

# Firme digitali

Corso di Sicurezza  
a.a. 2019-20

**Alfredo De Santis**

Dipartimento di Informatica  
Università di Salerno

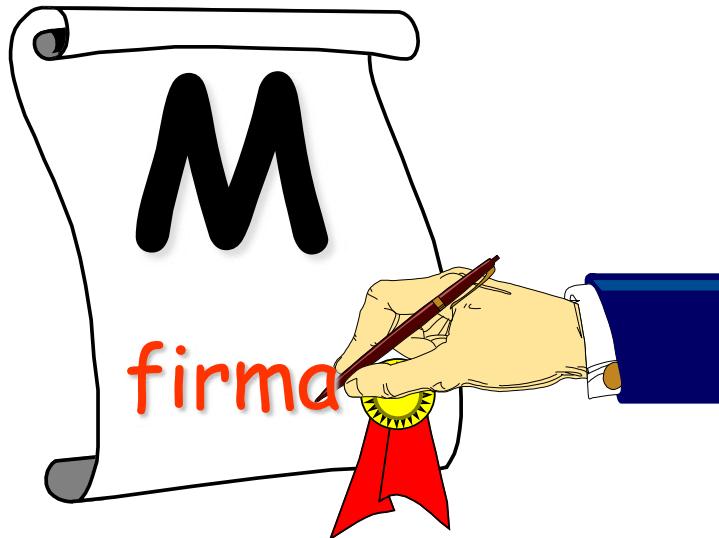
**ads@unisa.it**

**<http://www.di-srv.unisa.it/~ads>**



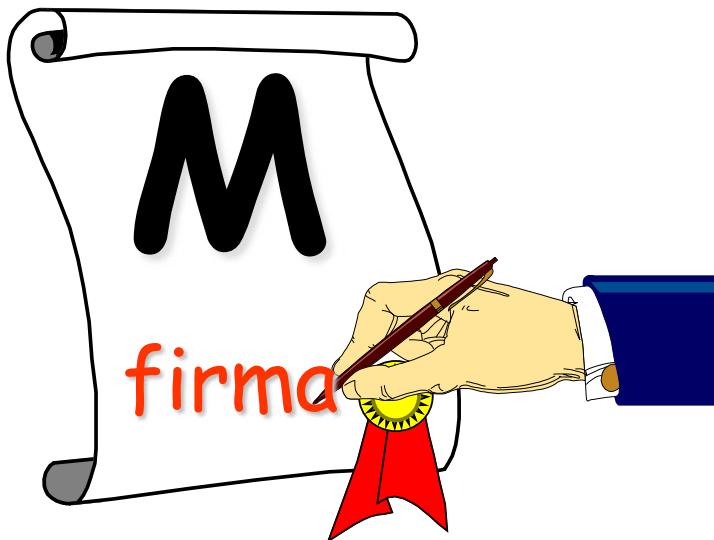
**Marzo 2020**

# Firma Digitale



Equivalente alla firma  
convenzionale

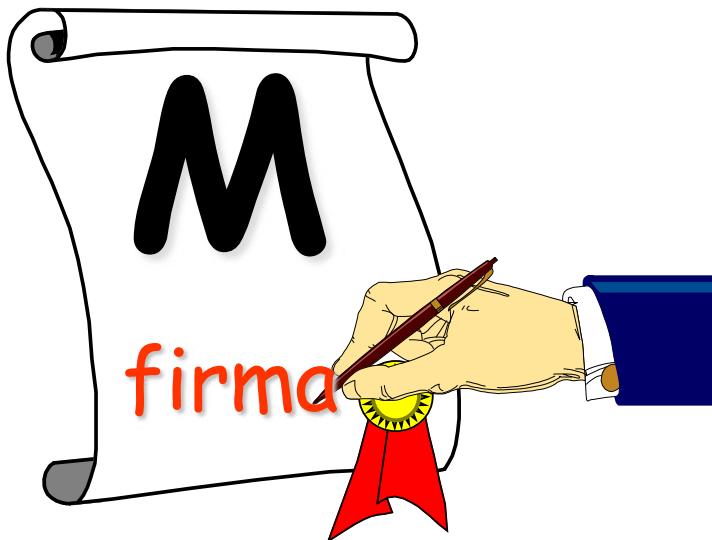
# Firma Digitale



Equivalent alla firma  
convenzionale

Soluzione naive:  
incollare firma digitalizzata

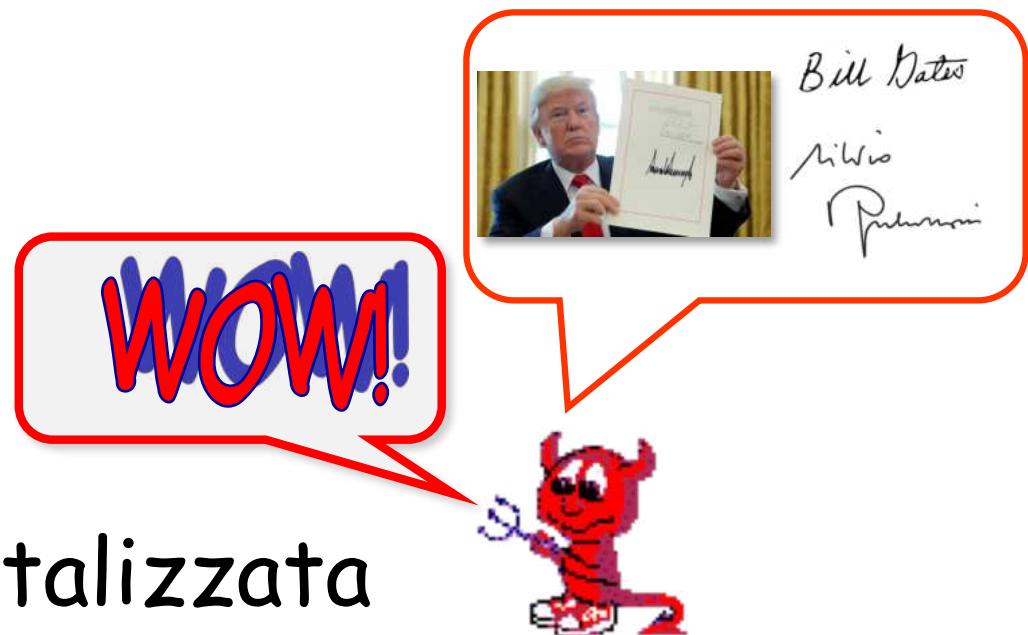
# Firma Digitale



Equivalent alla firma  
convenzionale

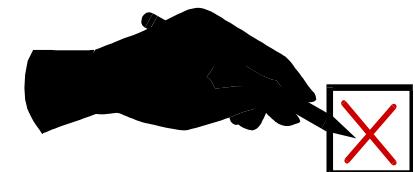
Soluzione naive:

incollare firma digitalizzata



# Requisiti per la Firma Digitale

La firma digitale deve poter essere facilmente prodotta dal legittimo firmatario

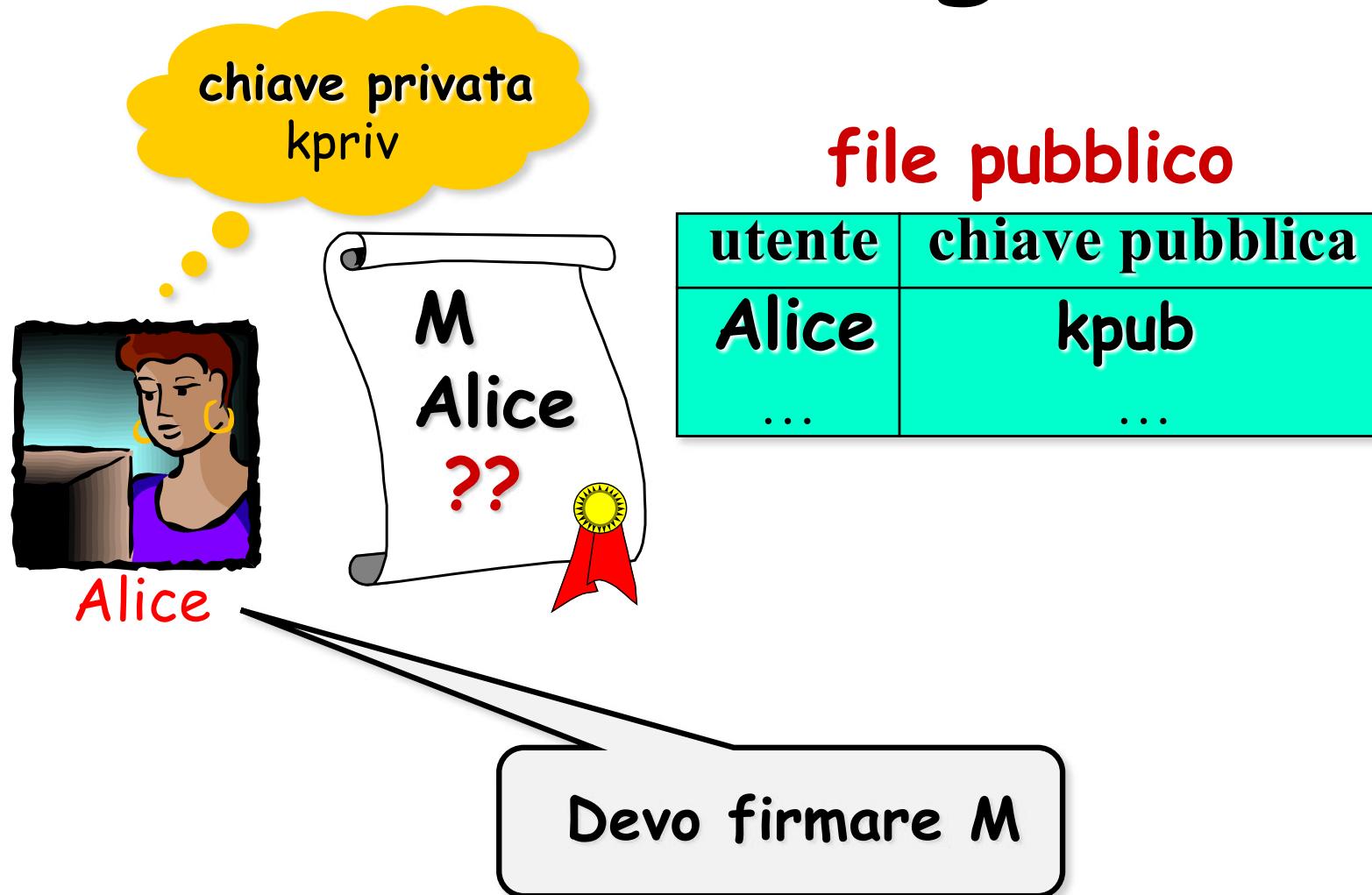


Nessun utente deve poter riprodurre la firma di altri

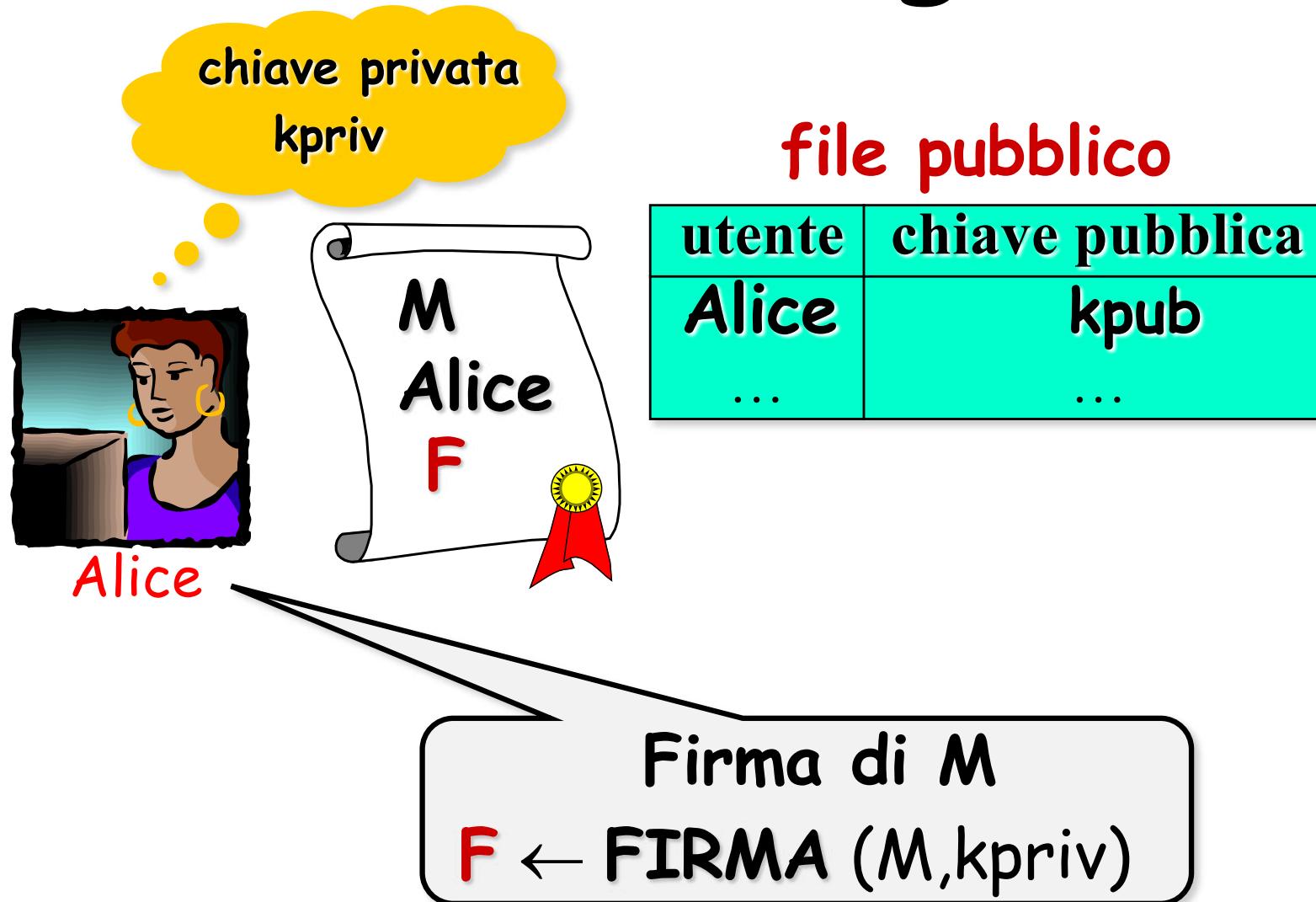
Chiunque può facilmente verificare una firma



