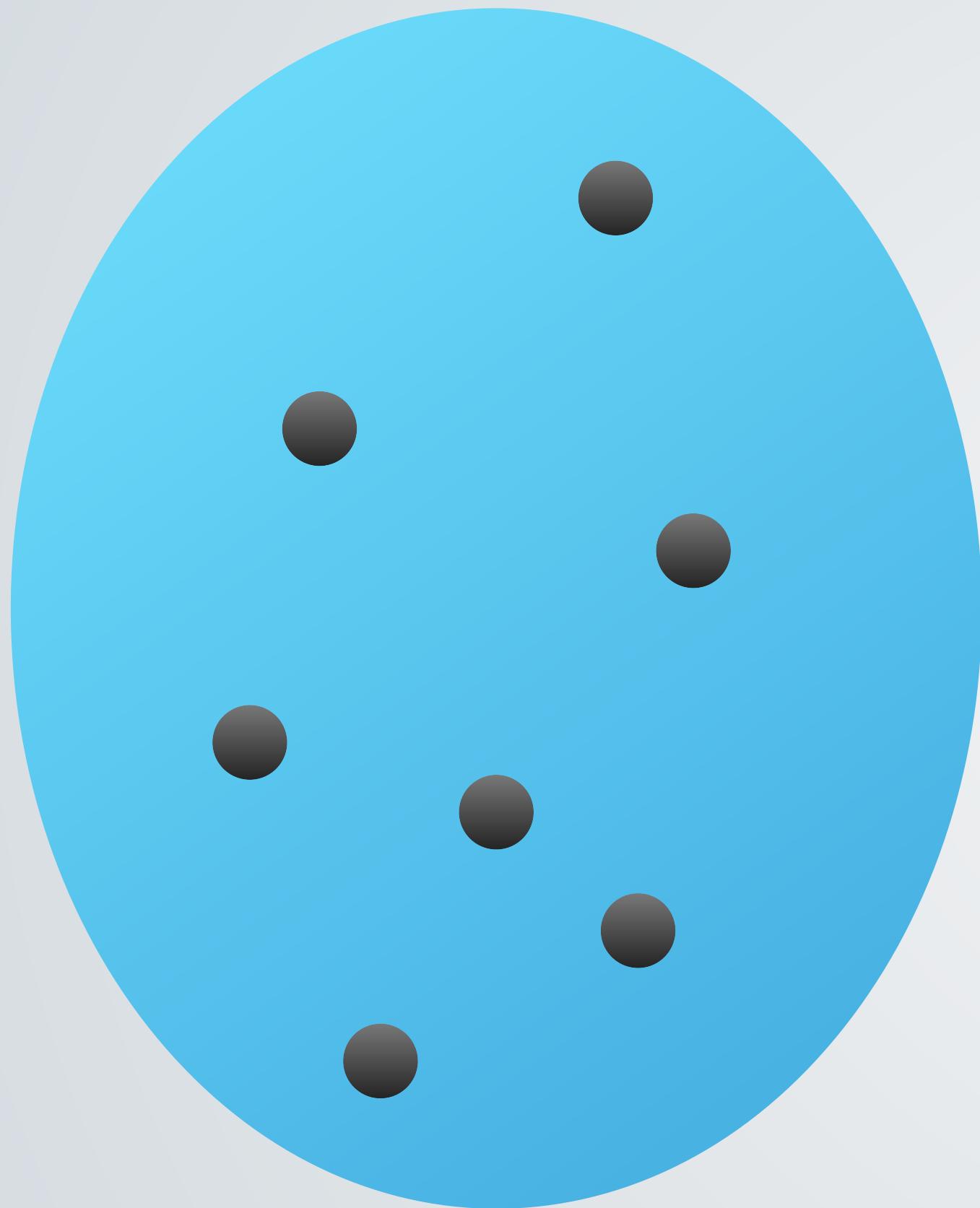
# Le funzioni di hashing



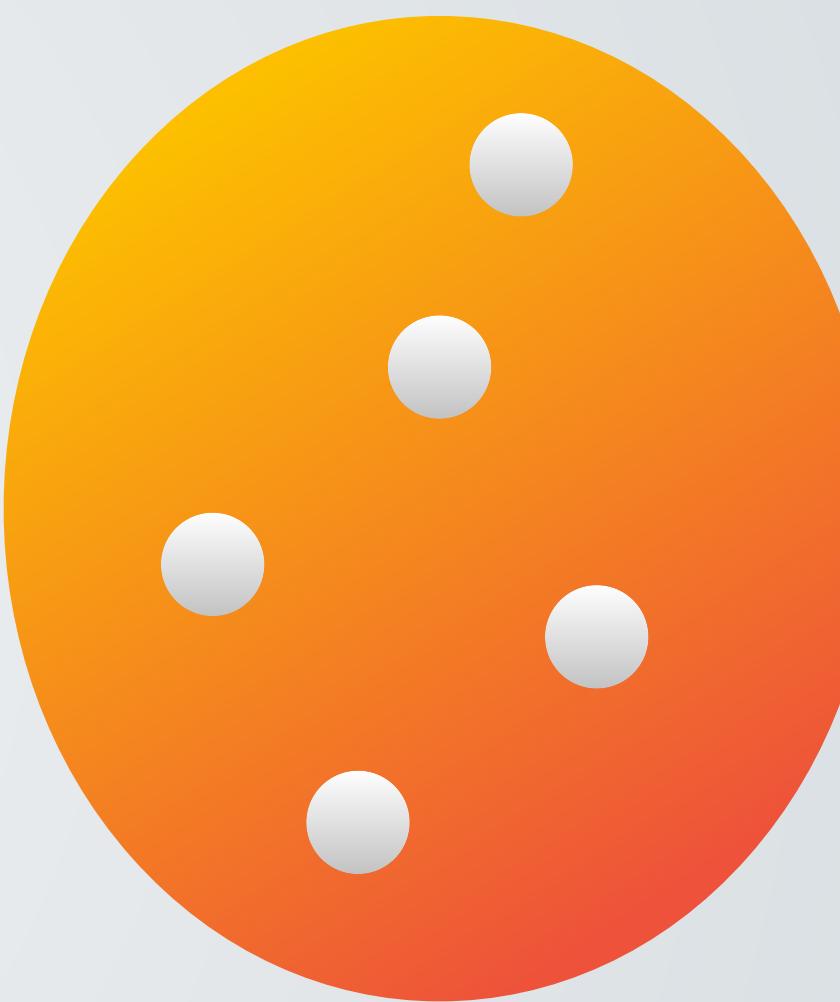
L'hash è una funzione non invertibile che mappa una stringa di lunghezza arbitraria in una stringa di **lunghezza predefinita**.