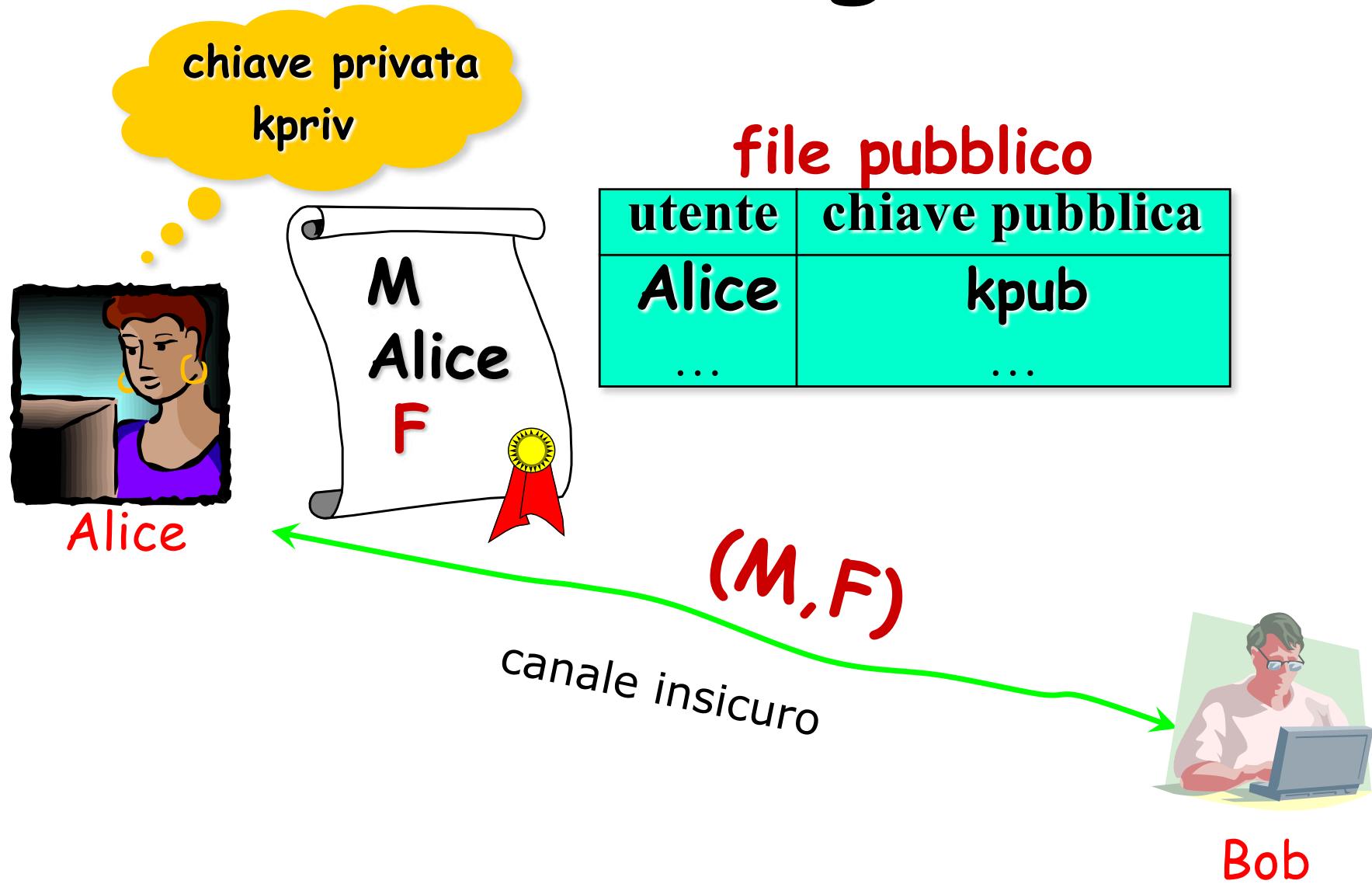
# Firma digitale



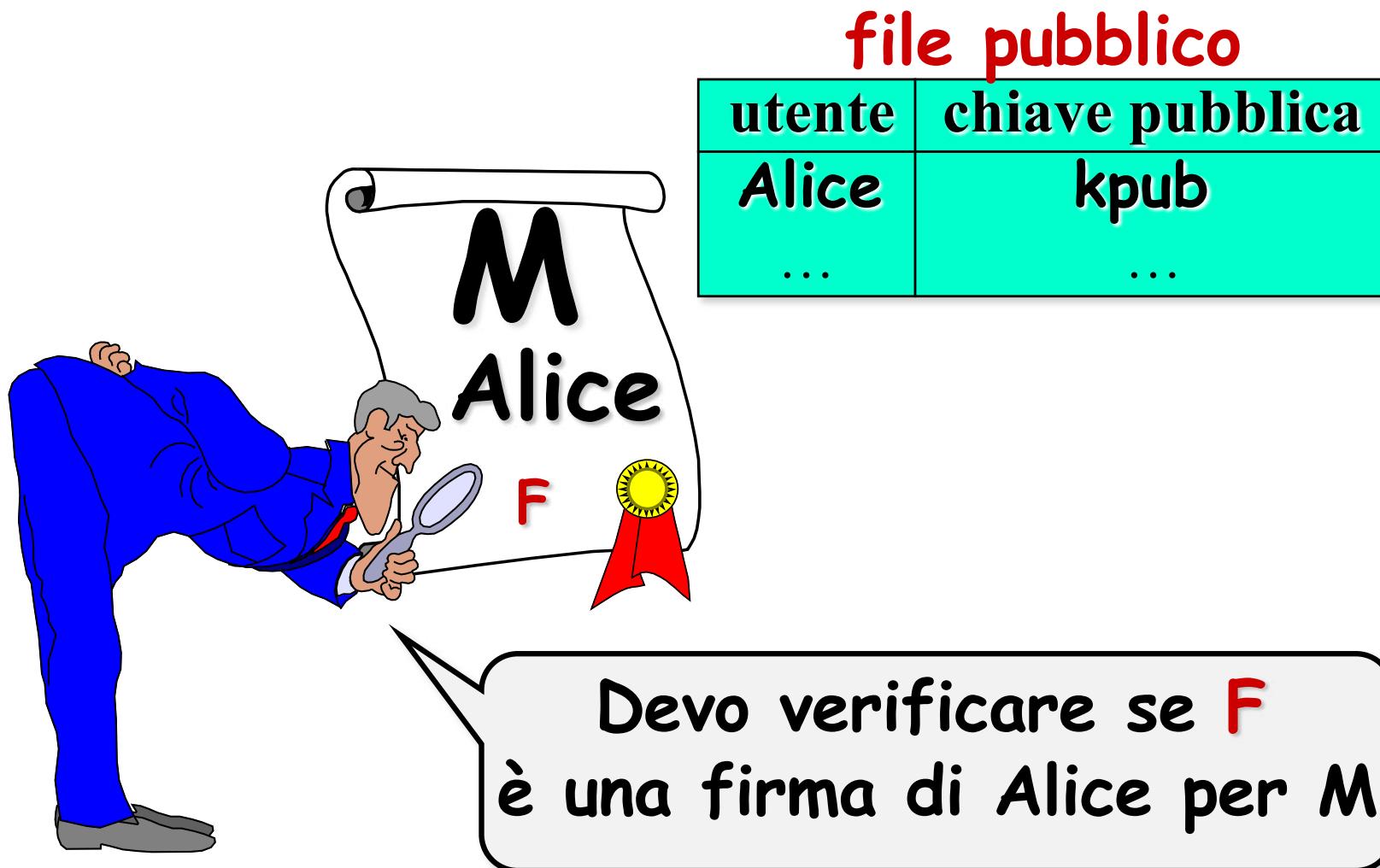
# Firma digitale



# Firma digitale



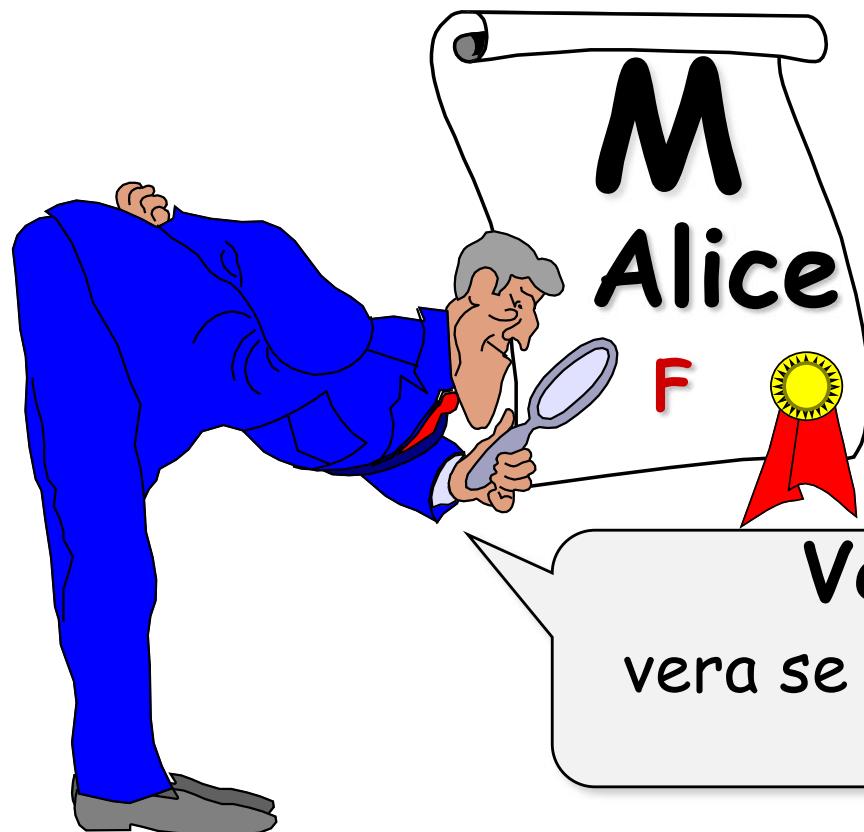
# Verifica firma digitale



# Verifica firma digitale

file pubblico

utente	chiave pubblica
Alice	kpub
...	...



Verifica firma di M  
vera se VERIFICA ( $F, M, k_{\text{pub}}$ ) = SI  
falsa altrimenti

# Sicurezza

- Cosa si intende per **sicurezza** di uno schema di firme digitali?
  
- Dobbiamo definire
  - Tipo di attacco
  - Scopo dell'attacco



# Tipo di attacco

## ➤ Key-only Attack

- Oscar conosce solo kpub di Alice



## ➤ Known Message Attack

- Oscar conosce una lista di messaggi e le relative firme di Alice

## ➤ Chosen Message Attack

- Oscar sceglie dei messaggi e chiede ad Alice di firmarli

# Scopo dell'attacco

## ➤ Total break

- Determinare  $k_{priv}$  di Alice per poter firmare qualsiasi messaggio



## ➤ Selective forgery

- Dato un messaggio  $M$ , determinare la firma  $F$  tale che  $VERIFICA(F, M, k_{pub}) = SI$

## ➤ Existential forgery

- Determinare una coppia  $(M, F)$  tale che  $VERIFICA(F, M, k_{pub}) = SI$

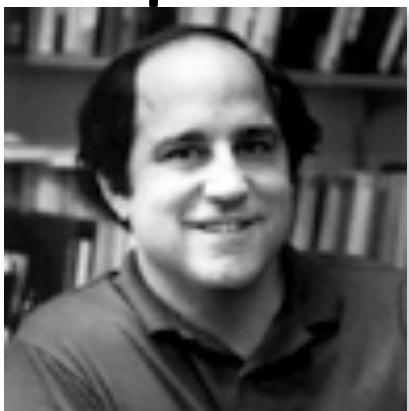
# Firme digitali che vedremo

- RSA
- ElGamal
- Digital Signature Standard (DSS)



# RSA

Proposto nel 1978 da



Rivest

Shamir

Adleman

Sicurezza basata sulla difficoltà di fattorizzare

# Chiavi RSA

chiave privata  
(n,d)

...

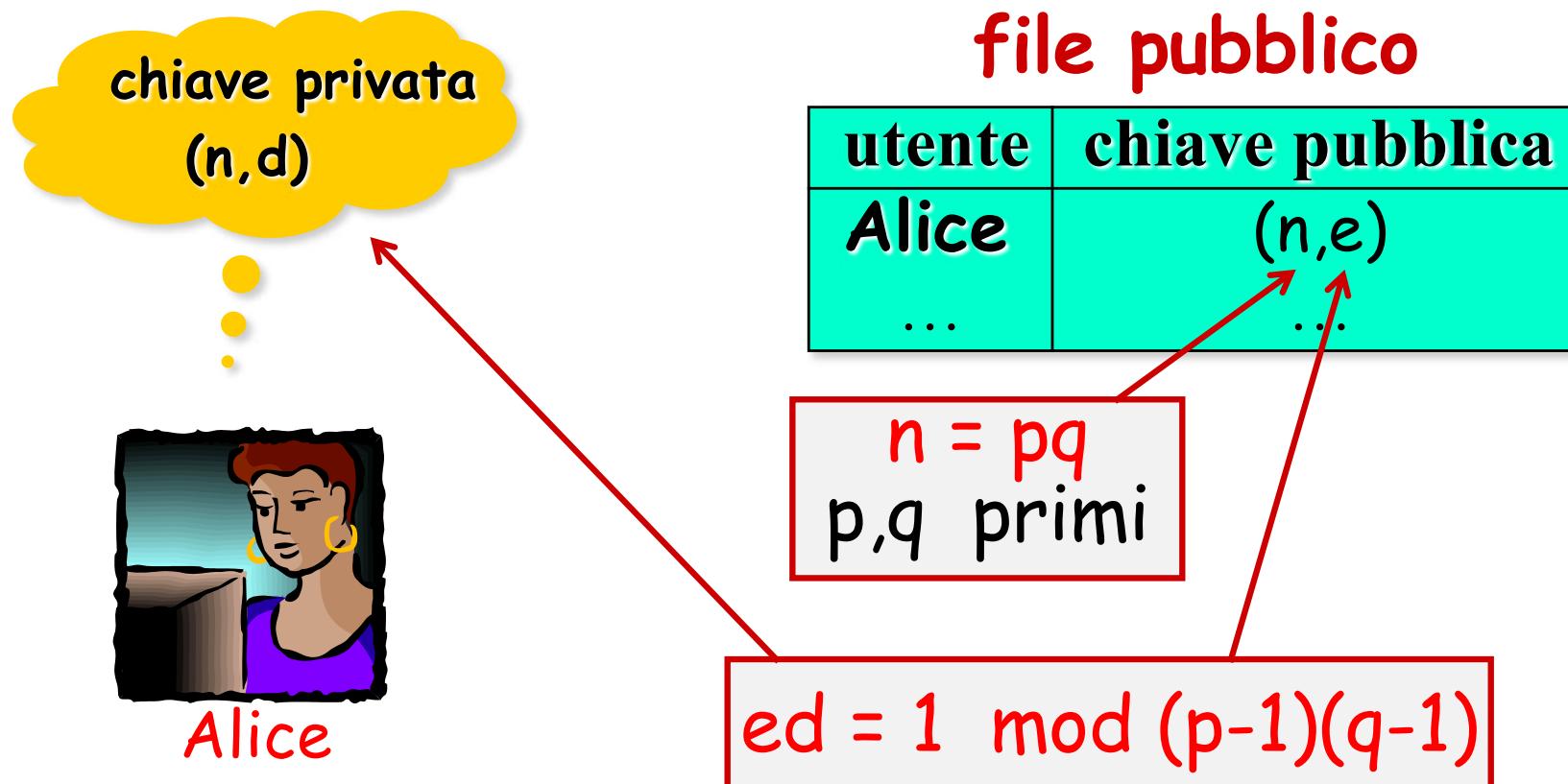


Alice

file pubblico

utente	chiave pubblica
Alice	(n,e)
...	...

# Chiavi RSA



# Firma RSA

chiave privata  
 $(n, d)$

⋮



Alice

file pubblico

utente	chiave pubblica
Alice	$(n, e)$
...	...

Devo firmare M



# Firma RSA

chiave privata  
(n,d)

⋮

file pubblico	
utente	chiave pubblica
Alice	(n,e)
⋮	⋮

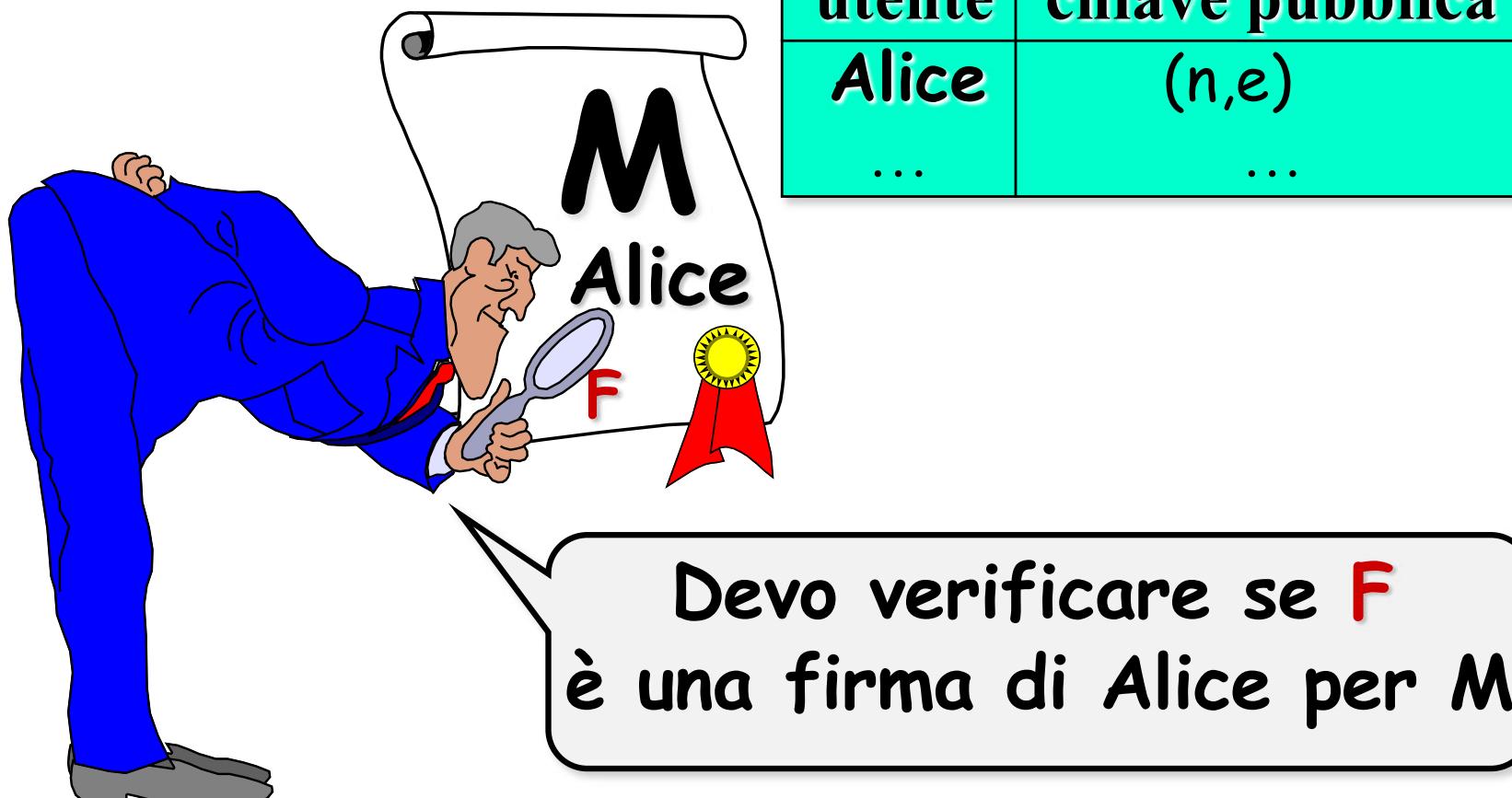


Alice

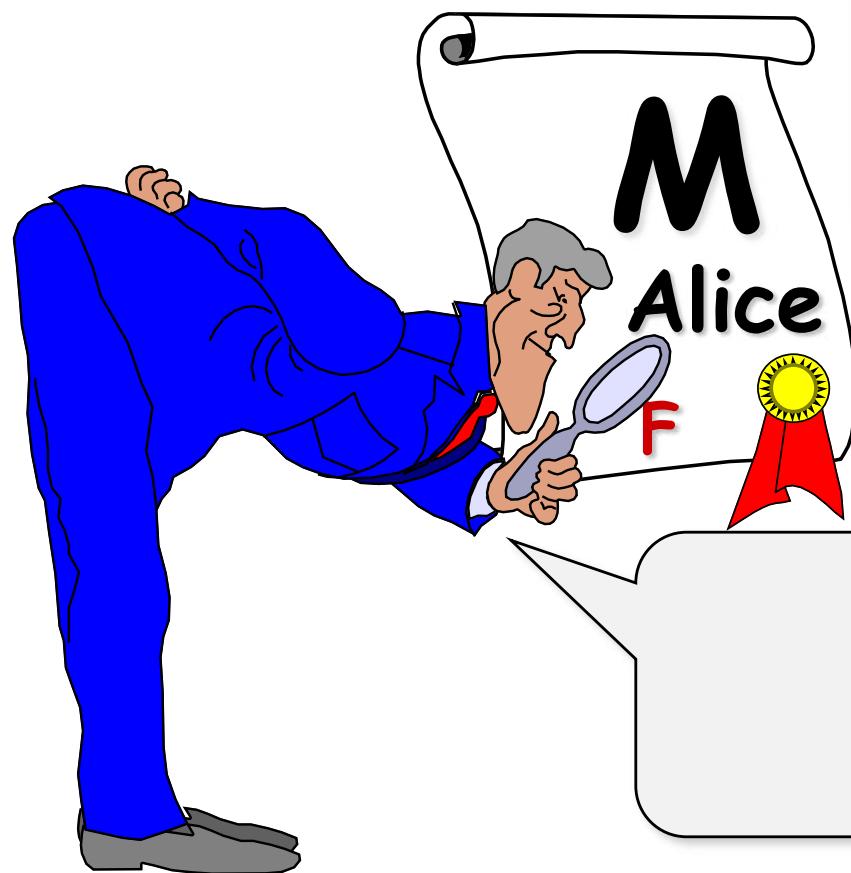
Firma di M

$$F \leftarrow M^d \text{ mod } n$$


# Verifica Firma RSA



# Verifica Firma RSA



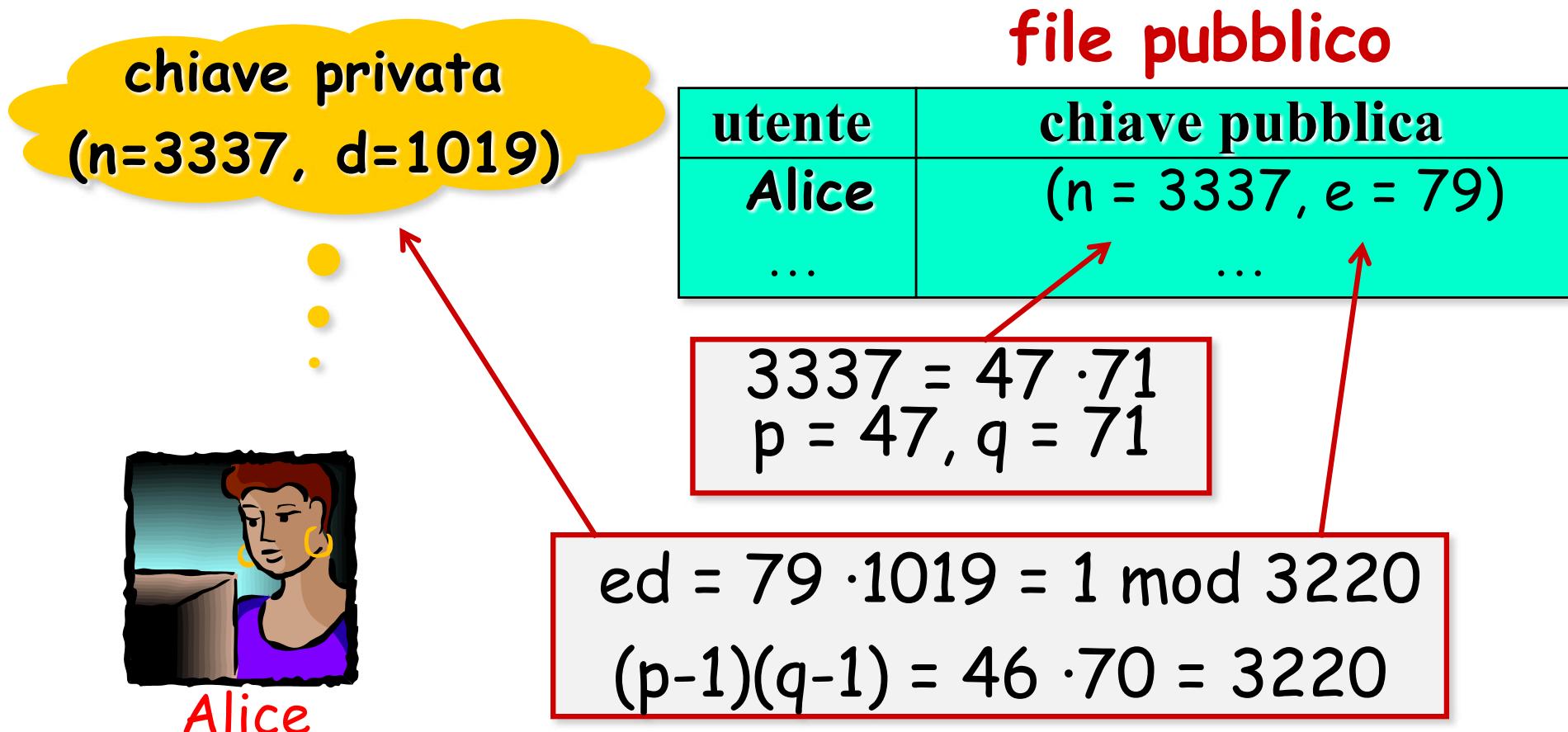
file pubblico

utente	chiave pubblica
Alice	(n,e)
...	...