1. A partire dall'hash non è possibile risalire alla stringa originale.
2. L'input può essere di qualunque dimensione.
3. L'output ha una dimensione fissa.

# Qualquadra non cosa.

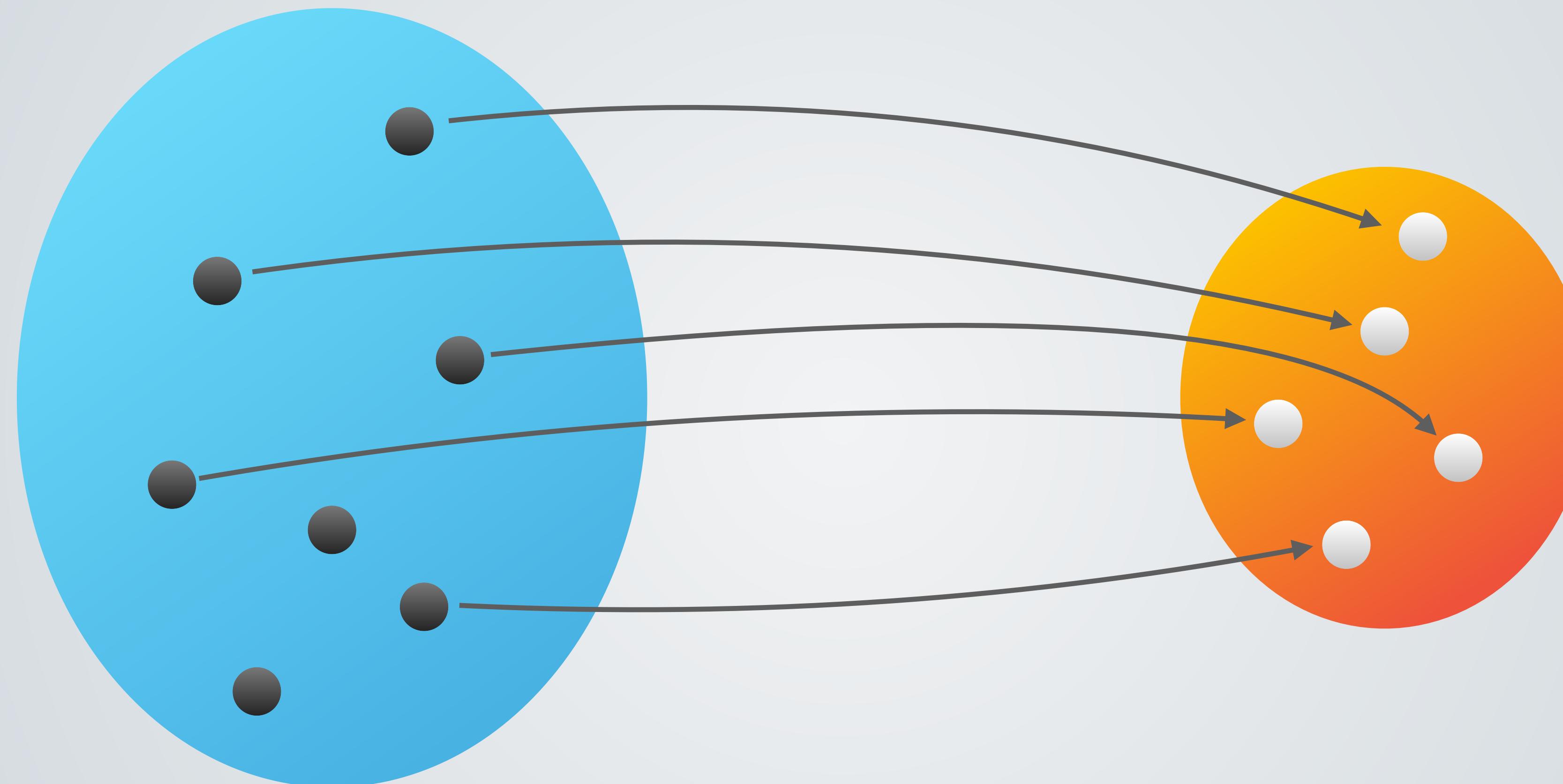


Tutti i messaggi  
possibili



tutti gli hash  
possibili.

# Qualquadra non cosa.

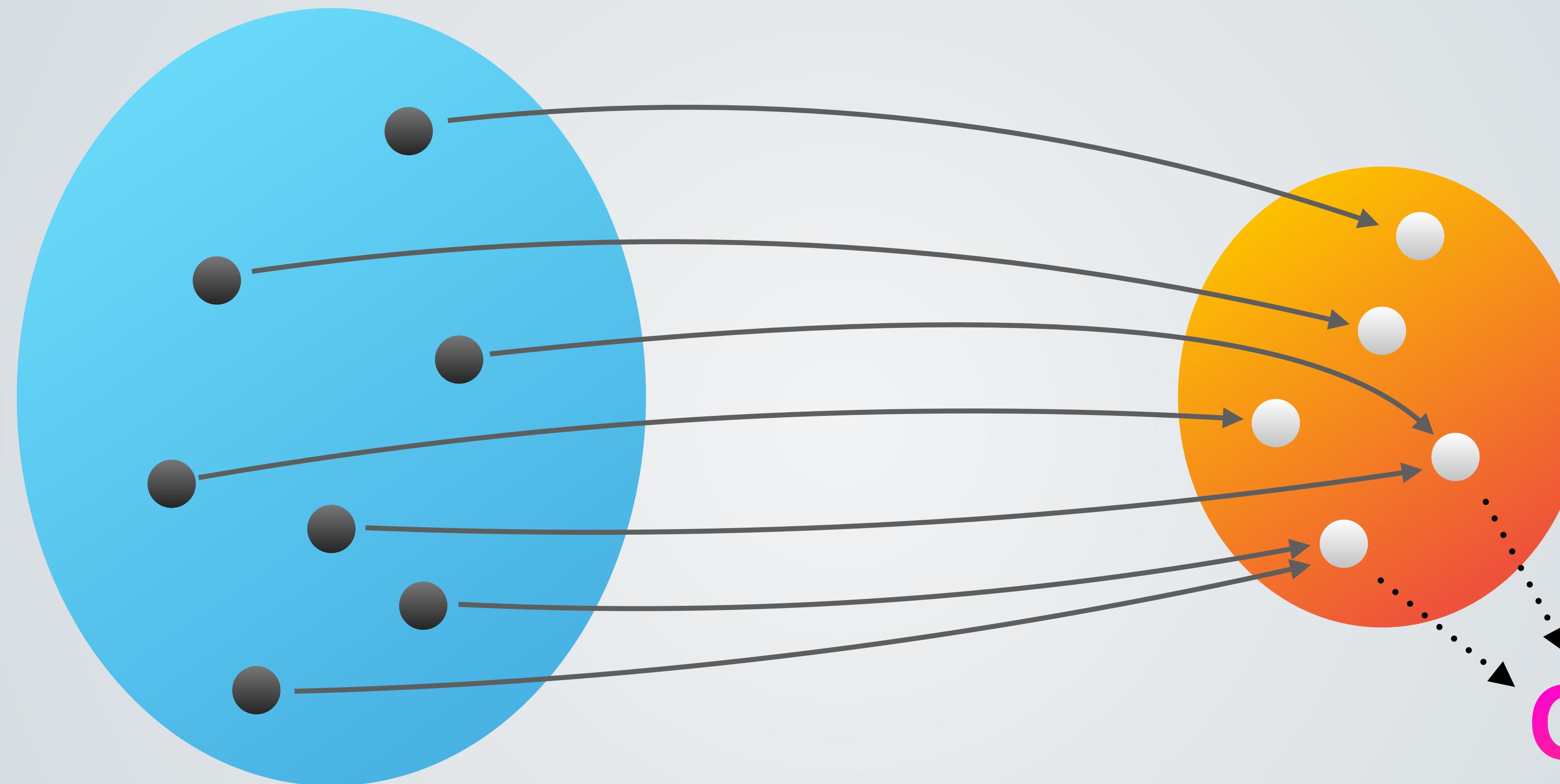


Tutti i messaggi  
possibili

sono di più di

tutti gli hash  
possibili.

# Qualquadra non cosa.



Tutti i messaggi  
possibili

sono di più di

tutti gli hash  
possibili.

# Resistenza alle collisioni

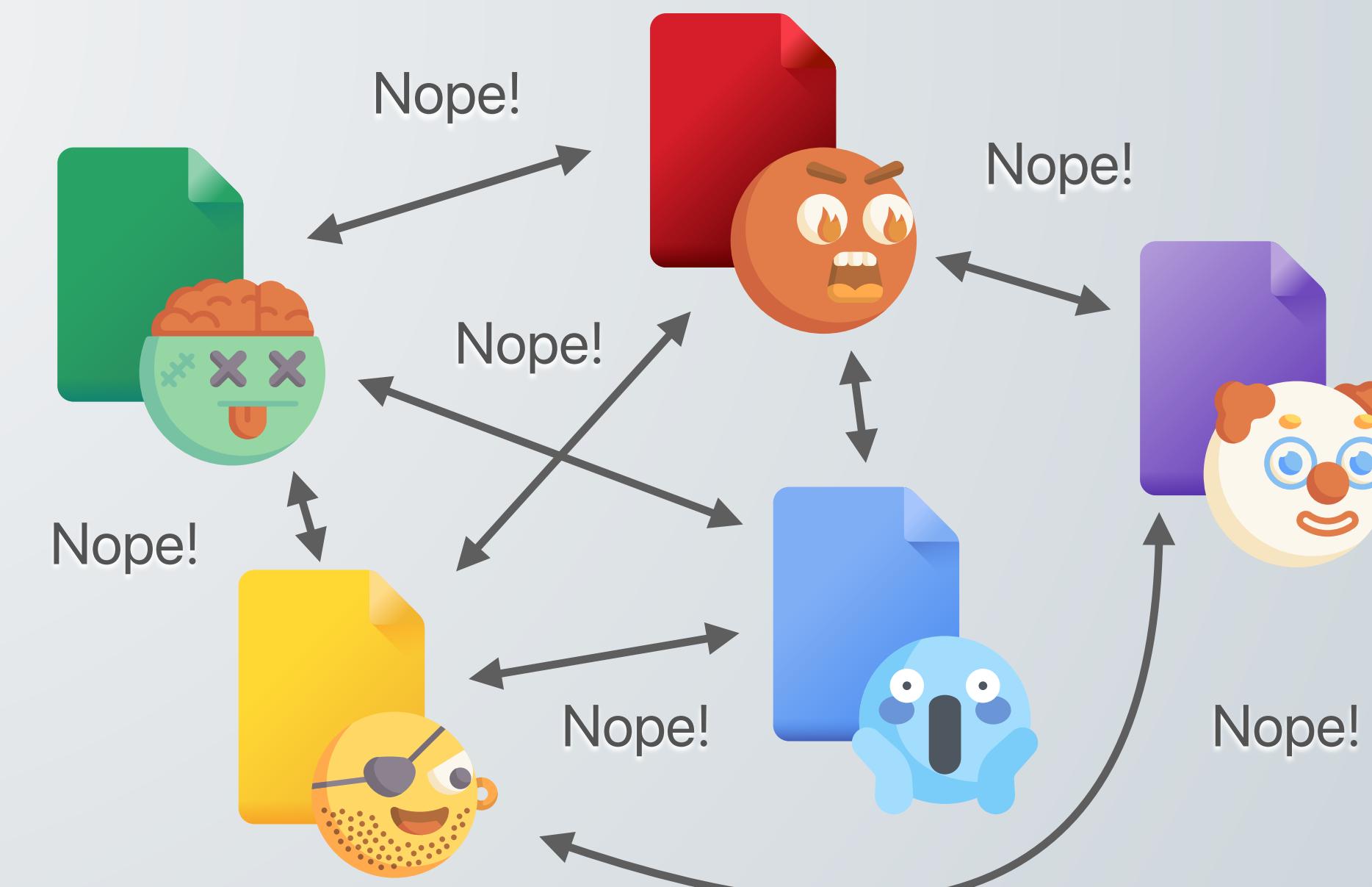
## Resistenza debole

Data una stringa  $x$  è computazionalmente impossibile trovare la stringa  $y \neq x$  tale che  $h(y) = h(x)$ .



## Resistenza forte

È computazionalmente impossibile trovare una qualsiasi coppia  $(x, y)$  tale che  $h(x) = h(y)$ .



# Una semplice funzione di hashing

Creiamo una funzione  $h(x)$  che prende in input  $n$  bit e restituisce un *digest* lungo 5.