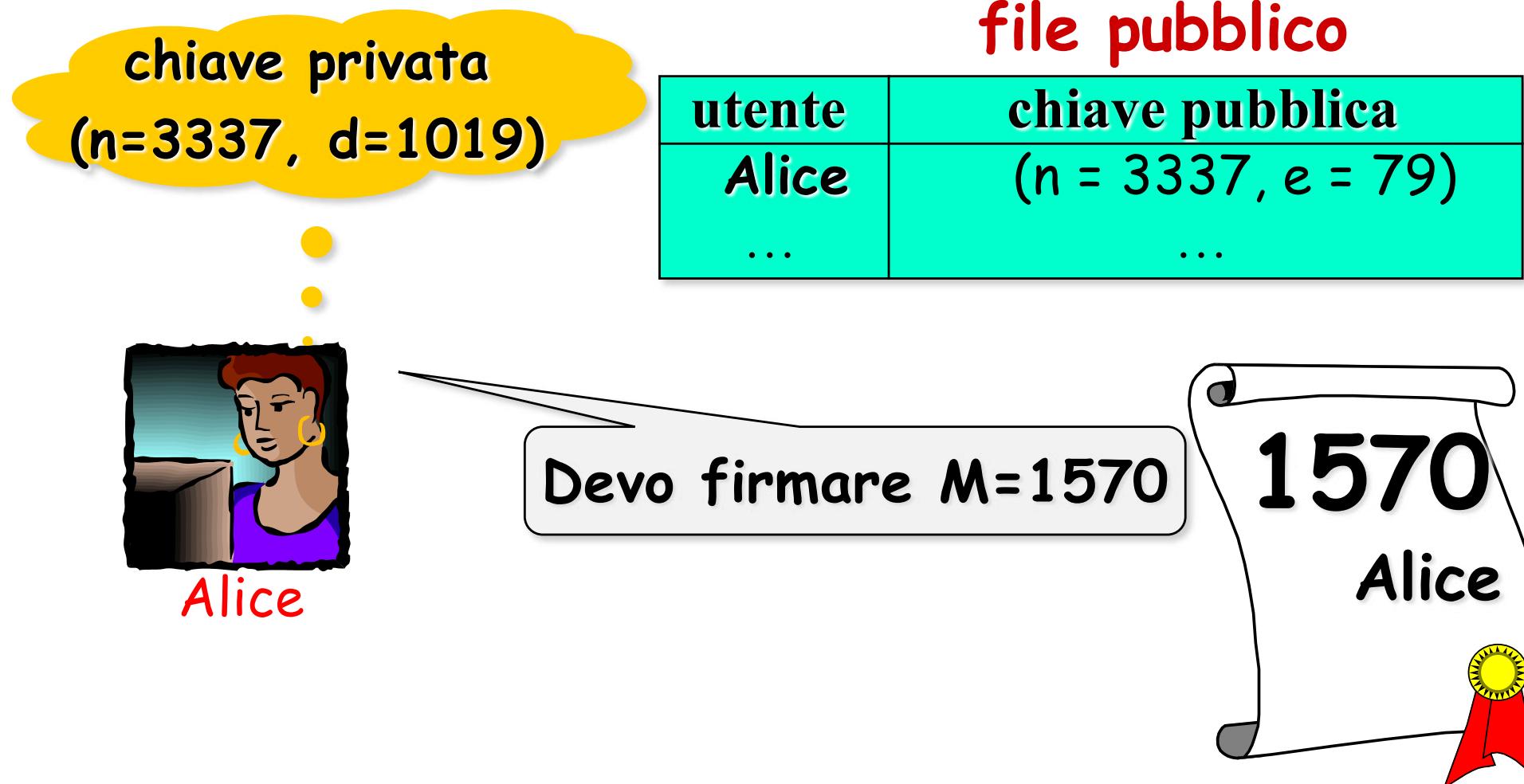
Verifica firma di M

vera se  $M = F^e \text{ mod } n$   
falsa altrimenti

# “Piccolo” esempio: Chiavi RSA



# “Piccolo” esempio: Chiavi RSA



# “Piccolo” esempio: generazione firma RSA

chiave privata  
( $n=3337$ ,  $d=1019$ )

file pubblico

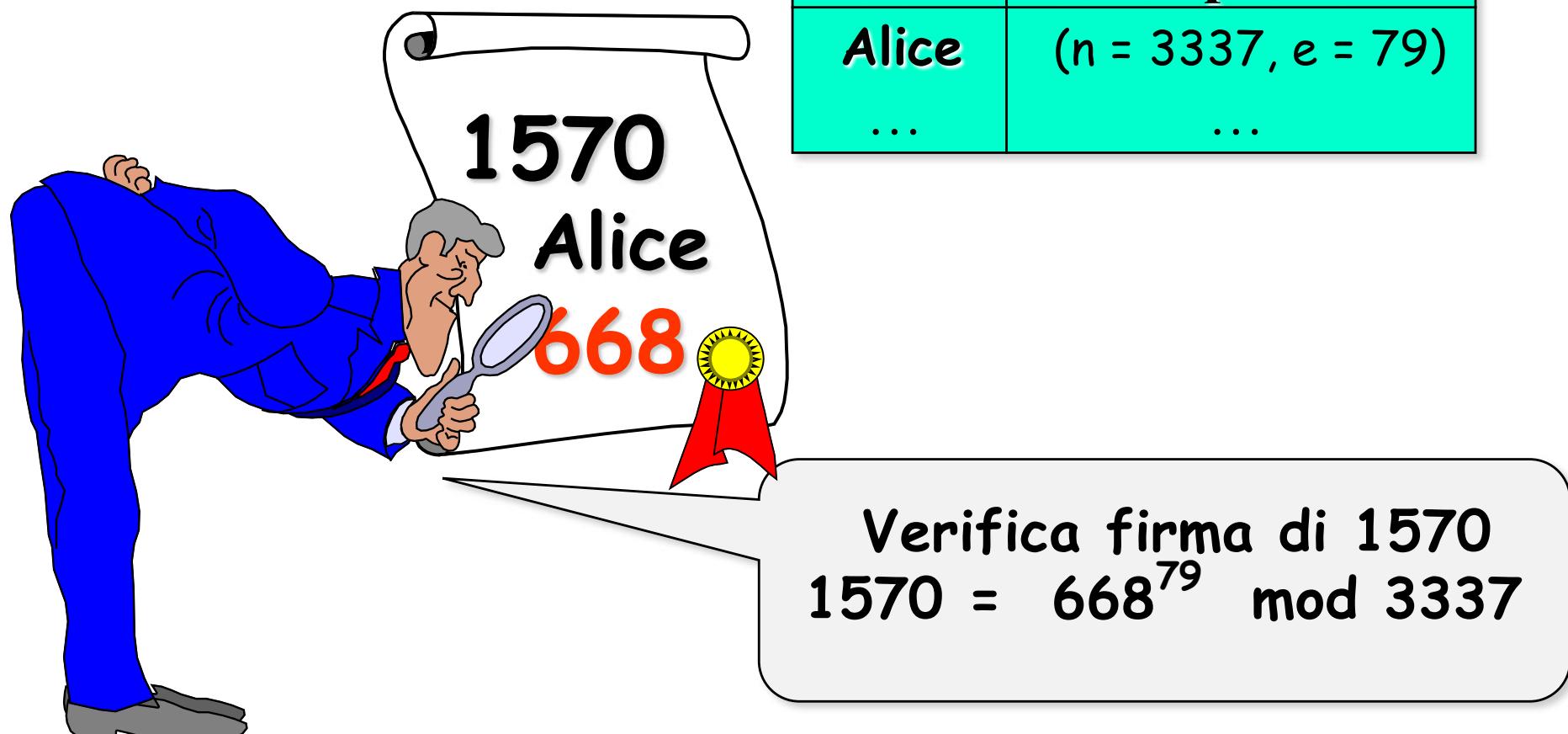
utente	chiave pubblica
Alice	( $n = 3337$ , $e = 79$ )
...	...



Firma di 1570  
 $= 1570^{1019} \text{ mod } 3337$   
 $= 668$



# “Piccolo” esempio: Verifica firma RSA



# Correttezza verifica firma RSA

$$F^e \bmod n = (M^d)^e \bmod n$$

$$= M^{ed} \bmod n$$

$ed \equiv 1 \pmod{(p-1)(q-1)}$

$$= M^{1+k(p-1)(q-1)} \bmod n$$

$$= M \cdot (M^{(p-1)(q-1)})^k$$

$$= M \bmod n$$

$$= M$$

Teorema di Eulero  
 $M \in \mathbb{Z}_n^* \Rightarrow M^{(p-1)(q-1)} \equiv 1 \pmod{n}$

poichè  $0 \leq M < n$

# Correttezza verifica firma RSA

$$F^e \bmod n = (M^d)^e \bmod n$$

$$= M^{ed} \bmod n$$

ed = 1 mod (p-1)(q-1)

$$= M^{1+k(p-1)(q-1)} \bmod n$$

$$= M \cdot (M^{(p-1)(q-1)})^k$$

$$= M \bmod n$$

Teorema di Eulero  
 $M \in \mathbb{Z}_n^* \Rightarrow M^{(p-1)(q-1)} = 1 \bmod n$

$$= M$$

Per  $M \in \mathbb{Z}_n / \mathbb{Z}_n^*$  usa  
il **teorema cinese del resto**

poichè  $0 \leq M < n$

# Sicurezza firma RSA

Voglio falsificare la firma  
di M da parte di Alice

file pubblico

utente	chiave pubblica
Alice	(n,e)
...	...



Selective forgery  
Key only attack



# Sicurezza firma RSA

Voglio falsificare la firma  
di  $M$  da parte di Alice

file pubblico

utente	chiave pubblica
Alice	(n,e)
...	...



Devo calcolare  
 $M^d \text{ mod } n$

Selective forgery  
Key only attack



# Sicurezza firma RSA

Voglio falsificare la firma  
di  $M$  da parte di Alice

file pubblico

utente	chiave pubblica
Alice	$(n, e)$
...	...



Devo calcolare  
 $M^d \text{ mod } n$

Equivalent to "breaking"  
the RSA cryptosystem

Selective forgery  
Key only attack



# Sicurezza firma RSA

Voglio falsificare una firma da parte di Alice

file pubblico

utente	chiave pubblica
Alice	(n,e)
...	...



Existential forgery  
Key only attack



# Sicurezza firma RSA

Voglio falsificare la firma  
di M da parte di Alice

file pubblico

utente	chiave pubblica
Alice	(n,e)
...	...



1. Scelgo F a caso
2.  $M \leftarrow F^e \text{ mod } n$

Existential forgery  
Key only attack



# Sicurezza firma RSA

## file pubblico

Voglio generare messaggi  
e firme da parte di Alice



utente	chiave pubblica
Alice	(n,e)
...	...

Existential forgery  
Known message attack

# Sicurezza firma RSA

## file pubblico



Voglio generare messaggi e firme da parte di Alice

Conosco le coppie  $(M_1, F_1)$  e  $(M_2, F_2)$

Proprietà di omomorfismo

$$F_1 = M_1^d \text{ mod } n \quad F_2 = M_2^d \text{ mod } n$$
$$(F_1 F_2)^e \text{ mod } n = F_1^e F_2^e \text{ mod } n = M_1 M_2 \text{ mod } n$$

$F_1 F_2 \text{ mod } n$  è una firma valida per  $M_1 M_2 \text{ mod } n$

Existential forgery  
Known message attack

utente	chiave pubblica
Alice	$(n, e)$
...	...

# Sicurezza firma RSA

Voglio falsificare la firma  
di M da parte di Alice



file pubblico

utente	chiave pubblica
Alice	(n,e)
...	...

Selective forgery  
Chosen message attack

# Sicurezza firma RSA

Voglio falsificare la firma  
di  $M$  da parte di Alice

file pubblico

utente	chiave pubblica
Alice	$(n,e)$
...	...



1. Scelgo  $M_1$  e  $M_2$  tali che  $M=M_1M_2 \text{ mod } n$
2. Chiedo ad Alice di firmare  $M_1$  e  $M_2$  ottenendo  $F_1$  e  $F_2$
3.  $F_1F_2 \text{ mod } n$  è una firma valida per  $M$

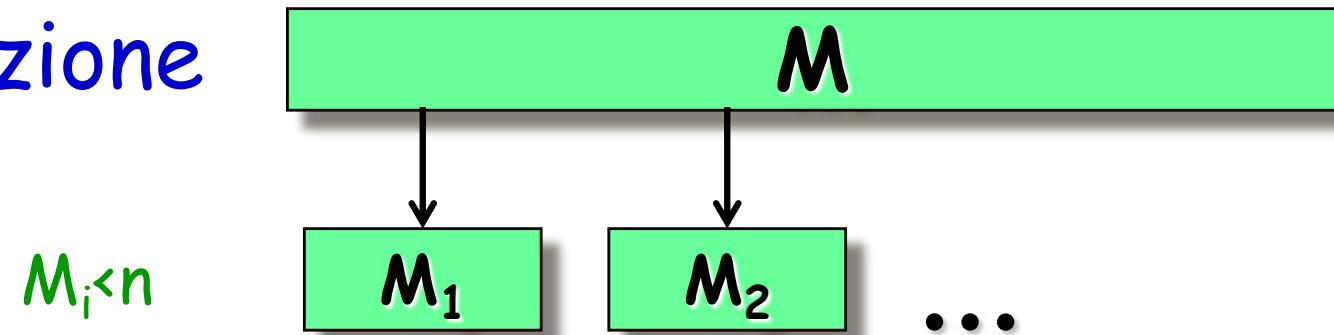
Selective forgery

Chosen message attack

# Firma digitale di messaggi grandi

Se  $M > n$ , come si firma?

Prima soluzione

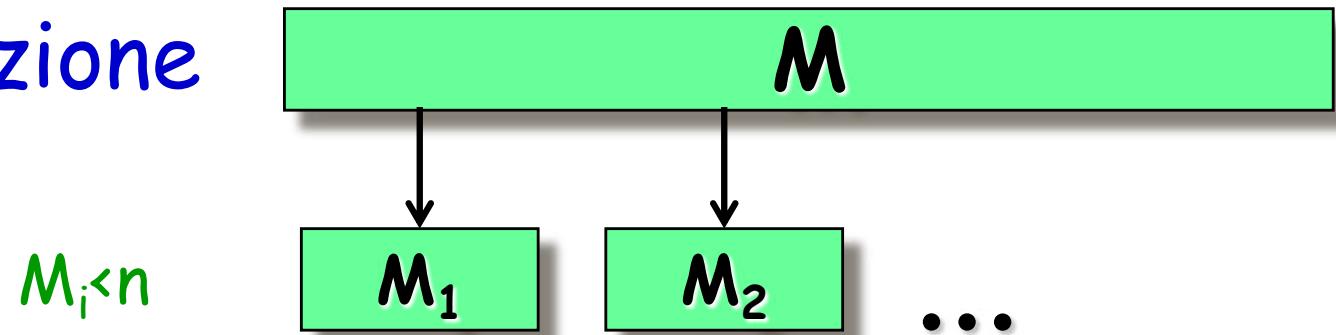


$\text{Firma}(M) \leftarrow (\text{Firma}(M_1), \text{Firma}(M_2), \dots)$

# Firma digitale di messaggi grandi

Se  $M > n$ , come si firma?

Prima soluzione

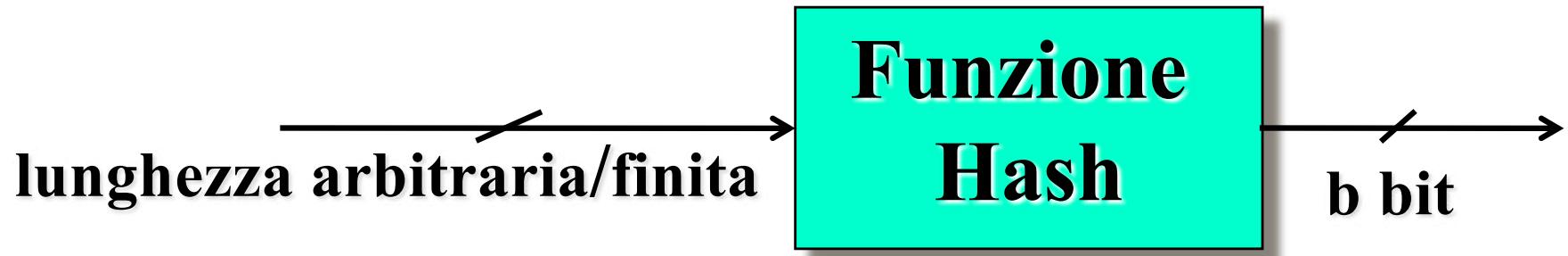


$\text{Firma}(M) \leftarrow (\text{Firma}(M_1), \text{Firma}(M_2), \dots)$

Problemi { Efficienza  
Permutazione/composizione delle firme → nuova firma



# Funzioni Hash



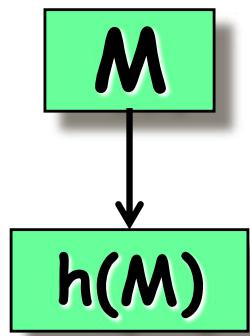
Il valore hash  $h(M)$  è una rappresentazione non ambigua e non falsificabile del messaggio  $M$

Proprietà:

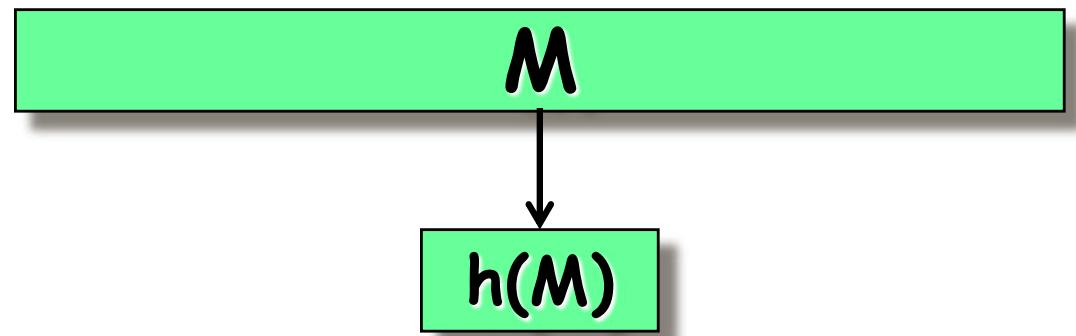
- comprime
- facile da computare
- **Sicurezza forte**: computazionalmente difficile trovare 2 diversi messaggi con lo stesso valore hash
- **One-way**: dato  $y$  è computazionalmente difficile trovare  $M$  tale che  $y = h(M)$

# Firma digitale con hash

messaggi piccoli



messaggi grandi



$\text{Firma}(M) \leftarrow \text{Firma}(h(M))$

Vantaggi {  
Efficienza  
Integrità  
Sicurezza}



# Firma RSA con hash



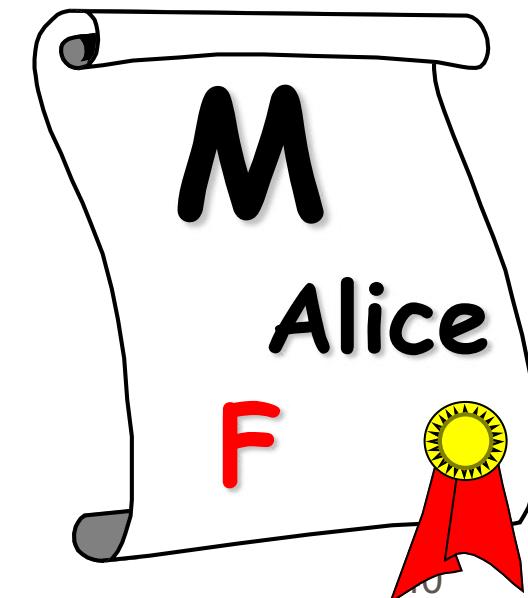
Alice

file pubblico

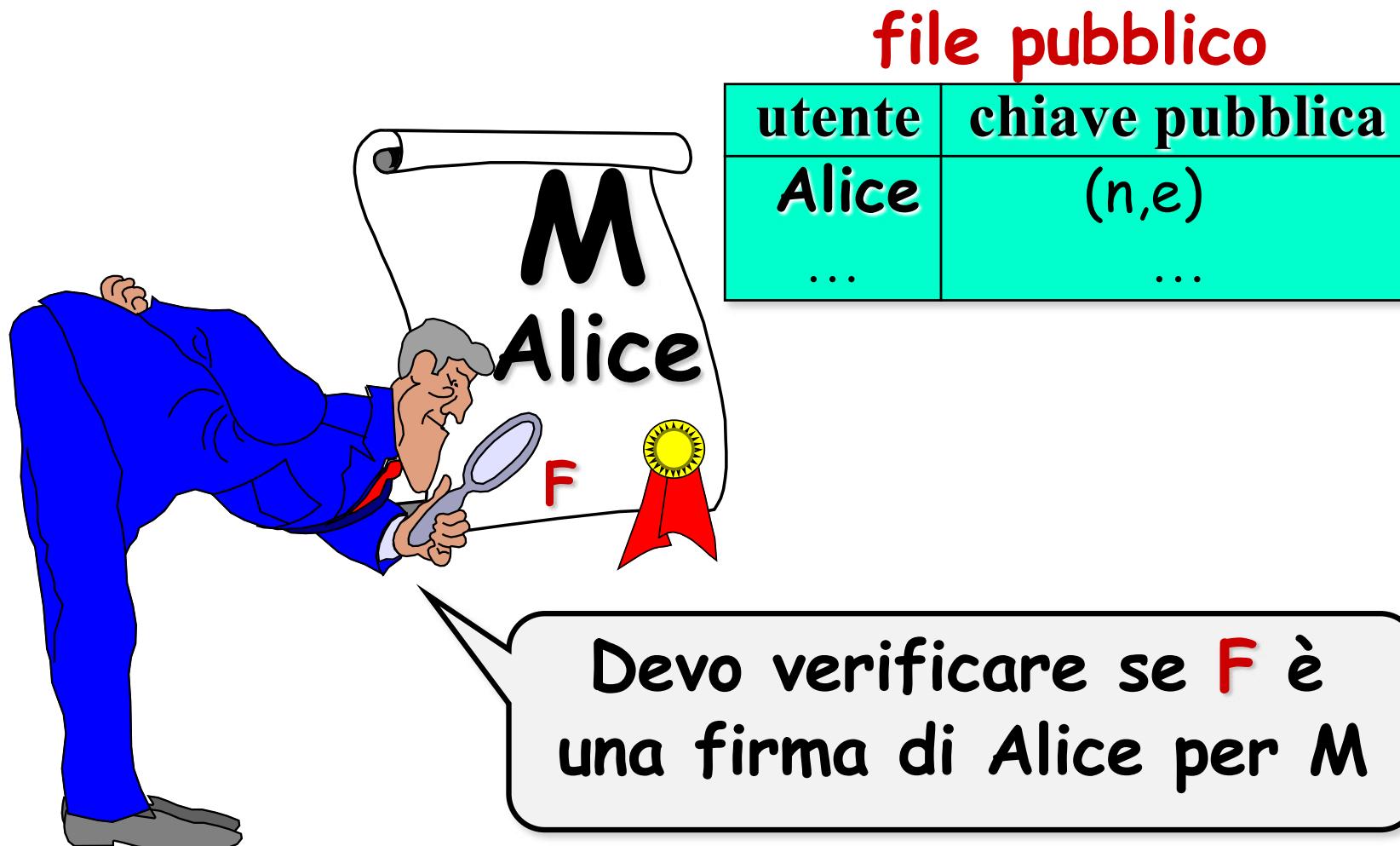
utente	chiave pubblica
Alice	(n,e)
...	...

Firma di M

$$F \leftarrow [h(M)]^d \text{ mod } n$$



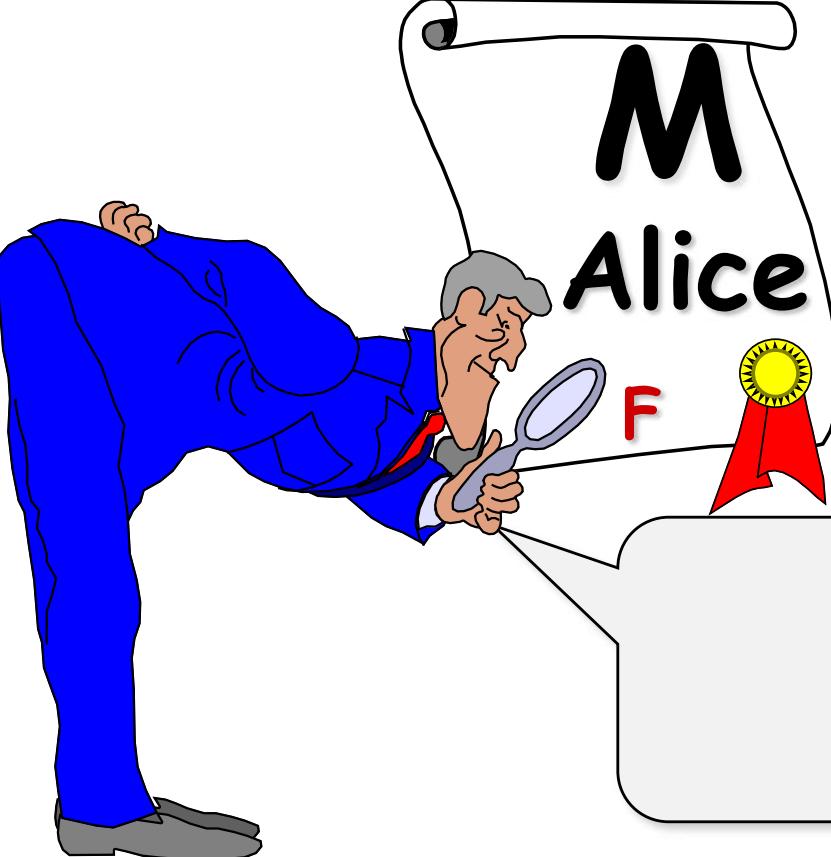
# Verifica Firma RSA con hash



# Verifica Firma RSA

file pubblico

utente	chiave pubblica
Alice ...	(n,e) ...



Verifica firma di M  
vera se  $h(M) = F^e \text{ mod } n$   
falsa altrimenti

# Sicurezza firma RSA con hash

Voglio generare messaggi  
e firme da parte di A



file pubblico

utente	chiave pubblica
Alice	(n,e)
...	...

Existential forgery  
Key only attack



# Sicurezza firma RSA con hash

Voglio generare messaggi  
e firme da parte di A

file pubblico

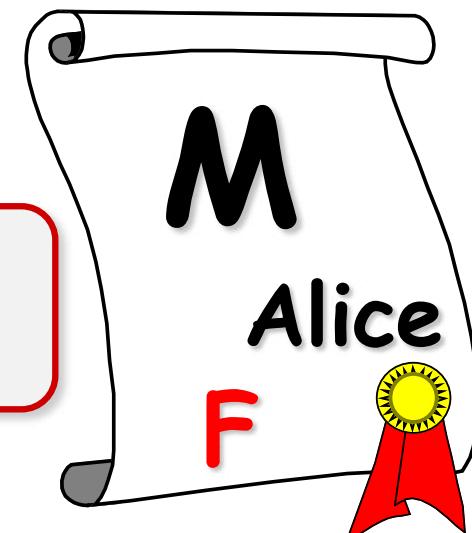
utente	chiave pubblica
Alice	(n,e)
...	...



1. Scelgo F a caso
2.  $z \leftarrow F^e \text{ mod } n$
3.  $M \leftarrow h^{-1}(z)$

Come faccio ad invertire h?  
 $M \leftarrow h^{-1}(z)$

Existential forgery  
Key only attack

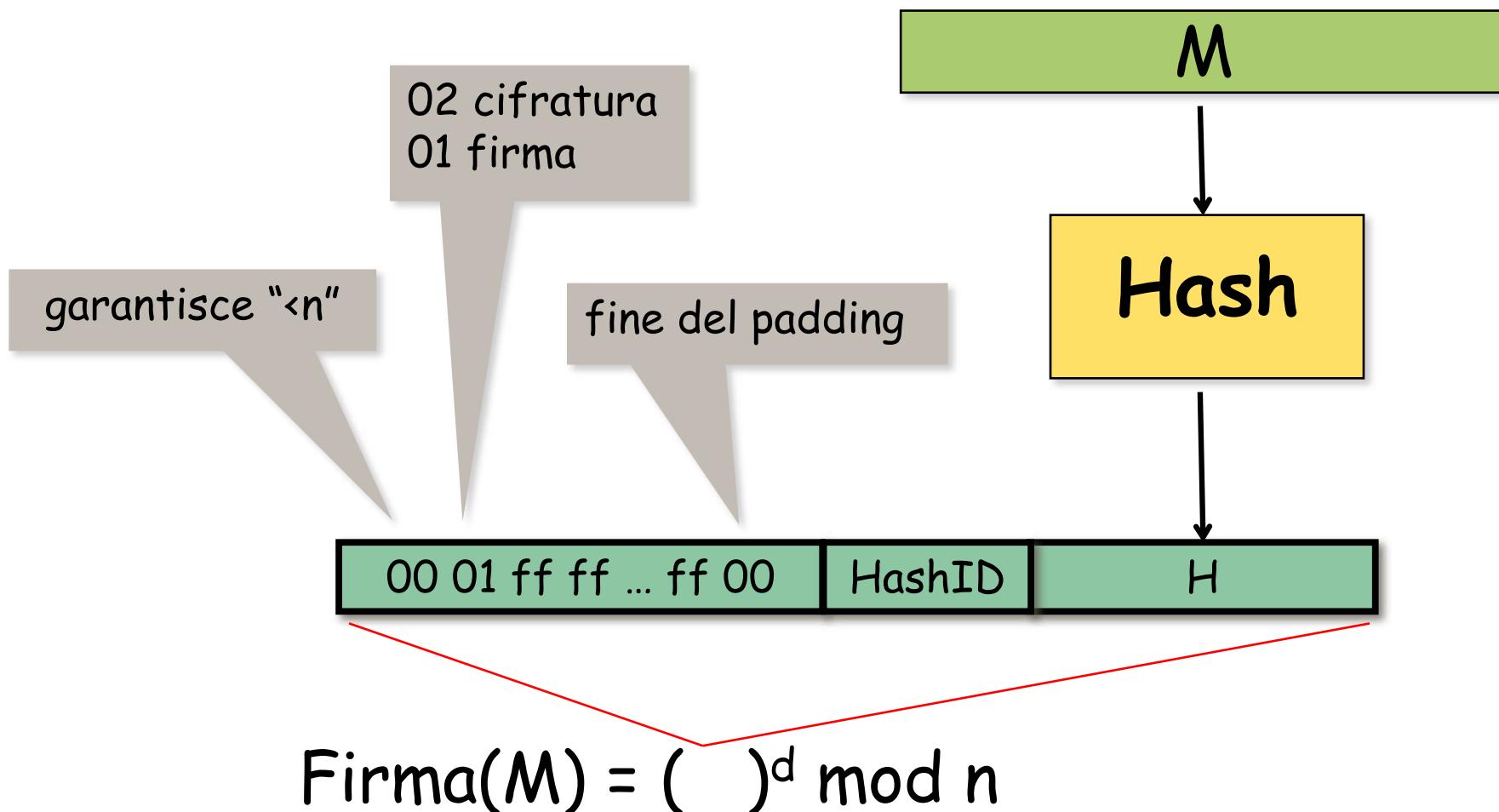


# PKCS #1

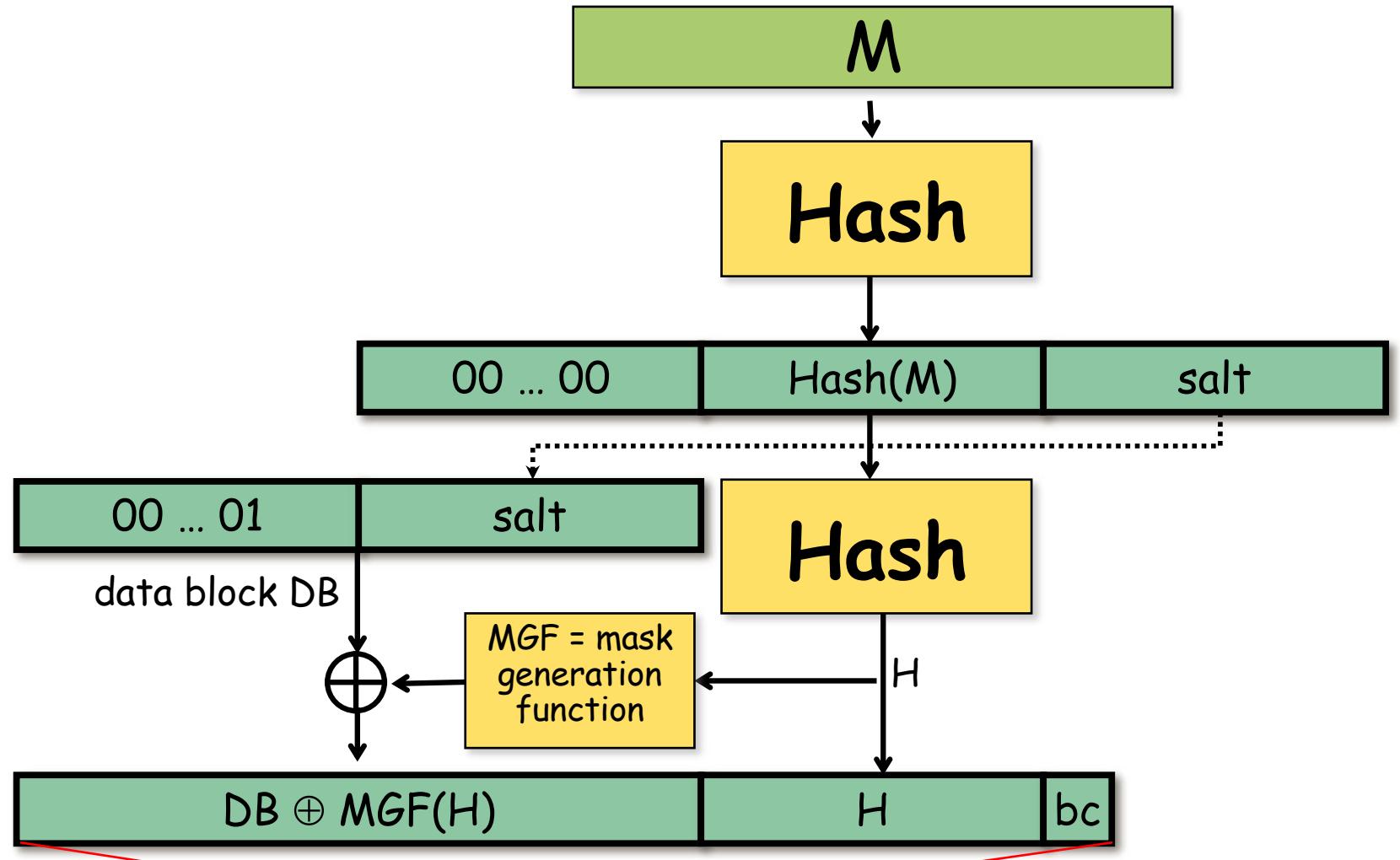
- Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications, Version 2.1
- Ver. 1.4, giugno 1991, ..., Ver. 2.1, giugno 2002 (= RFC 3447 nel feb 2003)
- Due schemi per la firma
  - RSASSA-PKCS1-v1\_5
    - Non ci sono prove di sicurezza, ma neanche attacchi
  - RSASSA-PSS. Basato su Probabilistic Signature Scheme
    - Hash del messaggio con *salt* casuale
    - M. Bellare and P. Rogaway.  
The Exact Security of Digital Signatures - How to Sign with RSA and Rabin,  
Eurocrypt 1996

Signature Scheme with Appendix":  
si calcola subito un hash del  
messaggio e poi lo si firma

# RSASSA-PKCS1-v1\_5

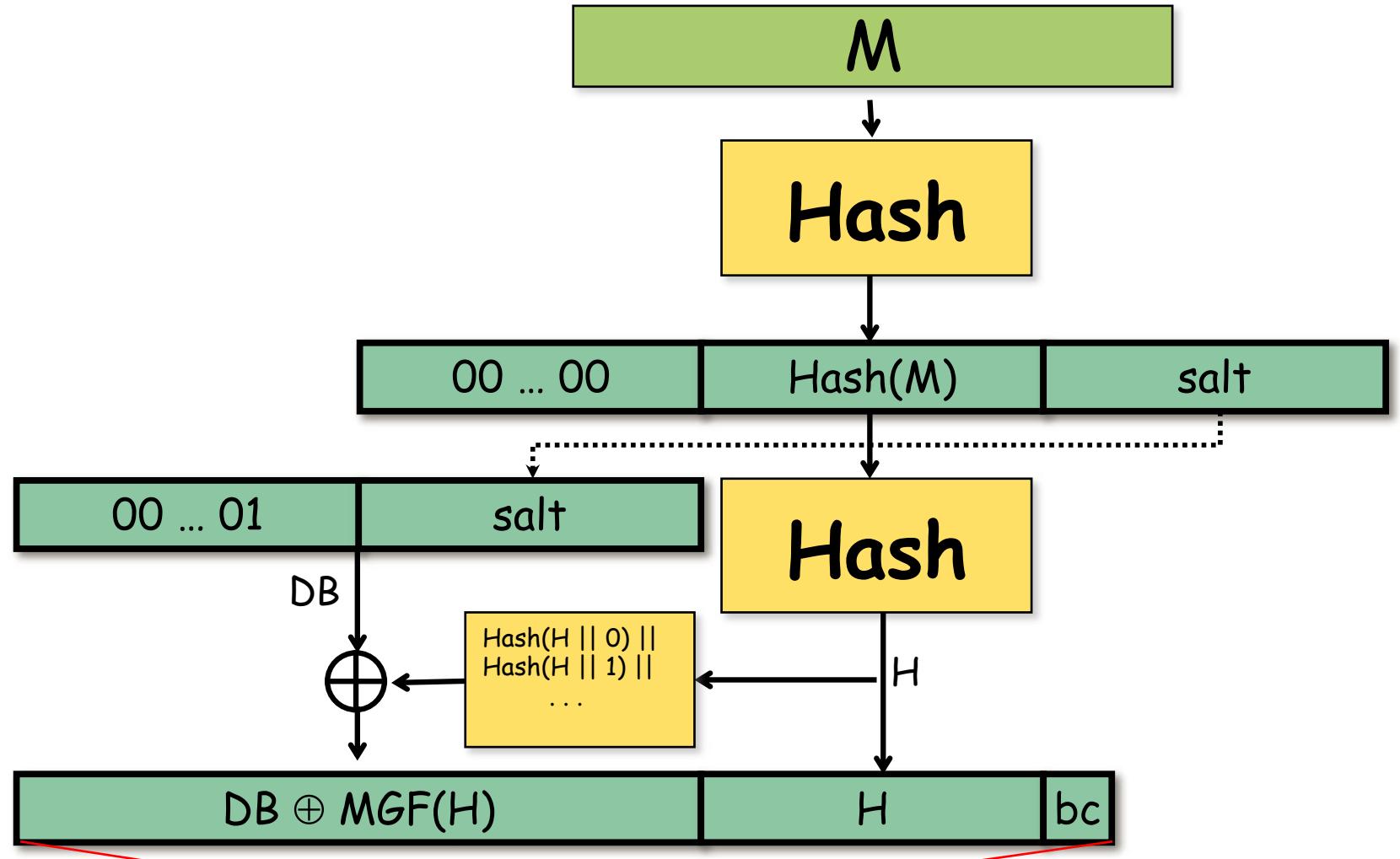


# RSASSA-PSS



$$\text{Firma}(M) = ( )^d \bmod n$$

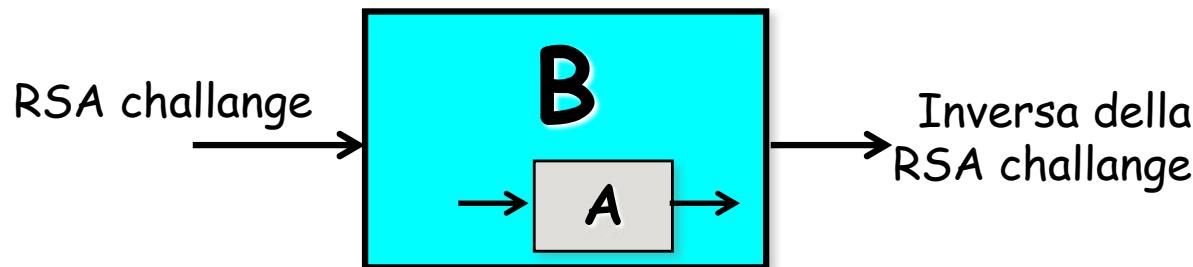
# RSASSA-PSS



$$\text{Firma}(M) = ( )^d \bmod n$$

# Provable security di PSS

- Supponiamo ci sia un algoritmo A che falsifica firme PSS senza usare dettagli di "Hash" e "MGF"
  - Chosen message attack, Existential forgery
  - Hash e MGF sono "random oracles" che possono essere interrogati
- Allora costruisco un algoritmo B che inverte RSA in quasi lo stesso tempo usando A come subroutine



- ⇒ Se RSA è difficile da invertire, allora PSS è sicura rispetto ad attacchi generici

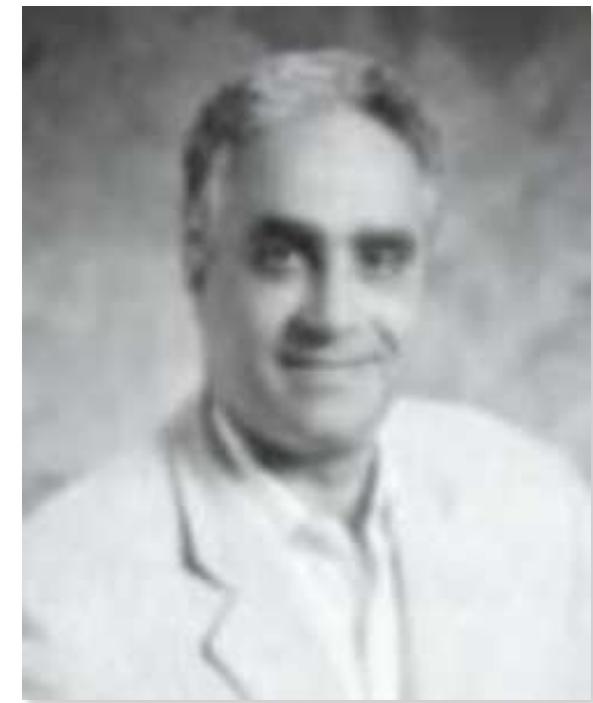
# Firme digitali che vedremo

- RSA
- ElGamal
- Digital Signature Standard (DSS)



# Firma digitale di ElGamal

- Taher Elgamal
- Sicurezza basata sull'intrattabilità del problema del **logaritmo discreto**



Taher El Gamal,  
A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms  
IEEE Transactions and Information Theory, vol. IT-31, No. 4, July 1985.