**Input:** 101110100101011

10111  $\oplus$

01001  $\oplus$

01011 =

---

**Output:** 10101



W Questa funzione prende il nome di *controllo di ridondanza longitudinale*.

# Back in the days: MD5

**Anno:** 1991

**Autore:** Ron Rivest

**Input:** di qualunque lunghezza, ovviamente.

**Output:** 128 bit

**OpenSSL:** openssl dgst -md5 filename

**php:** md5(\$string)

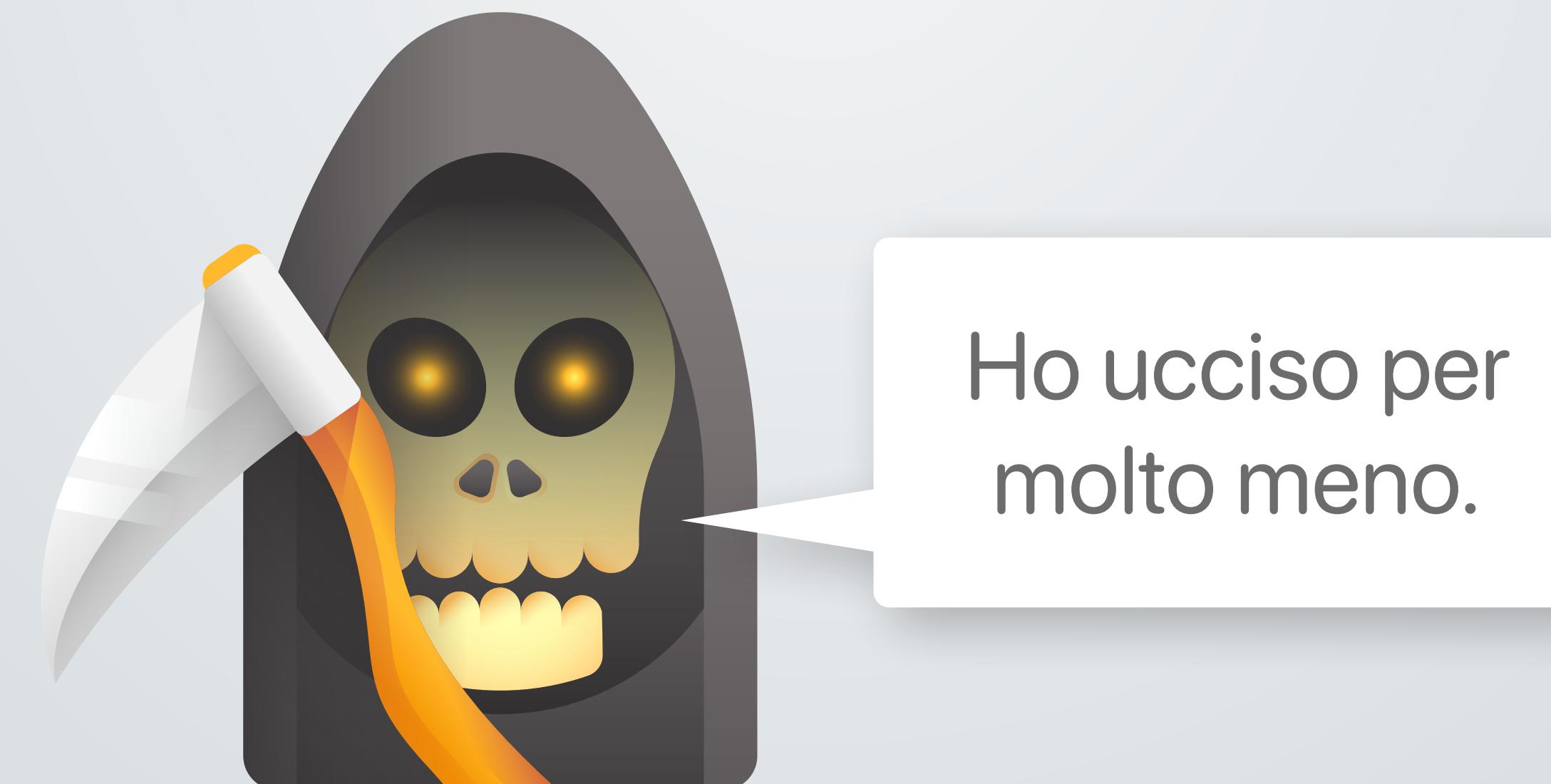
md5\_file(\$filename)



# PLEASE DON'T DO THAT

MD5 è **deprecato** per qualunque funzione di sicurezza.

```
<?php  
$notSoSecureDigest = md5("monkey");  
$suchStringMuchSecurity = md5(md5("monkey"));  
$pleaseKillMeNow =  
md5(md5(md5(md5(md5(md5(md5(md5(md5(md5(md5("monkey"))))))))));  
?>
```



# Secure Hash Algorithm

SHA è una famiglia di algoritmi.

## SHA-1

(deprecato dal 2011)

- Digital Certificate signatures
- Email PGP/GPG signatures
- Software vendor signatures
- Software updates
- ISO checksums
- Backup systems
- Deduplication systems
- GIT
- ...



[shattered.it](http://shattered.it)

## SHA-2

(2001)

- SHA-224
- SHA-256
- SHA-384
- SHA-512

`openssl dgst -sha256 filename`

## SHA-3

(2015)

- algoritmo Keccak

(Si pronuncia kæk,  
un po' come ketchup,  
ma con la k finale)