# Firme digitali di ElGamal

- Utilizza il concetto di **generatore** di  $Z_p^*$
- $p$  primo
- $g$  è generatore di  $Z_p^*$  se  $\{g^i \mid 1 \leq i \leq p-1\} = Z_p^*$

# Potenze in $\mathbb{Z}_{19}^*$

# Chiavi ElGamal

chiave privata  
 $(p,\alpha,s)$

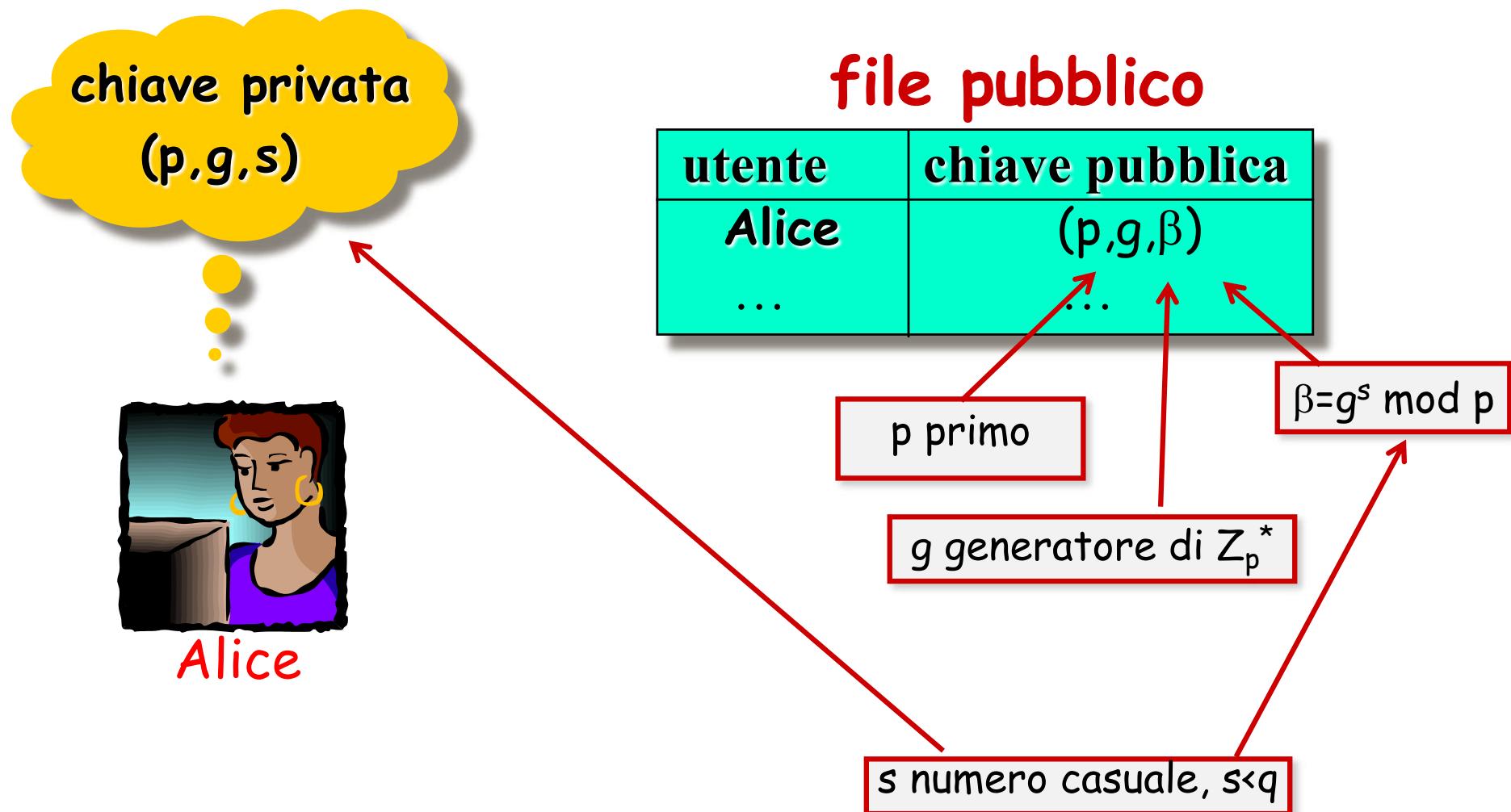


Alice

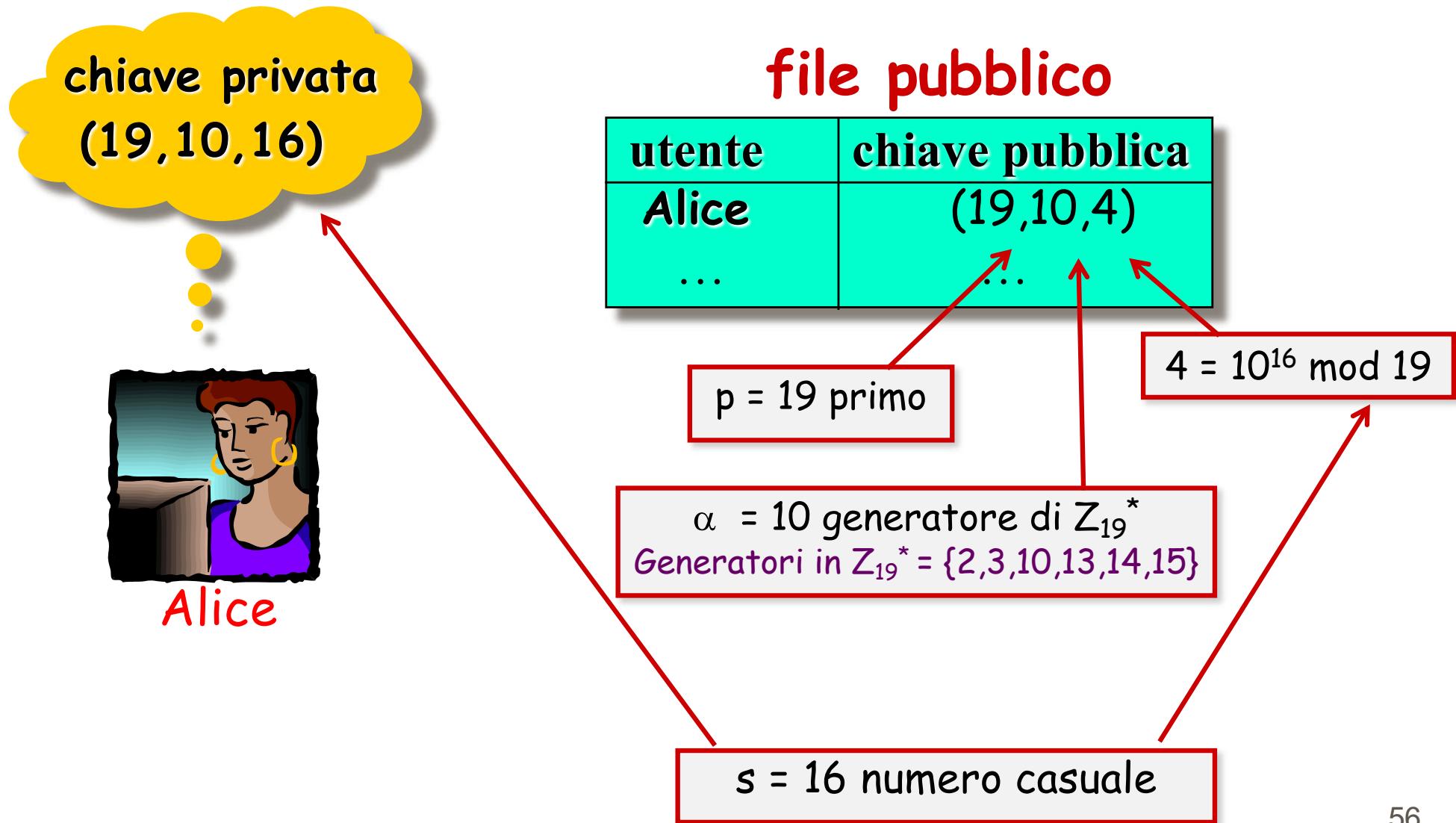
file pubblico

utente	chiave pubblica
Alice	$(p,\alpha,\beta)$
...	...

# Chiavi ElGamal



# Chiavi ElGamal ("piccolo" esempio)



# Firma ElGamal

chiave privata  
( $p, g, s$ )



Alice

file pubblico

utente	chiave pubblica
Alice	( $p, g, \beta = g^s$ )
...	...

Devo firmare M



# Firma ElGamal

chiave privata  
( $p, g, s$ )



Alice

file pubblico

utente	chiave pubblica
Alice	( $p, g, \beta = g^s$ )
...	...

Firma di  $M$

$r \leftarrow$  a caso in  $\mathbb{Z}_p^*$  con  $\gcd(r, p-1) = 1$

$\gamma \leftarrow g^r \bmod p$

$\delta \leftarrow (M - s\gamma)r^{-1} \bmod p-1$

$\text{firma}_{(p,g,s)}(M, r) = (\gamma, \delta)$

$M$

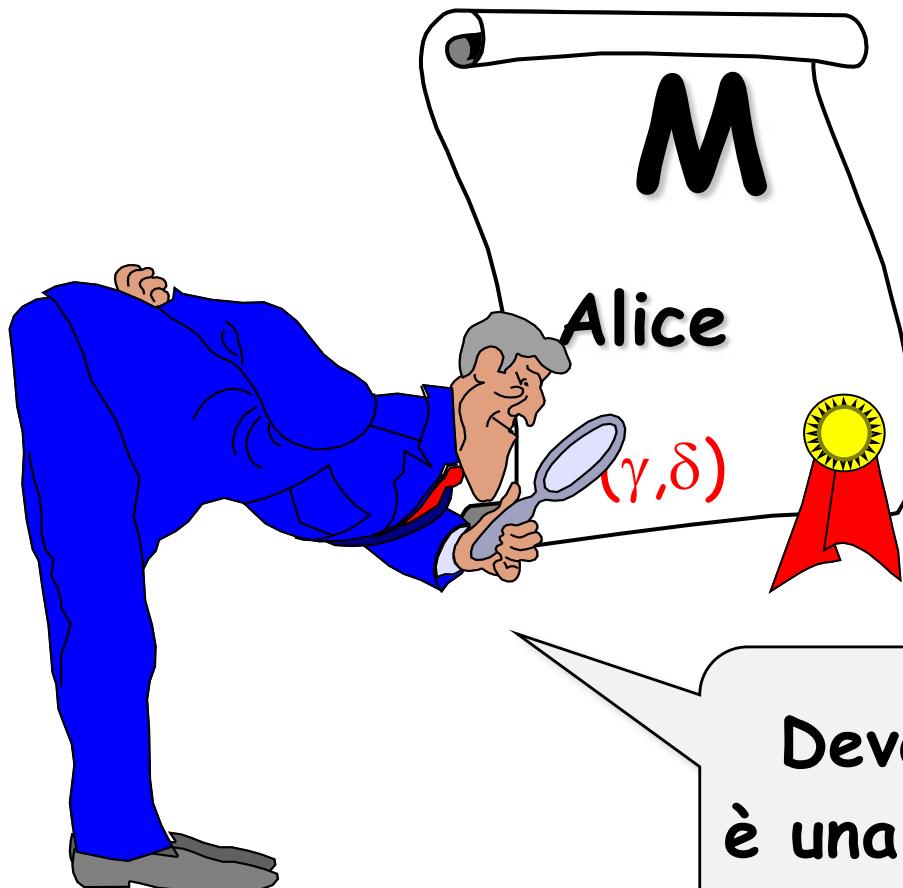
Alice  
( $\gamma, \delta$ )



# Verifica firma ElGamal

file pubblico

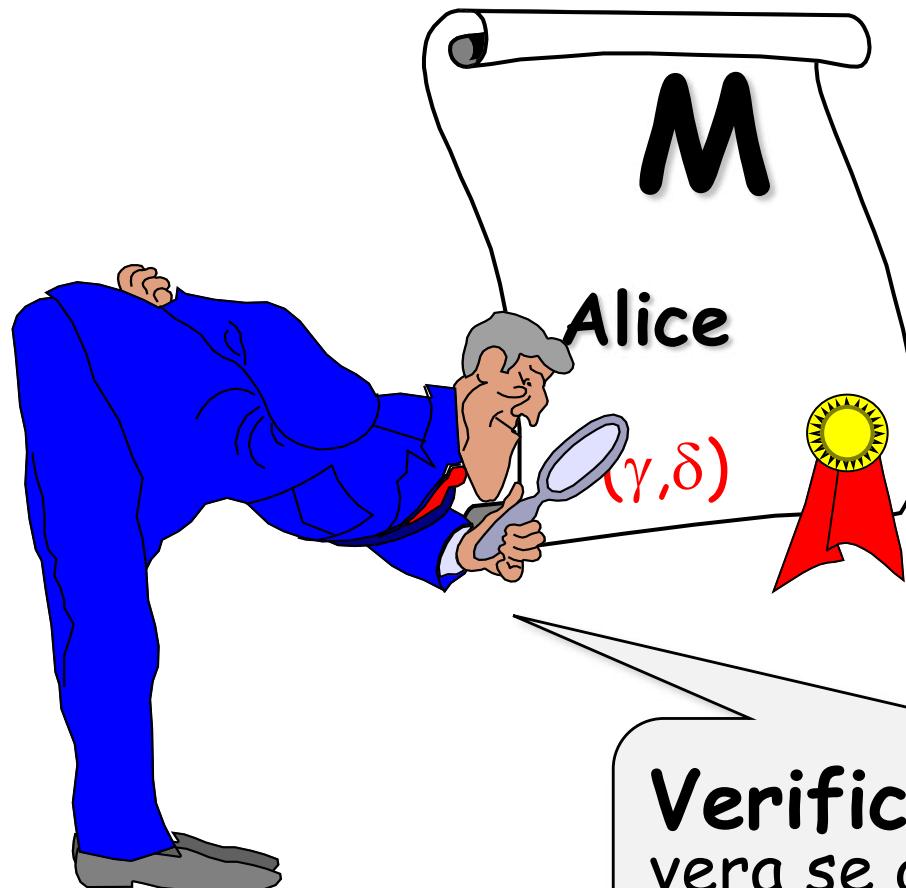
utente	chiave pubblica
Alice	$(p,g,\beta)$
...	...



# Verifica firma ElGamal

file pubblico

utente	chiave pubblica
Alice	$(p,g,\beta)$
...	...



Firma di  $M$

$r \leftarrow$  numero casuale in  $[1,p-1]$

$\gamma \leftarrow g^r \bmod p$

$\delta \leftarrow (M - s\gamma)r^{-1} \bmod p-1$

$\text{firma}_{(p,g,s)}(M,r) = (\gamma, \delta)$

Verifica firma di  $M$   
vera se  $g^M = \beta^\gamma \gamma^\delta \bmod p$   
falsa altrimenti

# Correttezza verifica firma ElGamal

$$\begin{aligned}\beta &= g^s \text{ mod } p \\ \beta^{\gamma} \gamma^{\delta} \text{ mod } p &= g^{s\gamma} \gamma^{\delta} \text{ mod } p \\ &= g^{s\gamma} g^{r\delta} \text{ mod } p \\ &= g^{s\gamma} g^{r(M-s\gamma)r^{-1}} \text{ mod } p \\ &= g^{s\gamma} g^{M-s\gamma} \text{ mod } p \\ &= g^M \text{ mod } p\end{aligned}$$

$\beta = g^s \text{ mod } p$

$\gamma = g^r \text{ mod } p$

$\delta = (M+s\gamma)r^{-1} \text{ mod } p-1$

$r r^{-1} = 1 \text{ mod } p-1$

Teorema di Fermat  
 $x \in \mathbb{Z}_p^* \Rightarrow x^{p-1} = 1 \text{ mod } p$   
quindi  
 $g^{p-1} = 1 \text{ mod } p$

# Firma ElGamal ("piccolo" esempio)

chiave privata  
(19, 10, 16)



Alice

file pubblico

utente	chiave pubblica
Alice	(19, 10, 4)
...	...

Firma di  $M=14$

$5 \leftarrow$  scelta in  $Z_{19}^*$ ,  $\gcd(5, 18) = 1$

$3 \leftarrow 10^5 \bmod 19$

$$5 \cdot 11 \equiv 1 \pmod{18}$$

$4 \leftarrow (14 - 16 \cdot 3)11 \bmod 18$

firma<sub>(19, 10, 16)</sub>(14, 5) = (3, 4)

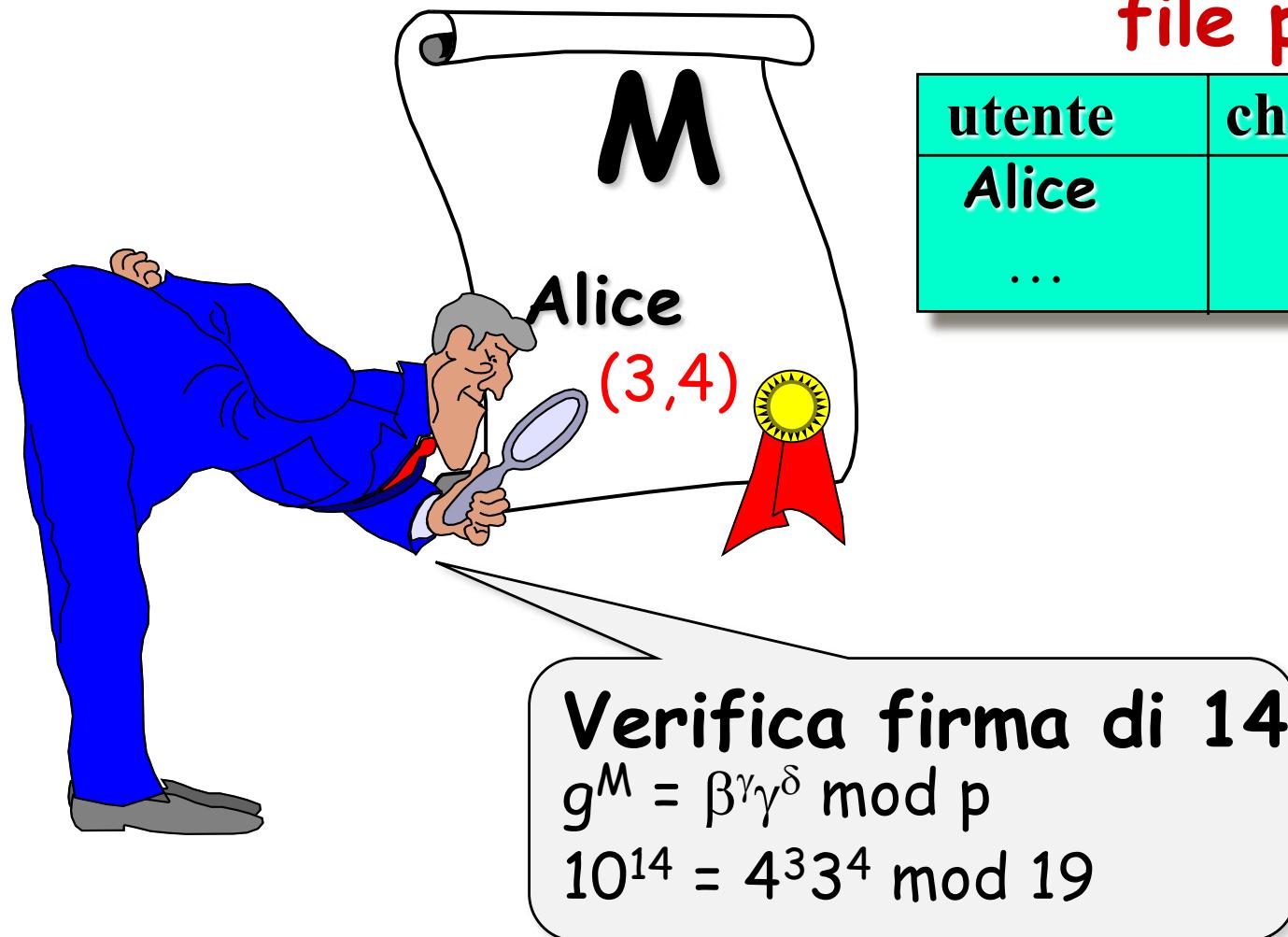
14

Alice

(3, 4)



# Verifica firma ElGamal ("piccolo" esempio)



file pubblico

utente	chiave pubblica
Alice	(19,10,4)
...	...