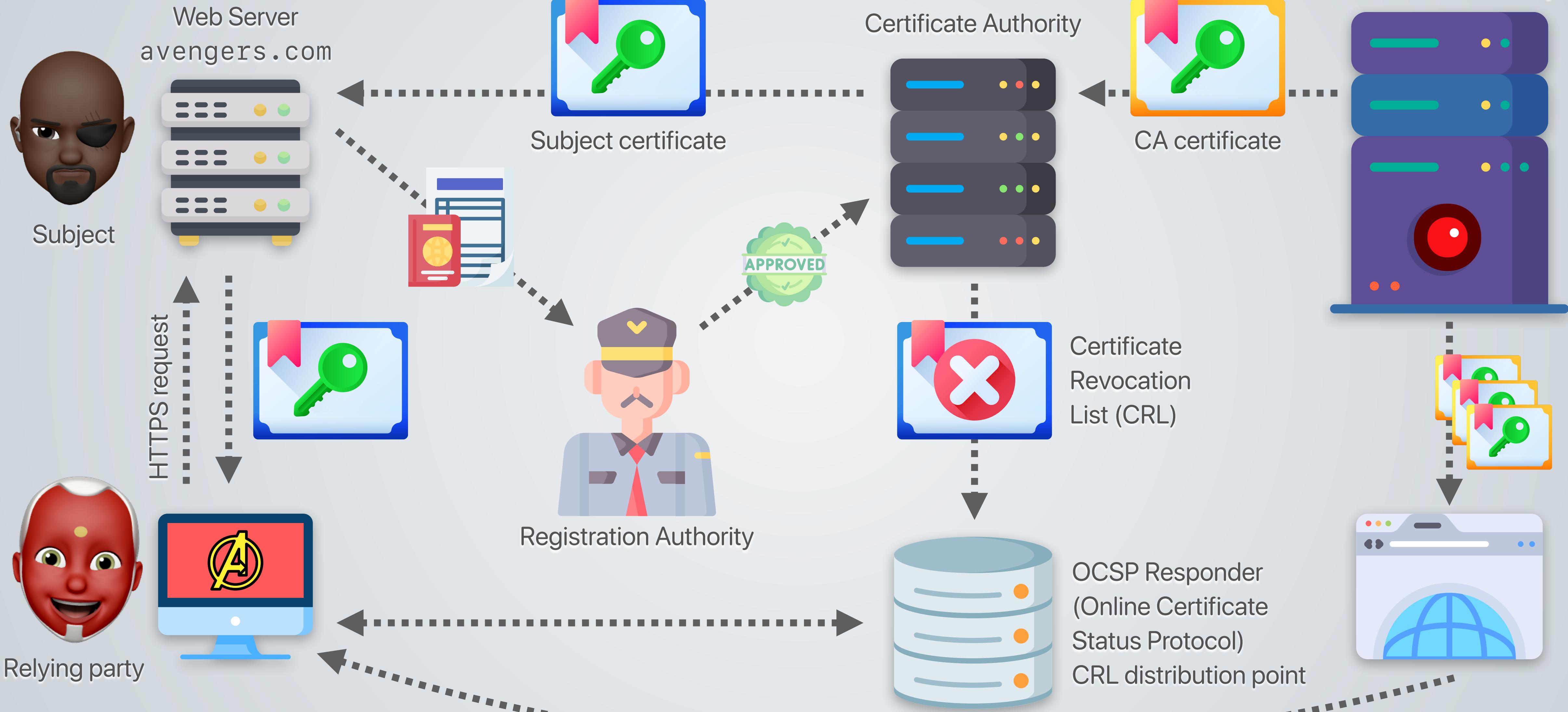


I certificati digitali

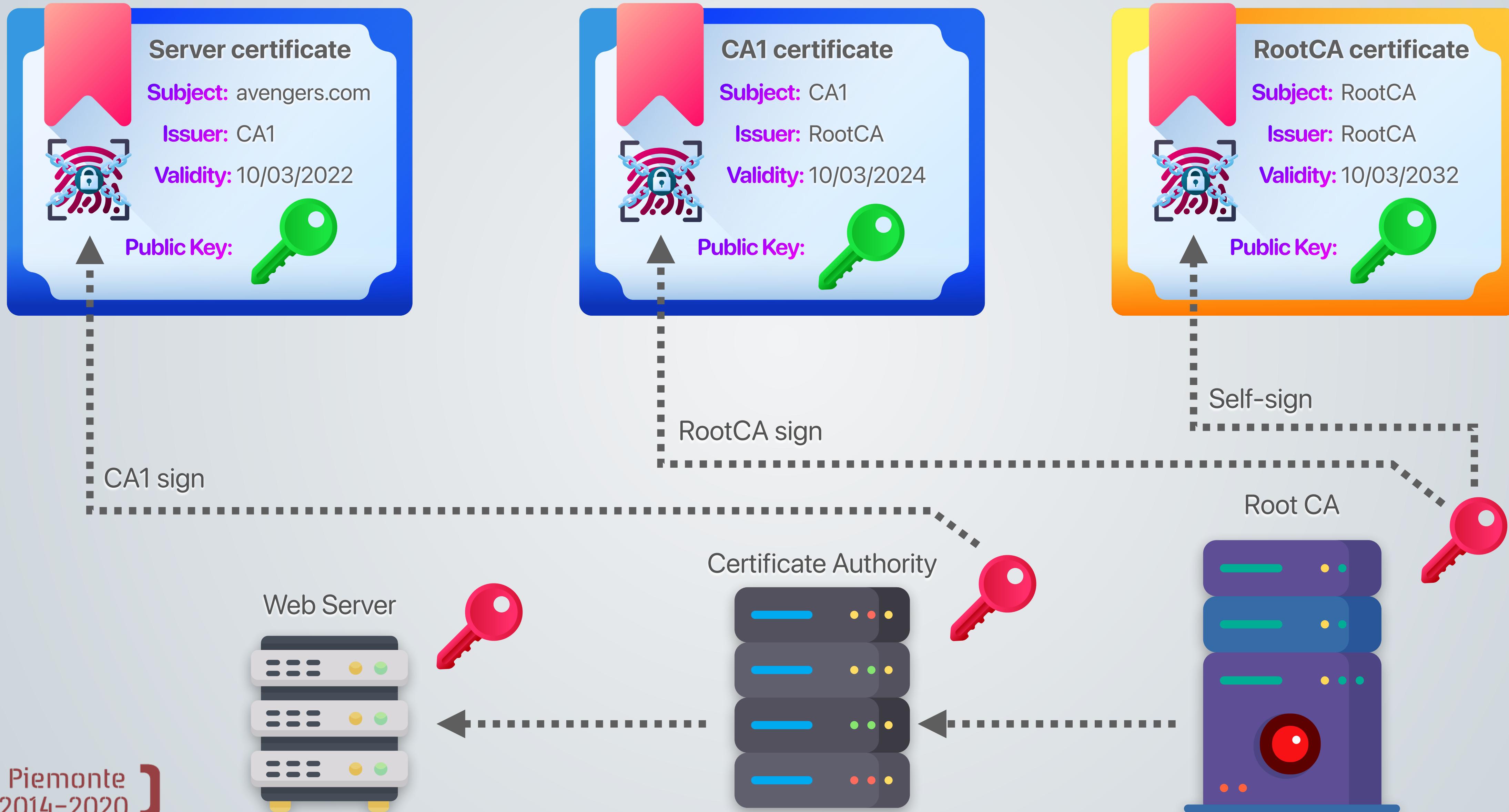
# Certificare la chiave pubblica



# Public Key Infrastructure



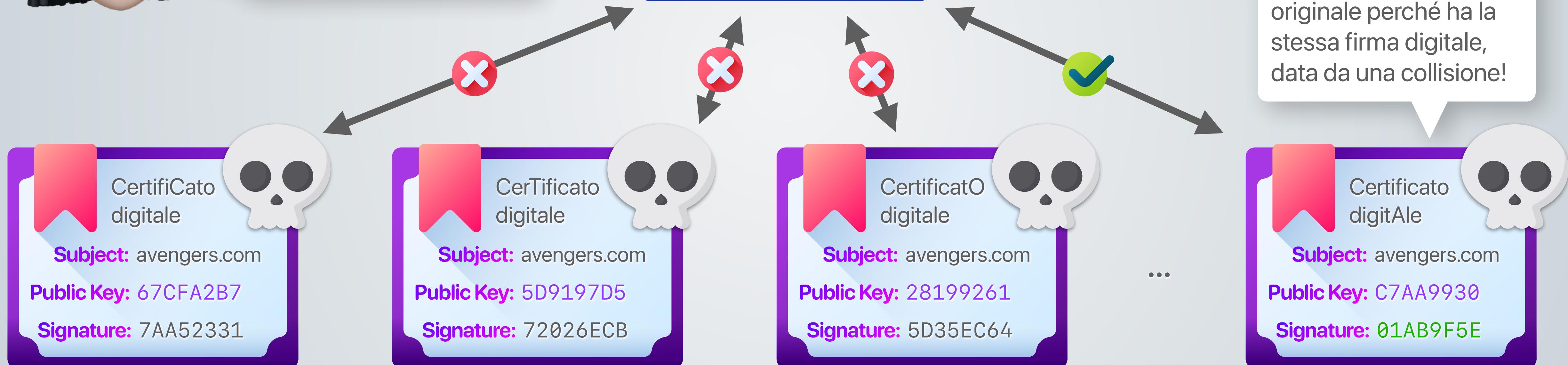
# X.509 Certificate issuance



# Perché le collisioni sono pericolose?



Se riuscissi a trovare una collisione potrei creare un certificato falso!

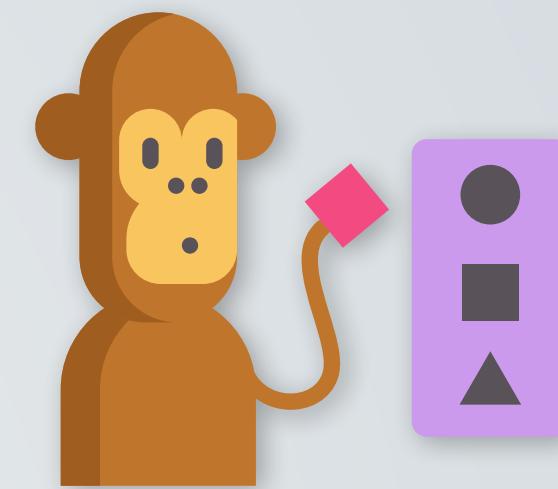
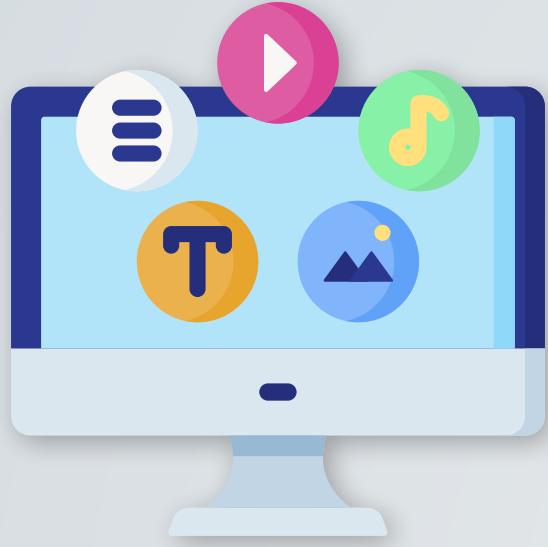


L'algoritmo di hash scelto è estremamente importante!



HTTPSeTLS

# Considerazioni sulla web security



## Complessità

I contenuti web sono straordinariamente complessi e possono nascondere problemi di sicurezza.

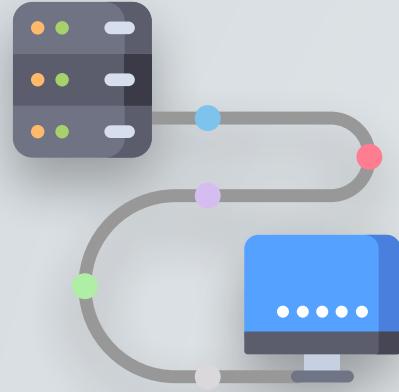
## Escalation

I server web possono essere exploitati e usati come trampolino verso la rete aziendale interna.

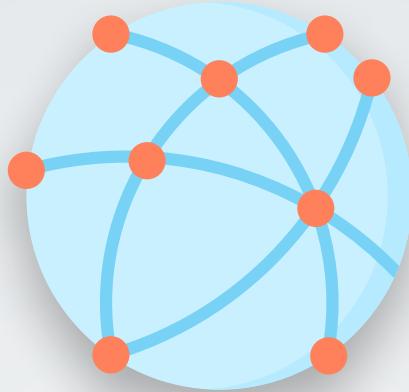
## Utonti

Gli utenti tipici dei servizi web non sono addestrati alle tematiche della security.