# Firma ElGamal

- Sicurezza basata sull'intrattabilità del problema del **logaritmo discreto** in  $Z_p^*$
- Lunghezza della firma:  $2 \log p$
- DSS modifica lo schema:
  - Generatore  $g \rightarrow \alpha$  in  $Z_p^*$  di ordine  $q$
  - Algebra esponenti modulo  $q$
  - Lunghezza della firma DSS:  $2 \log q$

# Firme digitali che vedremo

- RSA
- ElGamal
- Digital Signature Standard (DSS)



# Digital Signature Standard (DSS)

- Proposto nell'agosto del 1991 dal NIST ([FIPS 186](#))
  - Digital Signature Algorithm (DSA)
  - Digital Signature Standard (DSS)
- Revisioni minori nel 1993 ([FIPS 186-1](#))
- Rivisto nel 2000 ([FIPS 186-2](#))  
Specifica altri 2 metodi:
  - Elliptic Curve Digital Signature Algorithm (ECDSA)
  - RSA
- Rivisto nel giugno 2009 ([FIPS 186-3](#))  
Incrementa lunghezza di DSS
- Rivisto nel luglio 2013 ([FIPS 186-4](#))
- Revisione proposta nell'ottobre 2019 ([Draft FIPS 186-5](#))
  - Non specifica più DSA
  - Specifica Edwards Curve Digital Signature Algorithm (EdDSA)
  - Commenti ricevuti disponibili a tutti dal 7 aprile 2020 <https://csrc.nist.gov>

# Digital Signature Standard (DSS)

U.S. Patent 5.231.668



David W. Kravitz

dato a "The United States of America as represented by the Secretary of Commerce, Washington, D.C.", royalty-free

26 luglio 1991

United States Patent [19] US05231668A  
Kravitz [11] Patent Number: 5,231,668  
[45] Date of Patent: Jul. 27, 1993

**[54] DIGITAL SIGNATURE ALGORITHM**

[75] Inventor: David W. Kravitz, Owings Mills, Md.  
[73] Assignee: The United States of America, as represented by the Secretary of Commerce, Washington, D.C.

[21] Appl. No.: 736,451  
[22] Filed: Jul. 26, 1991

[51] Int. Cl. 5 H04K 1/00  
[52] U.S. Cl. 380/28; 380/30  
[58] Field of Search 380/28, 30

[56] References Cited  
U.S. PATENT DOCUMENTS

4,00,770	4/1980	Hellman	380/30
218,582	8/1980	Hellman	380/30
4,405,829	9/1983	Rivest	380/30
4,424,414	1/1984	Hellman	380/30
4,641,346	2/1987	Clark	380/51
4,748,661	5/1988	Shamir et al.	380/30
4,881,264	11/1989	Merkle	380/28
4,933,970	6/1990	Shamir	380/30
4,995,082	2/1991	Schnorr	380/30
5,005,200	4/1991	Fischer	380/30
5,097,504	3/1992	Camion et al.	380/30

OTHER PUBLICATIONS  
C. P. Schnorr, letter (8 pages) to Director, Computer

Systems Laboratories, Attn: Proposed FIPS, Oct. 30, 1991.  
El Gamal, Taher, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", IEEE Transactions on Information Theory, vol. IT-31, No. 4, Jul. 1985.  
Primary Examiner—Salvatore Cangialosi  
Attorney, Agent, or Firm—Schnader, Harrison, Segal & Lewis

**[57] ABSTRACT**

A method is provided for generating and verifying a digital signature of a message m. This method requires a pair of corresponding public and secret keys (y and x) for each signer, as well as a pair of public and secret values (r and k) generated for each message by the signer. The public value r is calculated according to the rule  $r = (g^k \bmod p) \bmod q$ . A value s is then selected according to the rule  $s = k^{-1} (H(m) + xr) \bmod q$  where H is a known conventional hashing function. The message m, along with the signature (r,s) is then transmitted. When the transmitted signal is received a verification process is provided. The received values of r and s are tested to determine whether they are congruent to 0 mod g. Additionally, r is tested to determine whether it is equal to v mod q, where v is computed from r, s, m and y. For legitimately executed signatures,  $v = g^k \bmod p$ .

44 Claims, 3 Drawing Sheets

```
graph TD
    START([START]) --> PICK{PICK RANDOM k}
    PICK --> MOD1["g^k MOD p"]
    MOD1 --> REDUCE["REDUCE TO  
r = (g^k MOD p) MOD q"]
    REDUCE --> MOD2["r^(-1) MOD q"]
    MOD2 --> H["H(m)"]
    H --> SUM["s = r^(-1) (H(m) + xr) MOD q"]
    SUM --> TRANSMIT["TRANSMIT (r, s)"]
    TRANSMIT --> END([A])
```

# Digital Signature Standard (DSS)

- Modifica ingegnosa dello schema di firme El Gamal
- Utilizza funzioni hash SHA-1 e SHA-224/256/384/512
  - Se più lunghe del necessario: troncate
  - SHA-1 in FIPS 186-1 e FIPS 186-2
- Firme DSS piccole (buone per smart card)
- Sicurezza basata sull'intrattabilità del problema del logaritmo discreto

# Digital Signature Standard (DSS)

- Usa numeri primi  $p$  e  $q$  di lunghezza  $L$  ed  $N$
- Lunghezza SHA  $\geq N$
- Lunghezza della firma =  $2q$

$L= p $	$N= q $	$ \text{firma} $	
1.024	160	320	Unica scelta in FIPS 186-1 e 186-2
2.048	224	448	Aggiunti nel FIPS 186-3
2.048	256	512	
3.072	256	512	

# Logaritmo discreto

Dati  $a, n, b$  calcolare  $x$  tale che  $a^x \equiv b \pmod{n}$

Esempio:  $3^x \equiv 7 \pmod{13}$  soluzione  $x = 6$

Se  $n$  è primo, i migliori algoritmi hanno complessità

$$L_n[a,c] = O(e^{(c+o(1))(\ln n)^a (\ln \ln n)^{1-a}})$$

con  $c > 0$  ed  $0 < a < 1$

Miglior algoritmo: **Number field sieve**

tempo medio euristico  $L_n[1/3, 1.923]$

# Chiavi DSA

chiave privata  
 $(p,q,\alpha,s)$



Alice

file pubblico

utente	chiave pubblica
Alice	$(p,q,\alpha,\beta)$
...	...

# Chiavi DSA

chiave privata  
( $p, q, \alpha, s$ )



Alice

file pubblico

utente	chiave pubblica
Alice ...	( $p, q, \alpha, \beta$ )

$p$  primo di  $L$  bit

$s$  numero casuale,  $s < q$

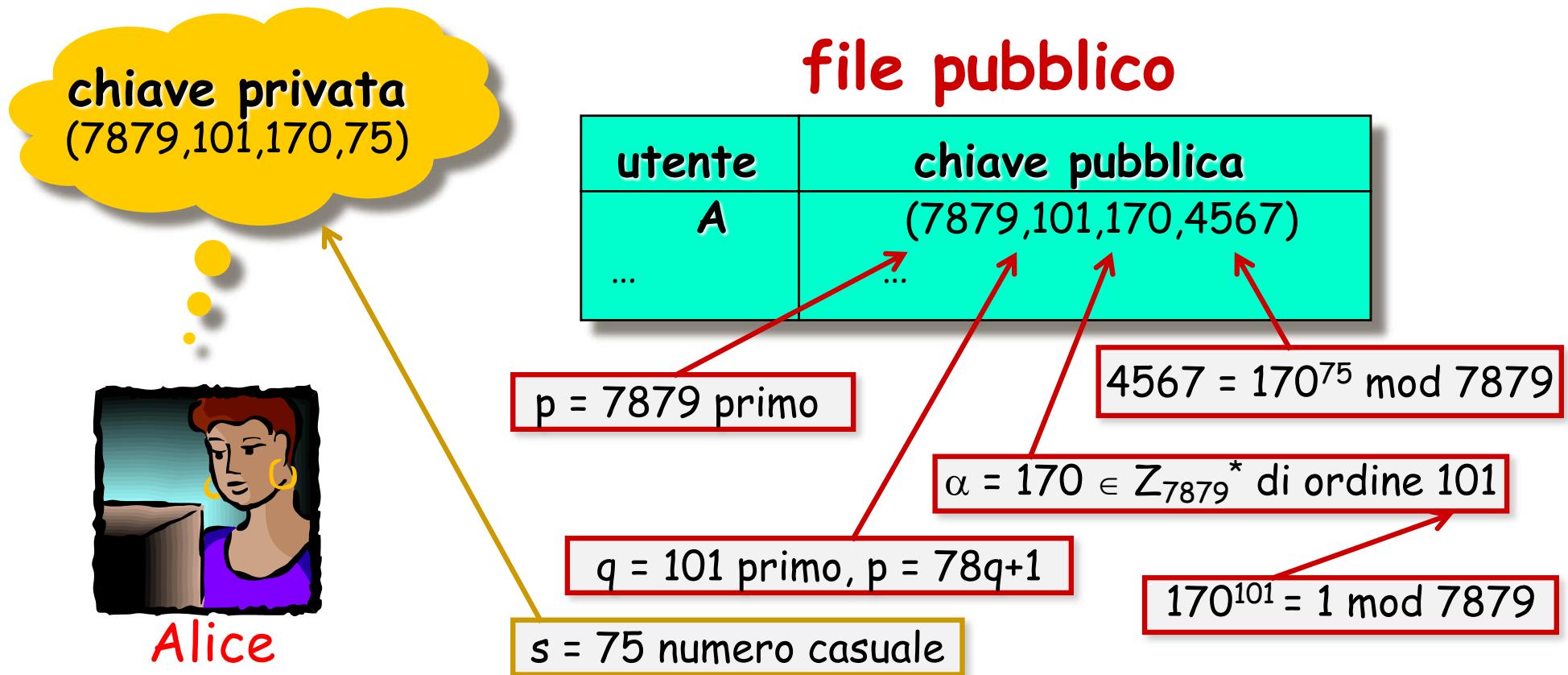
$q$  primo di  $N$  bit,  $q | (p-1)$

$\beta = \alpha^s \text{ mod } p$

$\alpha$  in  $Z_p^*$  di ordine  $q$

$\alpha^q = 1 \text{ mod } p$

# Chiavi DSA ("piccolo" esempio)



# Firma DSA



Alice

file pubblico

utente	chiave pubblica
Alice	(p, q, α, β)
...	...

Devo firmare M



# Firma DSA

chiave privata  
 $(p, q, \alpha, s)$



Alice

file pubblico

utente	chiave pubblica
Alice	$(p, q, \alpha, \beta)$
...	...

## Firma di M

$r \leftarrow$  numero casuale in  $[1, q-1]$

$\gamma \leftarrow (\alpha^r \bmod p) \bmod q$

$\delta \leftarrow (SHA(M) + s\gamma)r^{-1} \bmod q$

$firma_{(p, q, \alpha, s)}(M, r) = (\gamma, \delta)$

$r^{-1} \bmod q$  esiste perché

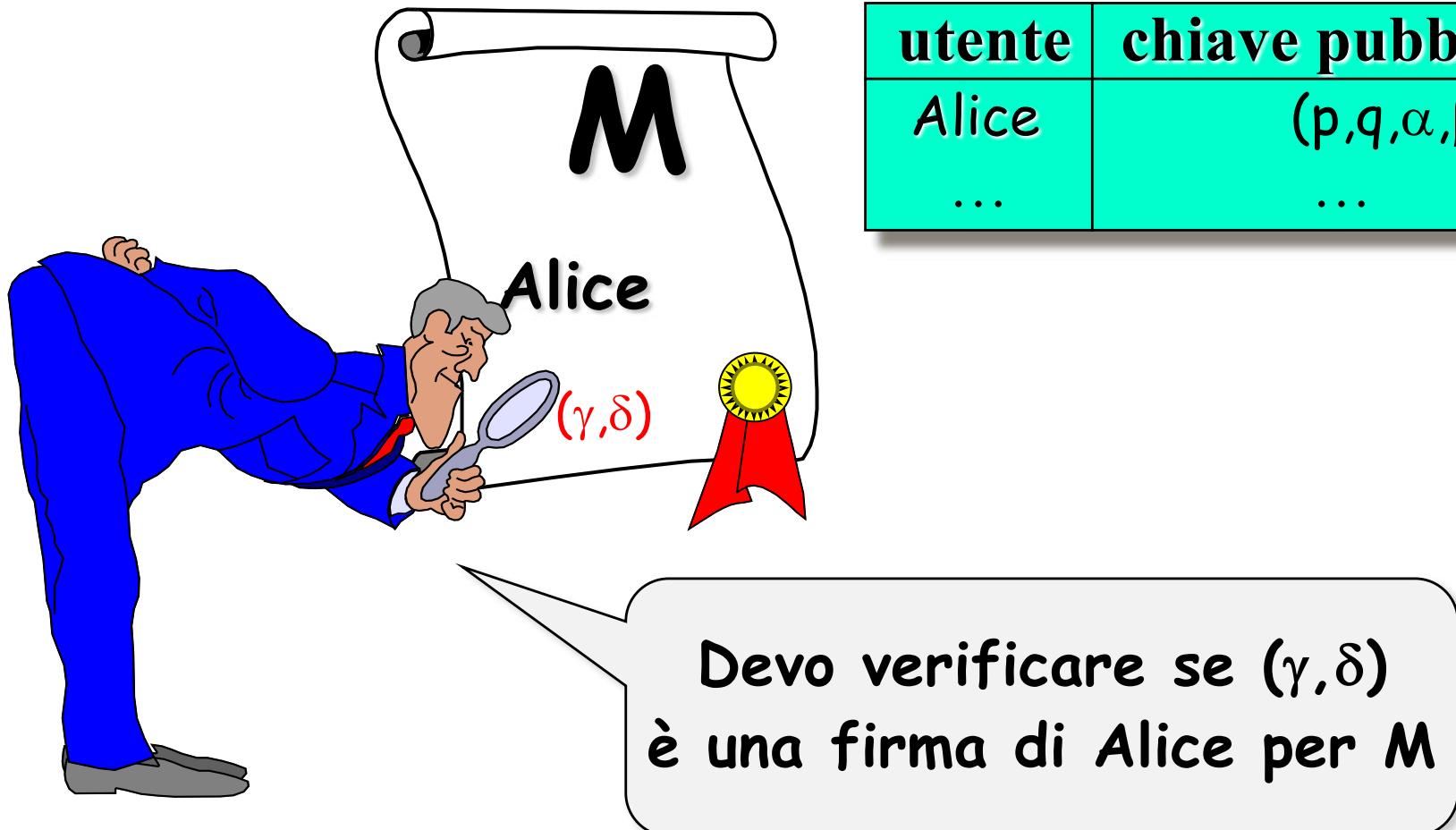
$r < q$  e  $q$  primo  $\rightarrow \gcd(q, r) = 1$



# Verifica firma DSA

file pubblico

utente	chiave pubblica
Alice	$(p, q, \alpha, \beta)$
...	...



# Verifica firma DSA

Alice is examining a document  $M$  with a magnifying glass. A red ribbon with the signature components  $(\gamma, \delta)$  is attached to the document. To the right, there is a table titled "file pubblico" (public file) containing user information and public key details.

utente	chiave pubblica
A ...	$(p, q, \alpha, \beta)$ ...

**Verifica firma di  $M$**

$e' \leftarrow \text{SHA}(M)\delta^{-1} \bmod q$   
 $e'' \leftarrow \gamma\delta^{-1} \bmod q$   
vera se  $\gamma = (\alpha^{e'}\beta^{e''} \bmod p) \bmod q$   
falsa altrimenti

# Verifica firma DSA

**Verifica\_firma\_DSA( $M, \gamma, \delta, p, q, \alpha, \beta$ )**

$$e' \leftarrow \text{SHA}(M)\delta^{-1} \bmod q$$

$$e'' \leftarrow \gamma\delta^{-1} \bmod q$$

$$\text{ver}_{(p,q,\alpha,\beta)}(M, \gamma, \delta) = \begin{cases} \text{vera se } \gamma = (\alpha^{e'}\beta^{e''} \bmod p) \bmod q \\ \text{falsa altrimenti} \end{cases}$$

**Output**  $\text{ver}_{(p,q,\alpha,\beta)}(M, \gamma, \delta)$

# Efficienza firma DSA

**Firma\_DSA( $M, p, q, \alpha, s$ )**

$r \leftarrow$  numero casuale in  $[1, q-1]$

$\gamma \leftarrow (\alpha^r \bmod p) \bmod q$

$\delta \leftarrow (SHA(M) + s\gamma)r^{-1} \bmod q$

**output**  $firma_{(p, q, \alpha, s)}(M, r) = (\gamma, \delta)$

- Lunghezza firma =  $2N$  bit
- Computazioni off-line:  $r, s\gamma, r^{-1} \bmod q$
- Computazioni on-line:  $SHA(M), +, \cdot$

# Ordine di un elemento

- Ordine di  $\alpha \in \mathbb{Z}_p^*$  = il più piccolo intero positivo  $r$  tale che  $\alpha^r \equiv 1 \pmod{p}$
- Sia  $\alpha \in \mathbb{Z}_p^*$  e sia  $q = \text{ordine}(\alpha)$ 
  - $\alpha^{s \cdot q} \pmod{p} = \alpha^s \pmod{p}$

# Potenze in $\mathbb{Z}_{19}^*$

# Correttezza verifica firma DSA

$$\begin{aligned} & e' = \text{SHA}(M)\delta^{-1} \bmod q \\ & (\alpha^{e'}\beta^{e''} \bmod p) \bmod q \\ &= (\alpha^{\text{SHA}(M)\delta^{-1}} \bmod q \quad \alpha^{s\gamma\delta^{-1}} \bmod q \bmod p) \bmod q \\ & \qquad \qquad \qquad \alpha \text{ è di ordine } q \\ &= (\alpha^{\text{SHA}(M)\delta^{-1}+s\gamma\delta^{-1}} \bmod p) \bmod q \\ & \qquad \qquad \qquad \delta^{-1}(\text{SHA}(M)+s\gamma) = r \bmod q \\ &= (\alpha^r \bmod p) \bmod q \\ &= \gamma \end{aligned}$$

# Efficienza delle computazioni

Come effettuare le computazioni?

- Generazione numeri primi  $p$  e  $q$
- Generazione di  $\alpha$  (elemento di ordine  $q$ )



# Generazione di p e q

Scegli p di L bit

Scegli q di N bit tale che  $q \mid (p-1)$

# Generazione di p e q

Scegli p di L bit

Scegli q di N bit tali che  $q \mid (p-1)$



# Generazione di p e q

- Scegli un primo  $q$  di  $N$  bit
- Scegli un primo  $p$  di  $L$  bit tale che  $q \mid (p-1)$ 
  1. Scegli  $X$  di  $L$  bit
  2.  $p \leftarrow X - (X \bmod 2q) + 1$
  3. if  $p$  è primo e  $p \geq 2^L$  then esci else go to 1.

$$2q \mid (X - (X \bmod 2q))$$
$$2q \mid (p-1)$$

# Scelta di un elemento di ordine q

- Ordine di  $\alpha \in \mathbb{Z}_n^*$  = il più piccolo intero positivo r tale che  $\alpha^r \equiv 1 \pmod{n}$
- p,q primi tali che  $q \mid (p-1)$

**Scegli\_ordineq (p,q)**

1.  $g \leftarrow$  elemento scelto a caso in  $\mathbb{Z}_p^*$
2.  $\alpha \leftarrow g^{(p-1)/q} \pmod{p}$
3. if  $\alpha \neq 1$  then return  $\alpha$  else go to 1.

# Potenze in $\mathbb{Z}_{19}^*$

# Scelta di un elemento di ordine q

**Scegli\_ordineq (p,q)**

1.  $g \leftarrow$  elemento scelto a caso in  $\mathbb{Z}_p^*$

2.  $\alpha \leftarrow g^{(p-1)/q} \bmod p$

3. if  $\alpha \neq 1$  then return  $\alpha$  else go to 1.

- $\alpha^q \equiv (g^{(p-1)/q})^q \equiv g^{p-1} \equiv 1 \bmod p$
- q è il più piccolo intero tale che  $\alpha^q \equiv 1 \bmod n$
- $\alpha$  è di ordine q

dal Teorema di Lagrange  
l'ordine di  $\alpha$  divide q

# Probabilità successo singola iterazione

- Se  $g$  è un generatore allora  $g^{(p-1)/q} \neq 1 \pmod{p}$
- Probabilità successo  $\geq$  Probabilità che  $g$  è generatore
  - >  $1/(6\ln\ln(p-1))$
- Numero medio di iterazioni  $< 6\ln\ln(p-1)$

512 bit	$6 \cdot \ln\ln(2^{512}) \approx 35,23$
1024 bit	$6 \cdot \ln\ln(2^{1024}) \approx 39,38$
2048 bit	$6 \cdot \ln\ln(2^{2048}) \approx 43,54$
3072 bit	$6 \cdot \ln\ln(2^{3072}) \approx 45,98$

# Sicurezza firma DSA

Vediamo:

- Total break - Key only attack
- Selective forgery - Key only attack
- Problemi uso dello stesso valore casuale r

# Sicurezza firma DSA

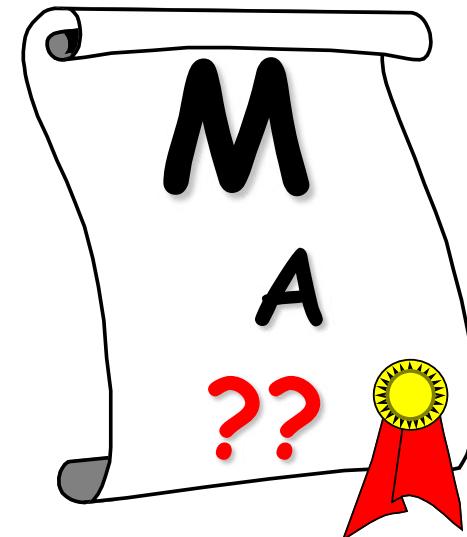
Voglio falsificare la  
firma di M da parte di A

file pubblico

utente	chiave pubblica
A	(p,q, $\alpha$ , $\beta$ )
...	...



Total break  
Key only attack



# Sicurezza firma DSA

Voglio falsificare la firma di M da parte di A

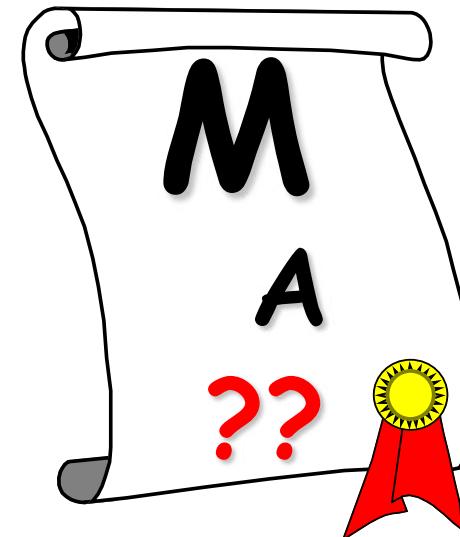
file pubblico

utente	chiave pubblica
A	(p,q, $\alpha$ , $\beta$ )
...	...



Devo calcolare  
 $s = \log_{\alpha} \beta \bmod p \dots$

Total break  
Key only attack



# Sicurezza firma DSA

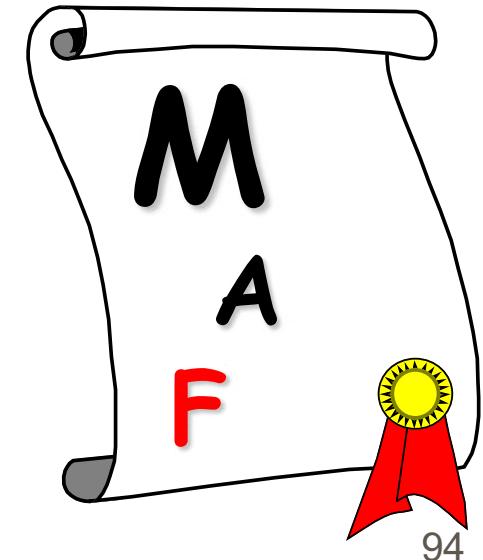
Voglio falsificare la firma  
di M da parte di A



file pubblico

utente	chiave pubblica
A	$(p,q,\alpha,\beta)$
...	...

Selective forgery  
Key only attack



# Sicurezza firma DSA

Voglio falsificare la firma  
di M da parte di A

file pubblico

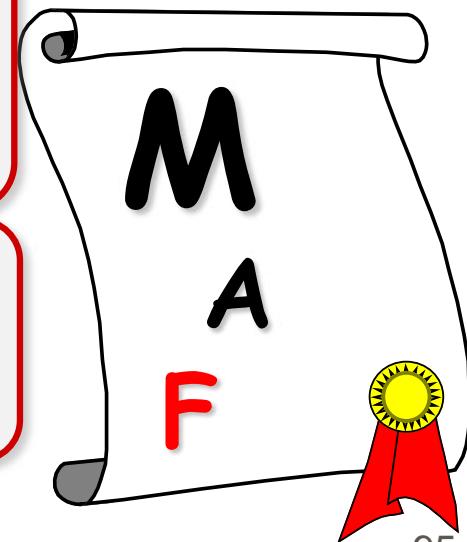
utente	chiave pubblica
A	(p,q, $\alpha$ , $\beta$ )
...	...



1. Scelgo  $\gamma$  a caso
2. Determino  $\delta$  tale che  
$$\delta \leftarrow (\text{SHA}(M) + s\gamma)r^{-1} \text{ mod } q$$

Selective forgery  
Key only attack

Devo calcolare  
$$\delta = \log_{\gamma} (\alpha^{\text{SHA}(M)} \cdot \beta^{\gamma}) \dots$$



# Sicurezza firma DSA

Voglio generare messaggi e firme da parte di A

file pubblico

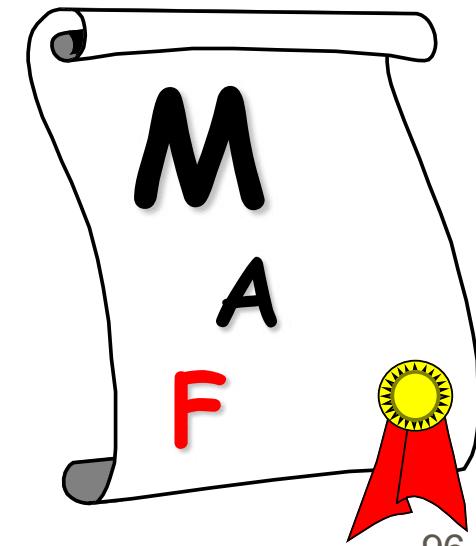
utente	chiave pubblica
A	(p,q, $\alpha$ , $\beta$ )
...	...



1. Scelgo  $\gamma, \delta$  a caso
2. Calcolo z tale che  
$$\alpha^z = \gamma^\delta \beta^{-\gamma}$$

Existential forgery  
Key only attack

Devo calcolare  
$$z = \log_{\alpha} (\gamma^\delta \beta^{-\gamma}) \dots$$
  
$$M \leftarrow \text{SHA}^{-1}(z) \dots$$



# Sicurezza firma DSA

con lo stesso valore casuale

chiave privata  
( $p, q, \alpha, s$ )



Alice

file pubblico

utente	chiave pubblica
Alice	( $p, q, \alpha, \beta$ )
...	...

Firma di  $M_1$

$$\begin{aligned} r &\leftarrow \text{numero casuale in } [1, q-1] \\ \gamma &\leftarrow (\alpha^r \bmod p) \bmod q \\ \delta_1 &\leftarrow (\text{SHA}(M_1) + s\gamma)r^{-1} \bmod q \\ \text{firma}_{(p,q,\alpha,s)}(M_1, r) &= (\gamma, \delta_1) \end{aligned}$$

Firma di  $M_2$

$$\begin{aligned} r &\leftarrow \text{stesso valore usato per } M_1 \\ \gamma &\leftarrow (\alpha^r \bmod p) \bmod q \\ \delta_B &\leftarrow (\text{SHA}(M_2) + s\gamma)r^{-1} \bmod q \\ \text{firma}_{(p,q,\alpha,s)}(M_2, r) &= (\gamma, \delta_2) \end{aligned}$$

# Sicurezza firma DSA

con lo stesso valore casuale

chiave privata  
( $p, q, \alpha, s$ )



Alice

file pubblico

utente	chiave pubblica
Alice	( $p, q, \alpha, \beta$ )
...	...

Firma di  $M_1$

$r \leftarrow$  numero casuale in  $[1, q-1]$   
 $\gamma \leftarrow (\alpha^r \bmod p) \bmod q$   
 $\delta_1 \leftarrow (\text{SHA}(M_1) + s\gamma)r^{-1} \bmod q$   
 $\text{firma}_{(p,q,\alpha,s)}(M_1, r) = (\gamma, \delta_1)$

Firma di  $M_2$

$r \leftarrow$  stesso valore usato per  $M_1$   
 $\gamma \leftarrow (\alpha^r \bmod p) \bmod q$   
 $\delta_B \leftarrow (\text{SHA}(M_2) + s\gamma)r^{-1} \bmod q$   
 $\text{firma}_{(p,q,\alpha,s)}(M_2, r) = (\gamma, \delta_2)$

Dati  $M_1 M_2 (\gamma, \delta_1) (\gamma, \delta_2)$

>calcolo r  
>poi calcolo s



# Sicurezza firma DSA

## con lo stesso valore casuale

Dati  $M_1$   $M_2$   $(\gamma, \delta_1)$   $(\gamma, \delta_2)$  calcolo r

da  $\delta_1 \leftarrow (\text{SHA}(M_1) + s\gamma) r^{-1} \pmod q$

$\delta_2 \leftarrow (\text{SHA}(M_2) + s\gamma) r^{-1} \pmod q$

otteniamo

$$\delta_1 - \delta_2 = (\text{SHA}(M_1) - \text{SHA}(M_2) + s\gamma - s\gamma) r^{-1} \pmod q$$

$$\delta_1 - \delta_2 = (\text{SHA}(M_1) - \text{SHA}(M_2)) r^{-1} \pmod q$$

$$r = (\text{SHA}(M_1) - \text{SHA}(M_2)) (\delta_1 - \delta_2)^{-1} \pmod q$$

$$\beta = \alpha^s \pmod p$$

Alice

Firma di  $M_2$

$r \leftarrow$  stesso valore usato per  $M_1$

$\gamma \leftarrow (\alpha^r \pmod p) \pmod q$

$\delta_B \leftarrow (\text{SHA}(M_2) + s\gamma) r^{-1} \pmod q$

firma<sub>(p,q, $\alpha$ ,s)</sub>( $M_2, r$ ) =  $(\gamma, \delta_2)$



$M_1 M_2 (\gamma, \delta_1) (\gamma, \delta_2)$

calcolo r

poi calcolo s

# Sicurezza firma DSA

## con lo stesso valore casuale

Dati  $M_1$   $M_2$   $(\gamma, \delta_1)$   $(\gamma, \delta_2)$  calcolo r

da  $\delta_1 \leftarrow (\text{SHA}(M_1) + s\gamma) r^{-1} \text{ mod } q$

$\delta_2 \leftarrow (\text{SHA}(M_2) + s\gamma) r^{-1} \text{ mod } q$

otteniamo

$$\delta_1 - \delta_2 = (\text{SHA}(M_1) - \text{SHA}(M_2) + s\gamma - s\gamma) r^{-1} \text{ mod } q$$

$$\delta_1 - \delta_2 = (\text{SHA}(M_1) - \text{SHA}(M_2)) r^{-1} \text{ mod } q$$

$$r = (\text{SHA}(M_1) - \text{SHA}(M_2)) (\delta_1 - \delta_2)^{-1} \text{ mod } q$$

$$\beta = \alpha^s \text{ mod } p$$

Dati  $M_1$   $M_2$   $(\gamma, \delta_1)$   $(\gamma, \delta_2)$  r calcolo s

da  $\delta_1 \leftarrow (\text{SHA}(M_1) + s\gamma) r^{-1} \text{ mod } q$

otteniamo  $s = (r\delta_1 - \text{SHA}(M_1)) \gamma^{-1} \text{ mod } q$

# Playstation 3 uso stesso valore casuale

Gruppo *failOverflow*  
annuncia recupero  
chiave privata  
ECDSA usata da  
Sony per firmare  
software per la  
PlayStation 3

<http://www.exophage.com/20540/hackers-describe-ps3-security-as-epic-fail-gain-unrestricted-access/>

## Hackers Describe PS3 Security As Epic Fail, Gain Unrestricted Access

BY MIKE BENDEL

DECEMBER 29, 2010 @ 11:19 AM



Prominent hackers Bushing, Marcan, and Sven took the stage at this year's annual Chaos Communication Congress (27C3) to showcase their latest underground efforts on PS3. The trio describe Sony's security measures as an 'epic fail,' pointing to the botched implementation of ECDSA. Apparently, the so-called 'random' number used to create the private key is always static.

What does mean for you, the end-user? Well, it means that homebrew devs can essentially sign their own applications. The keys generated as every bit as valid Sony's own official signatures. Full control means custom firmware is within grasp. What's more, is that the feat is valid for all current firmware up to 3.55 and possibly beyond.

# Elliptic Curve Digital Signature Algorithm (ECDSA)

- Variante del DSS
- Computazioni su curve ellittiche
  - usa un punto su curva ed il suo ordine
- Lunghezza firma inferiore a DSS con la stessa sicurezza



# Curve Ellittiche sui Reali

Descritte da equazioni cubiche

$$y^2 = x^3 + ax + b$$

costanti tali che  $4a^3 + 27b^2 \neq 0$

(Condizione necessaria e sufficiente perché  $x^3+ax+b$  abbia 3 radici distinte, reali o complesse)