# Approcci alla web security



Network



Transport



Application

HTTP	FTP	SMTP
TCP		
IP/IP Sec		

HTTP	FTP	SMTP
TLS/SSL		
TCP		
IP		

S/MIME	HTTPS
Kerberos	SMTP
UDP	TCP
IP	

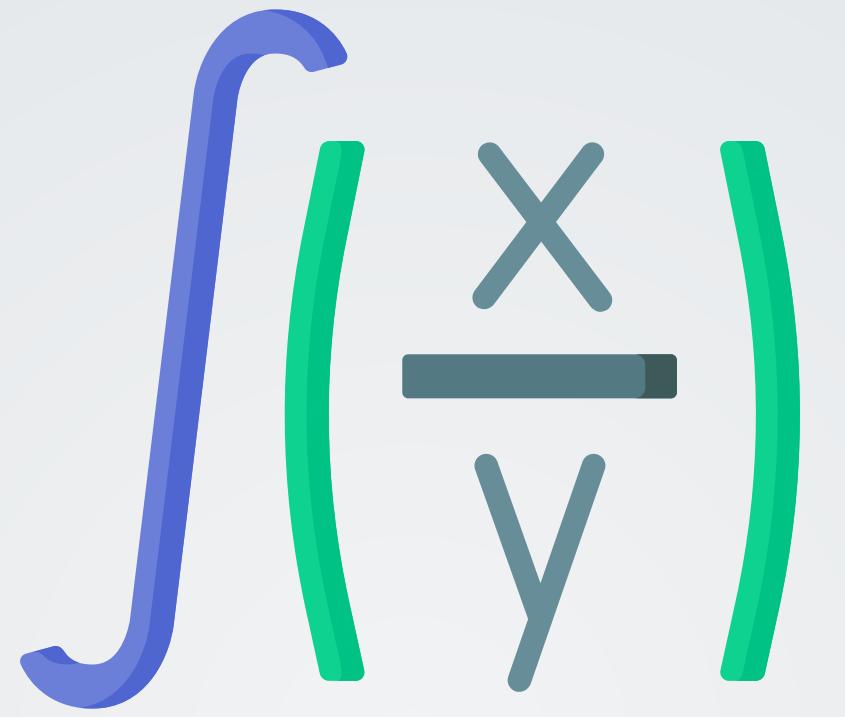
# Transport Layer Security

Sembri ingassato



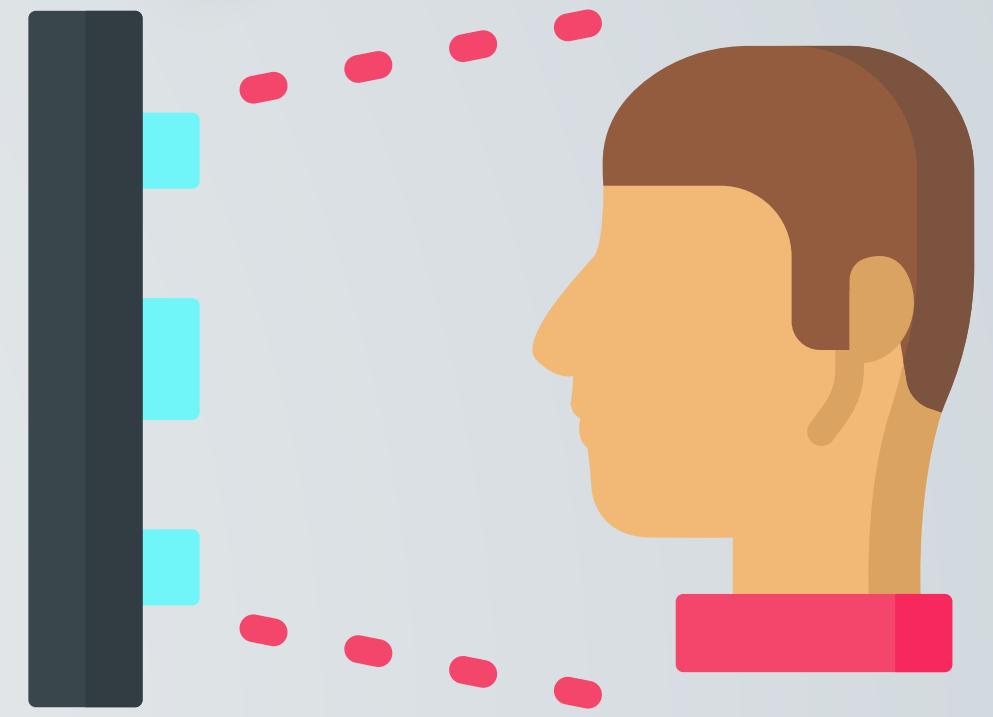
## Privacy

Algoritmi crittografici  
per nascondere il  
traffico dati.



## Integrità

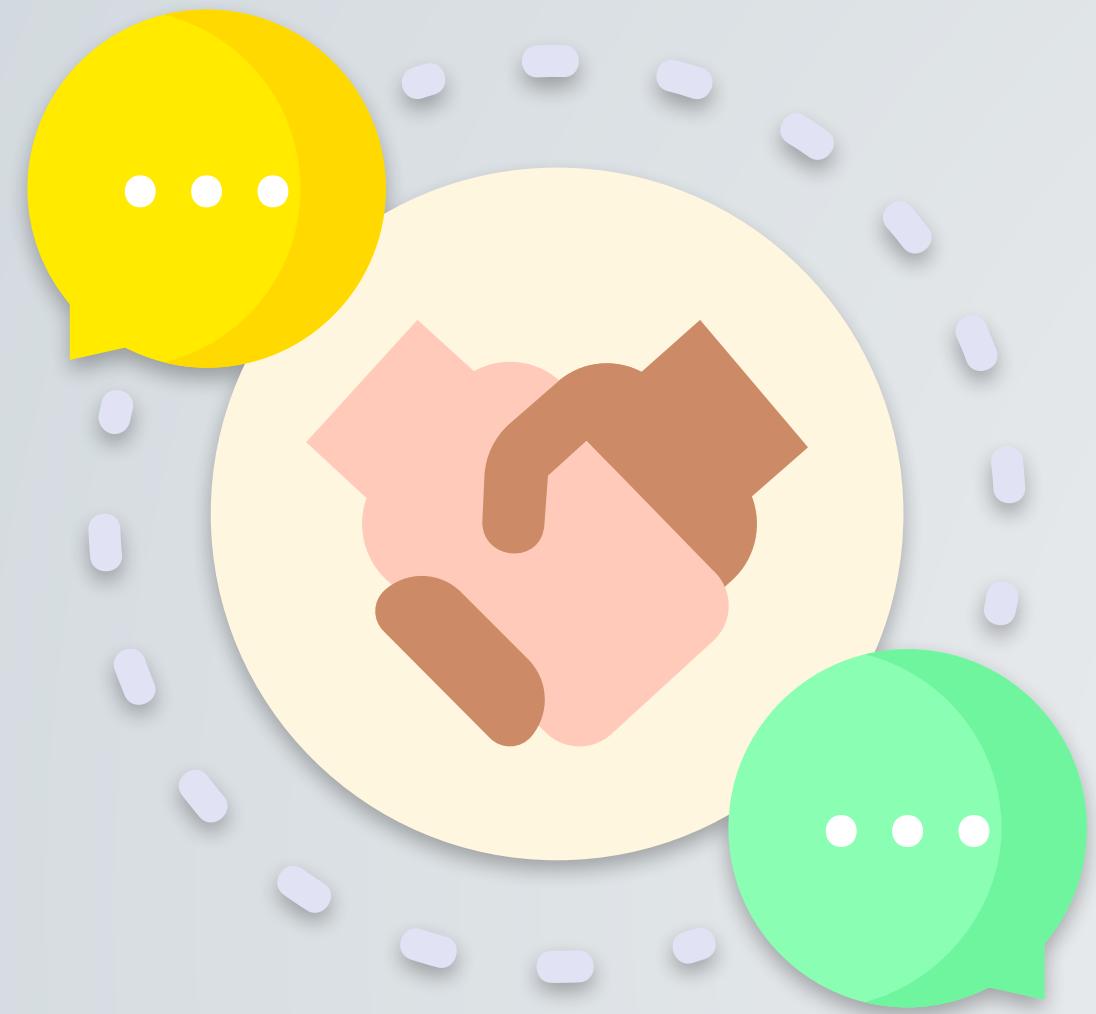
I dati non vengono  
alterati durante il  
transito in rete.



## Identificazione

Il certificato digitale  
permette di identificare  
l'altra parte coinvolta.

# SSL/TLS



## Fase 1

Negoziazione fra le parti  
degli algoritmi da utilizzare



## Fase 2

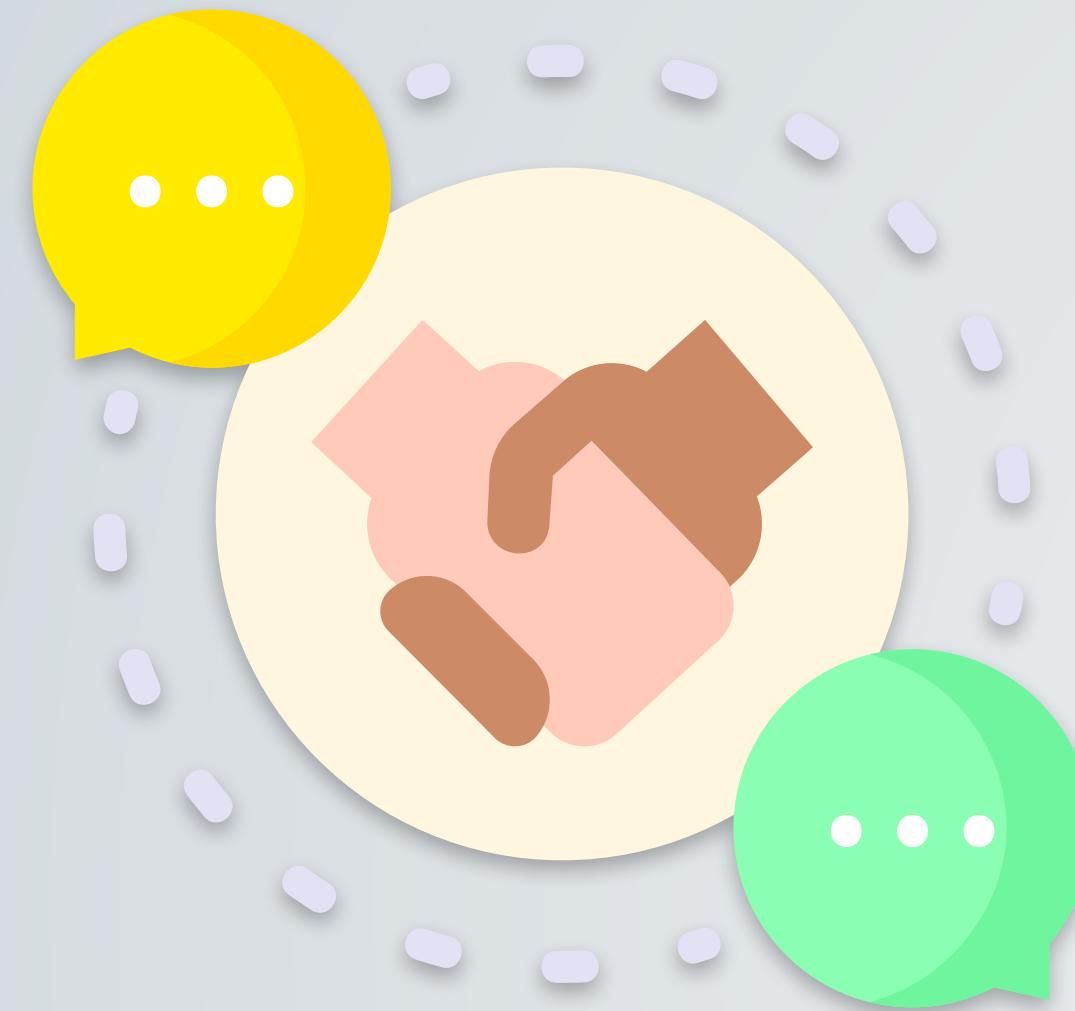
Scambio delle chiavi  
e autenticazione



## Fase 3

Cifratura simmetrica e  
autenticazione dei messaggi

# SSL/TLS



## Fase 1

Negoziazione fra le parti  
degli algoritmi da utilizzare



## Fase 2

Scambio delle chiavi  
e autenticazione



## Fase 3

Cifratura simmetrica e  
autenticazione dei messaggi

Diffie-Hellman

RSA

AES-256

HMAC-SHA



**https://**

HTTPS è la combinazione di HTTP e SSL/TLS che implementa una connessione sicura tra browser (client) e web server, fornendo:

Autenticazione del sito

Integrità dei dati

Protezione della privacy

Con l'utilizzo di HTTPS viene usata la porta 443 e viene invocato TLS che cifra:

- l'URL del documento richiesto;
- il contenuto del documento;
- il contenuto dei form riempiti dall'utente;
- i cookie scambiati tra browser e web server;
- il contenuto dell'header HTTP.

# Puoi trovare TLS in...



Web

HTTPS



VPN



e-mail

S/MIME



instant message

# Esercizio: S/MIME

<https://extrassl.actalis.it/portal/uapub/freemail>

The screenshot shows a web page for obtaining a free email certificate. At the top, there are logos for ACTALIS and ARUBA GROUP. Below them, a header bar contains the text "Free Email Certificate". The main content area features a small icon of an envelope with a checkmark and the text "Free Email Certificate". A section titled "Step 1 - Controllo di validità della Email" contains fields for "Email" (with an input field and a "INVIA EMAIL DI VERIFICA" button), "Codice di verifica" (with an input field), and "Captcha" (with an input field containing the text "d246m" and a "Rigenerare" link). The background of the page has a subtle grid pattern.