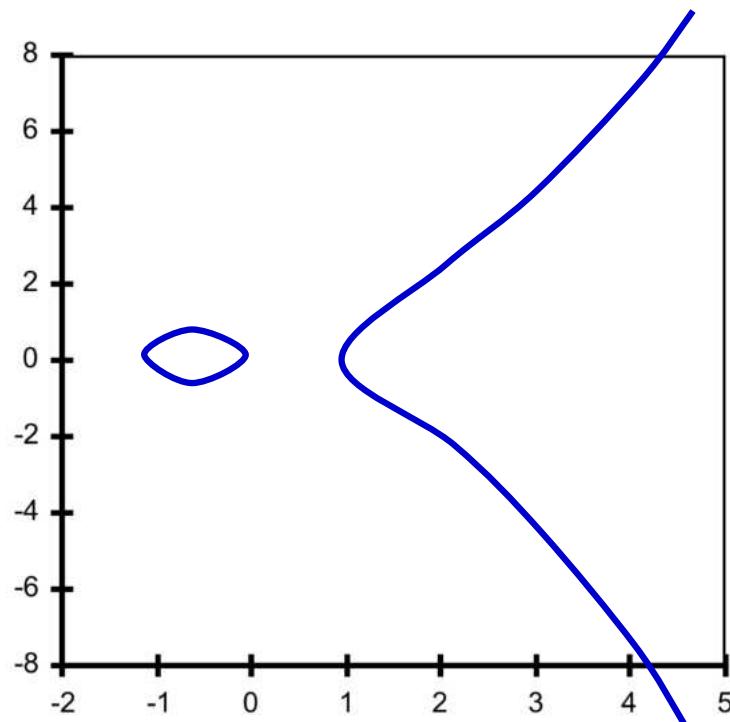
Includono

Punto all'infinito o punto zero  $O$

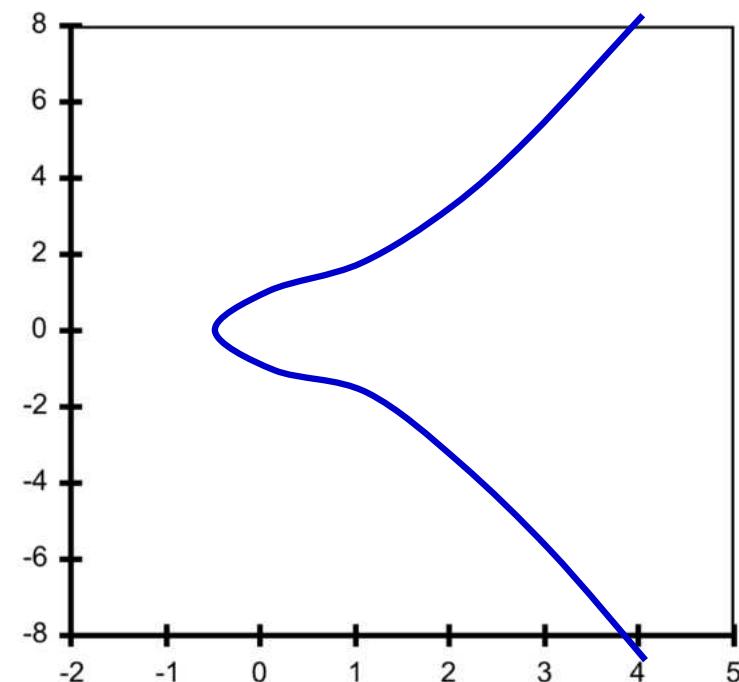


# Esempi

$$y^2 = x^3 - x$$



$$y^2 = x^3 + x + 1$$

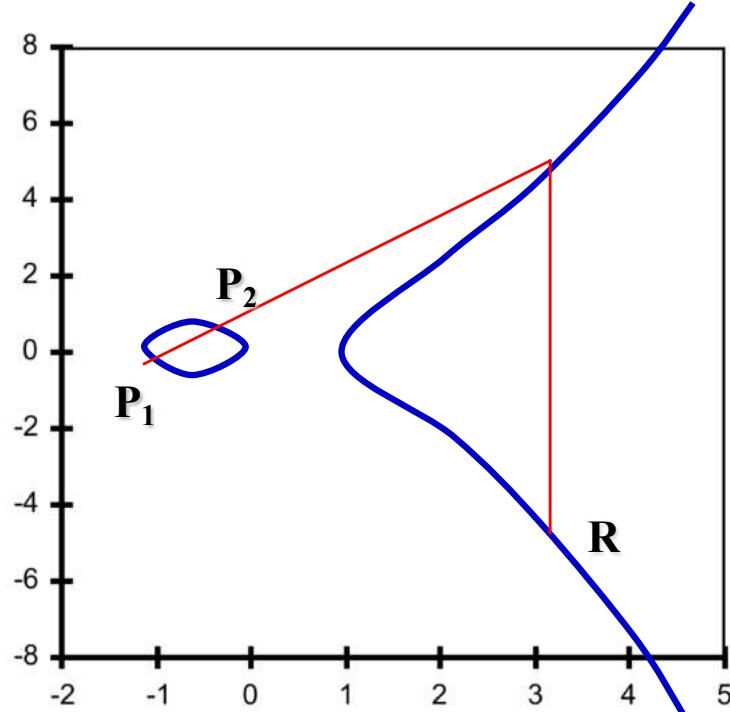




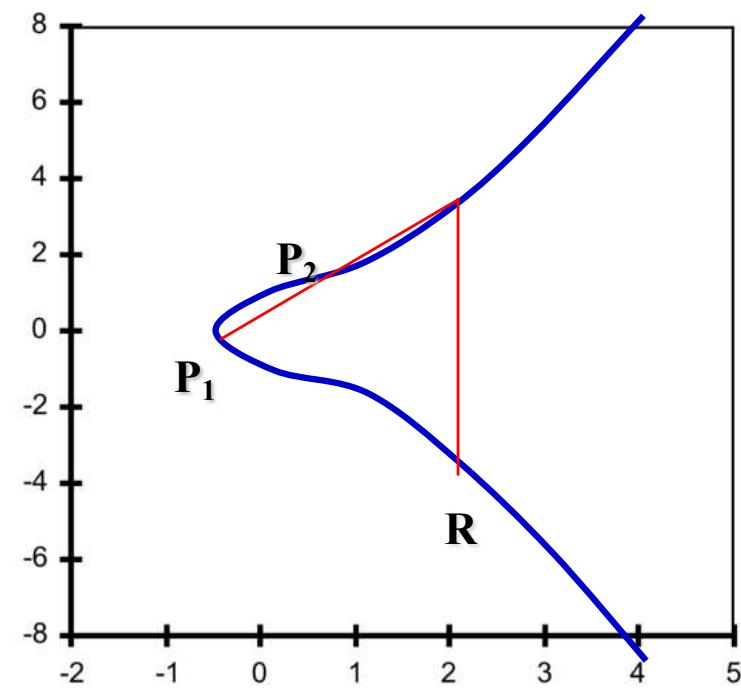
# Addizione

$$P_1 + P_2 = R$$

$$y^2 = x^3 - x$$



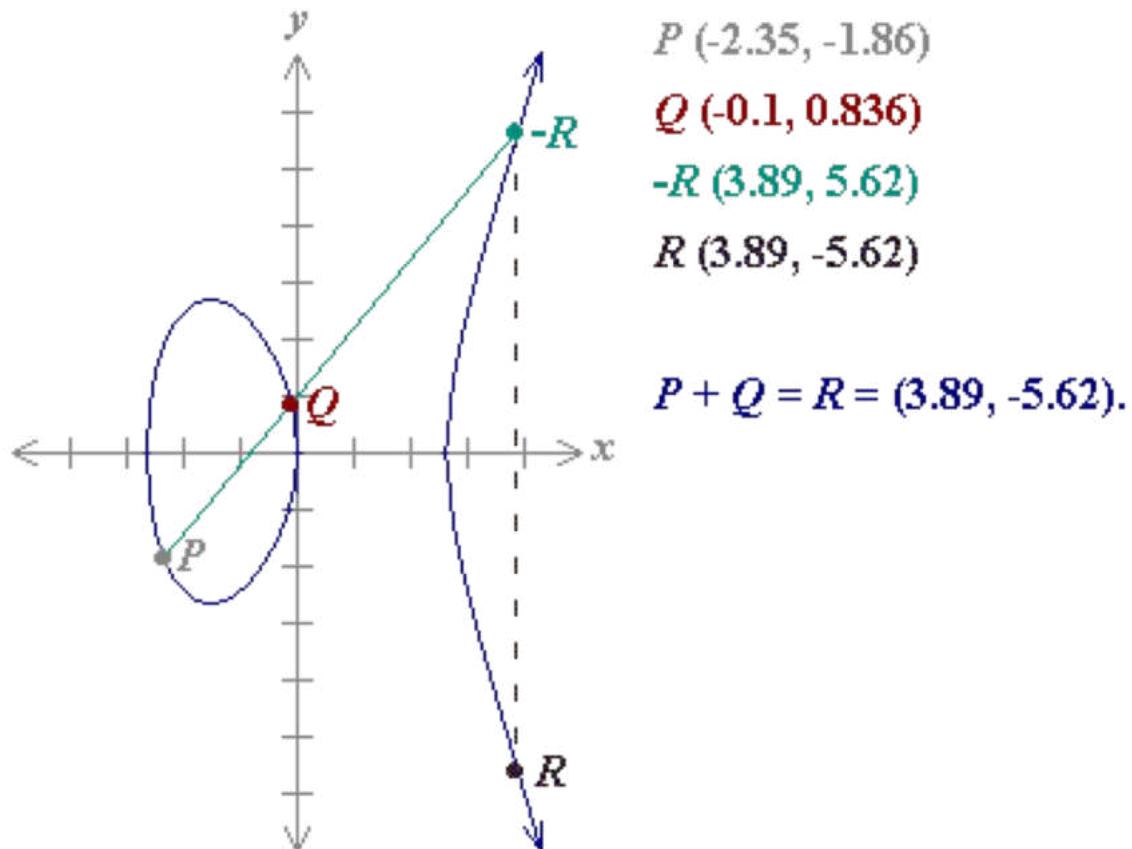
$$y^2 = x^3 + x + 1$$



Interpretazione geometrica di una addizione



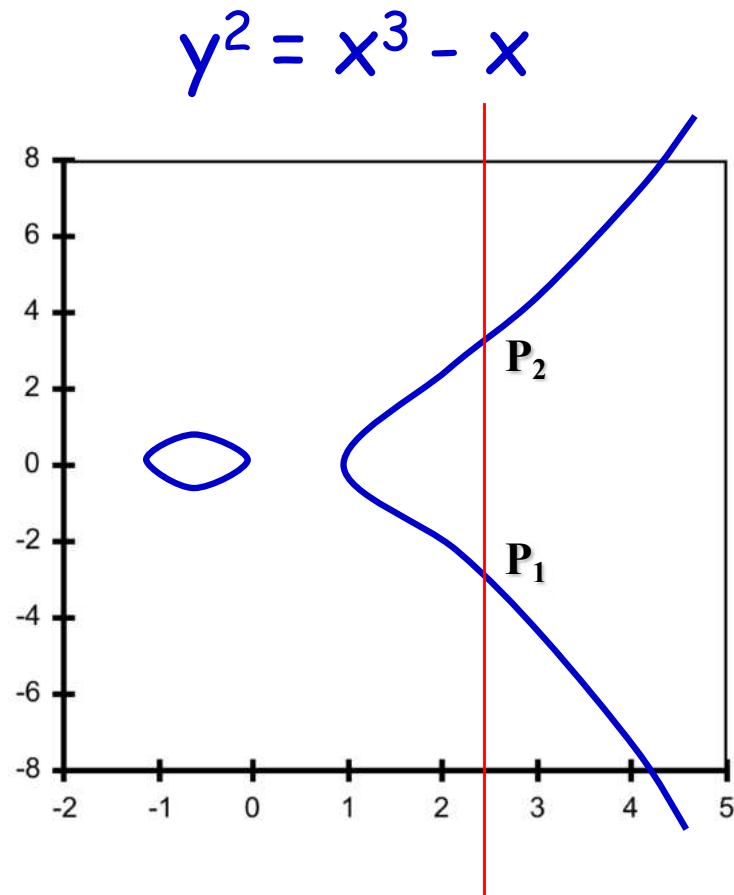
# Addizione



$$y^2 = x^3 - 7x$$



# Addizione



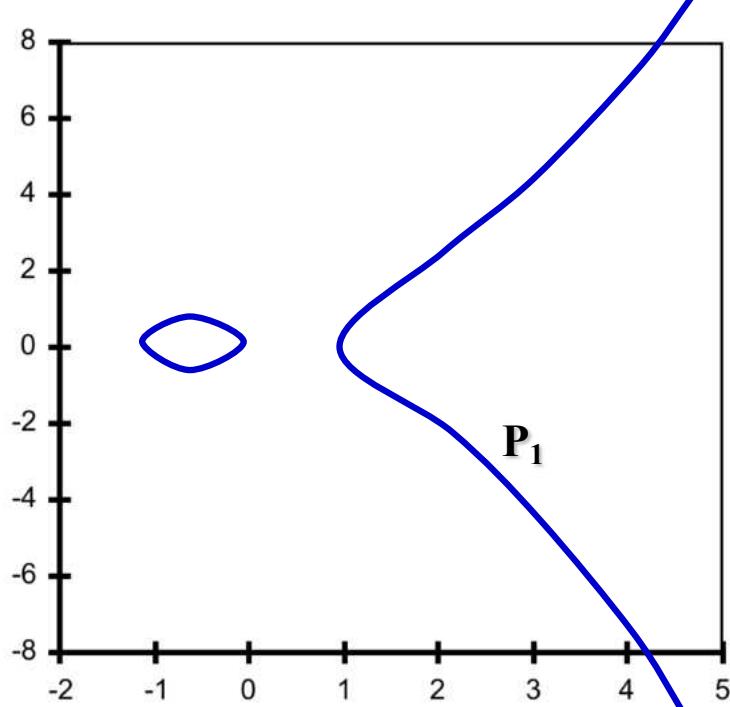
$P_1 P_2$  con stessa  $x$

$$P_1 + P_2 = O$$

$$P_1 = -P_2$$

# Addizione

$$y^2 = x^3 - x$$

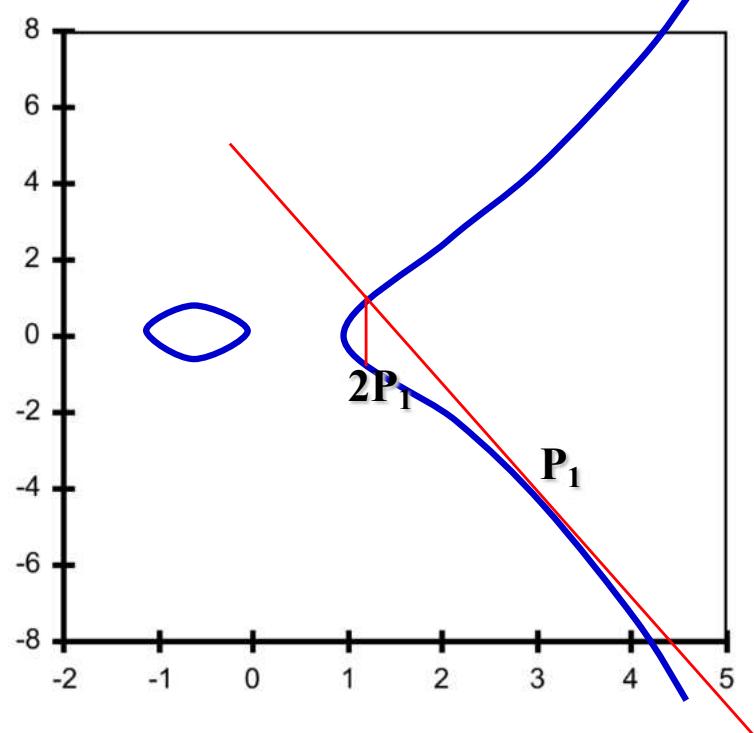


Identità additiva

$$P_1 + O = O + P_1 = P_1$$
$$O = -O$$

# Moltiplicazione

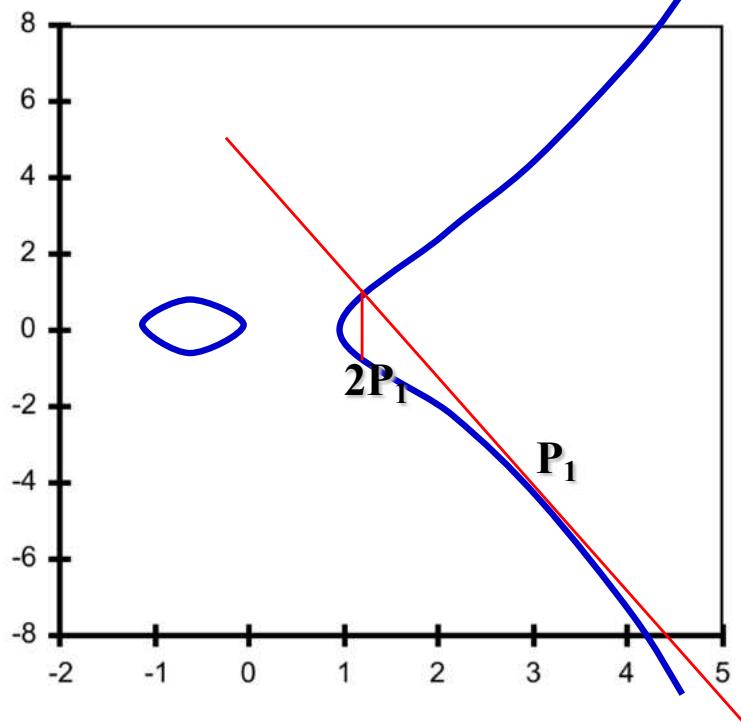
$$y^2 = x^3 - x$$



$$2 P_1 = P_1 + P_1$$

# Moltiplicazione

$$y^2 = x^3 - x$$



$$2 P_1 = P_1 + P_1$$

$$k P_1 = \underbrace{P_1 + \dots + P_1}_{k \text{ volte}}$$

# Curve Ellittiche su $\mathbb{Z}_p$

Sono i punti  $(x,y)$  in  $\mathbb{Z}_p \times \mathbb{Z}_p$  tali che

$$y^2 = x^3 + ax + b \pmod{p}$$

$p > 3$  numero primo

$a, b$  in  $\mathbb{Z}_p$  tali che  $4a^3 + 27b^2 \neq 0 \pmod{p}$

Punto all'infinito o punto zero  $O$

# Addizione

$$P_3 = P_1 + P_2$$
$$P_3 = (x_3, y_3)$$
$$P_1 = (x_1, y_1)$$
$$P_2 = (x_2, y_2)$$

$$\begin{cases} x_1 = x_2 \\ y_1 = -y_2 \end{cases} \quad \text{allora } P_3 = O$$

Altrimenti

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2 \\ y_3 = \lambda(x_1 - x_3) - y_1 \end{cases}$$

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{se } P_1 \neq P_2 \\ \frac{3x_1^2 + a}{2y_1} & \text{se } P_1 = P_2 \end{cases}$$

# Addizione

$$P_3 = P_1 + P_2$$

$$P_3 = (x_3, y_3)$$

$$P_1 = (x_1, y_1)$$

$$P_2 = (x_2, y_2)$$

$$P_1 + O = O + P_1 = P_1$$

$$O = -O$$

Inverso additivo  $- (x_1, y_1) = (x_1, -y_1)$

$E_p(a,b)$  è un gruppo abeliano

# Esempio $E_{23}(1,1)$

$$y^2 = x^3 + x + 1 \pmod{23}$$

(0,1)	(6,4)	(12,19)
(0,22)	(6,19)	(13,7)
(1,7)	(7,11)	(13,16)
(1,16)	(7,12)	(17,3)
(3,10)	(9,7)	(18,3)
(3,13)	(9,16)	(18,20)
(4,0)	(11,3)	(19,5)
(5,4)	(11,20)	(19,18)
(5,19)	(12,4)	

$$4a^3 + 27b^2 \neq 0 \pmod{p}$$

$$4 \cdot 1^3 + 27 \cdot 1^2 = 8 \neq 0 \pmod{23}$$

Approccio geometrico  
non più valido!

# Elliptic Curve Digital Signature Algorithm (ECDSA)

FIPS PUB 186-4, July 2013

# Elliptic Curve Digital Signature Algorithm (ECDSA)

$$y^2 = x^3 - 3x + b \pmod{p}$$

Curve P-224

$p = 26959946667150639794667015087019630673557916260026308143510066298881$

...

Recommended Elliptic Curves for Federal Government Use, July 1999

<http://csrc.nist.gov/groups/ST/toolkit/documents/dss/NISTReCur.pdf>

# Chiavi globali ed individuali



**file pubblico**

utente	chiave pubblica
A	(p,q,\alpha,\beta)
...	...

- Sicurezza basata sul valore privato  $s$
- I valori  $p,q,\alpha$  possono essere gli stessi per un gruppo di utenti
- Un'autorità sceglie  $p,q,\alpha$
- Il singolo utente sceglie solo  $s$  e calcola  $\beta$

# Chiavi globali ed individuali



Alice

file pubblico

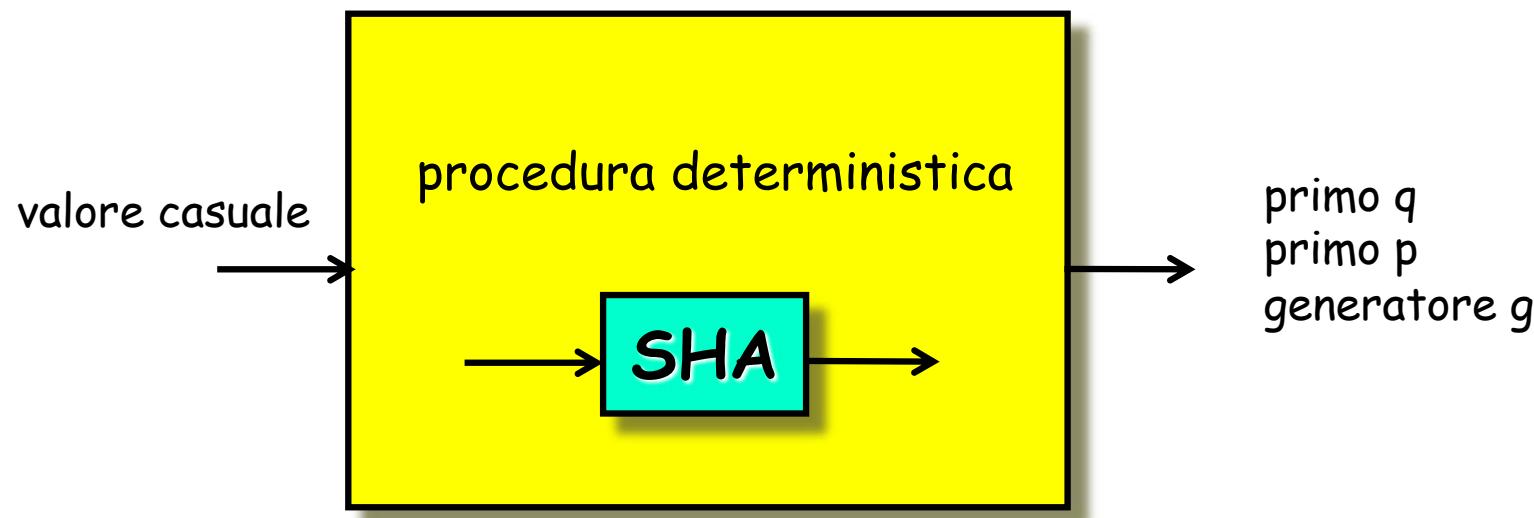
utente	chiave pubblica
A	( $p, q, \alpha, \beta$ )
...	...

- Sicurezza basata sul valore privato  $s$
- I valori  $p, q, \alpha$  possono essere gli stessi per un gruppo di utenti
- Un'autorità sceglie  $p, q, \alpha$
- Il singolo utente sceglie solo  $s$  e calcola  $\beta$



# Costruzione e validazione dei parametri

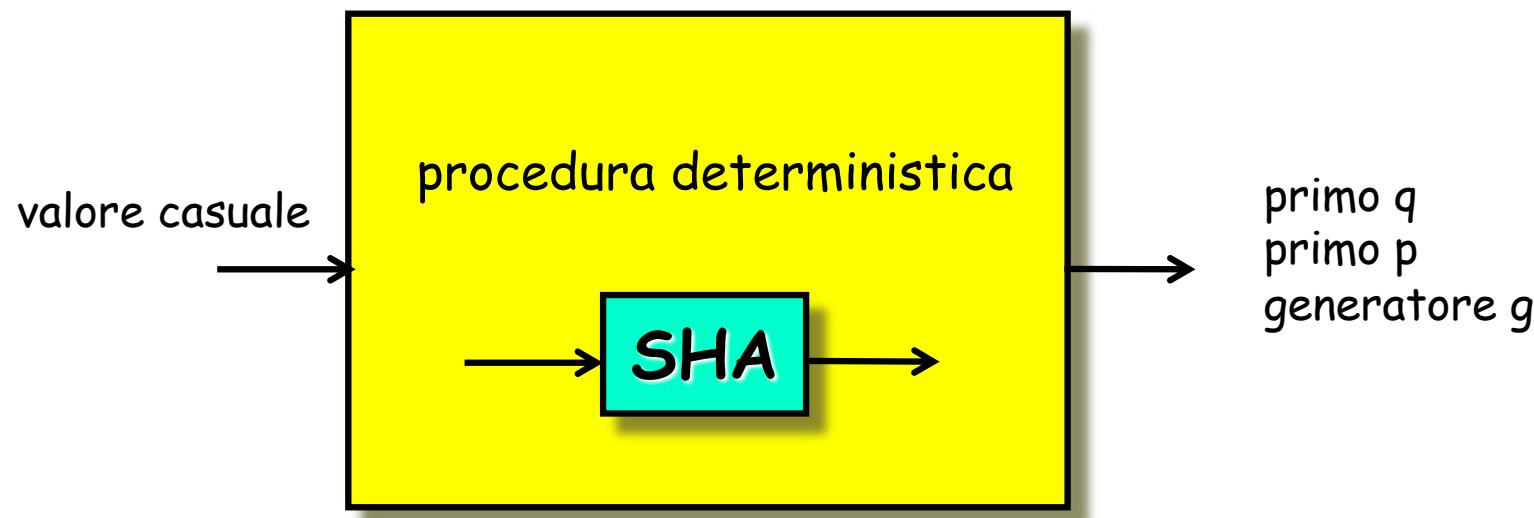
FIPS 186-1, 186-2, 186-3 e 186-4



"valore casuale" è un testimone della validità dei parametri

# Costruzione e validazione dei parametri

FIPS 186-1, 186-2, 186-3 e 186-4



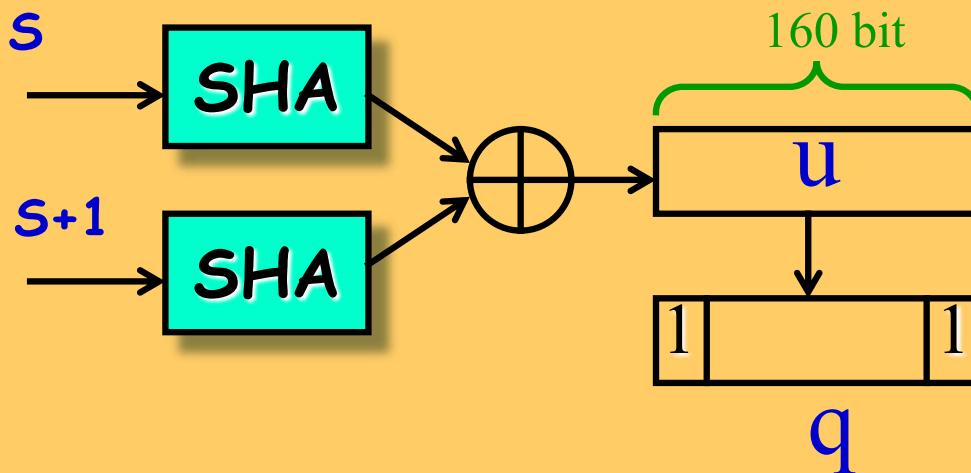
"valore casuale" è un testimone della validità dei parametri

Vediamo un esempio: scelta di  $q$

# Generazione e validazione di q

## FIPS 186-1 e 186-2

- Scegli a caso  $S$  di  $\geq 160$  bit



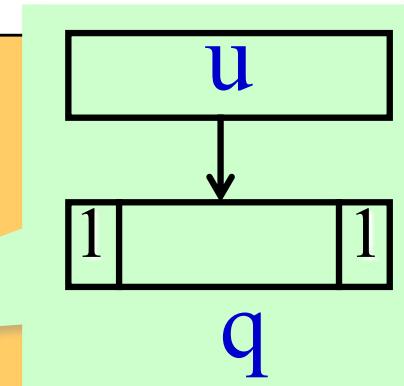
- Ripeti con un nuovo  $S$  finchè  $q$  è primo

$S$  è un testimone della validità di  $q$

# Generazione e validazione di q

## FIPS 186-3

- Scegli a caso  $S$  di  $\geq N$  bit
- $U = \text{SHA}(S) \bmod 2^{N-1}$
- $q = 2^{N-1} + U + 1 - (U \bmod 2)$
- Ripeti con un nuovo  $S$  finché  $q$  è primo



$S$  è un testimone della validità di  $q$

# Confronto tempi firme RSA e DSA

	DSA	RSA	DSA con $p, q, \alpha$ comuni
precomputazioni	14 sec		4 sec
firma	0.3 sec	15 sec	0.3 sec
verifica	16 sec	1.5 sec	10 sec
	1-5 sec Off Cards		1-3 sec Off Cards

- Implementazioni su smart card [1993]
- Computazioni Off Cards su 80386 a 33MHz

# Prestazioni implementazioni

AMD Opteron 8354 2.2GHz, Linux, Crypto++ 5.6.0 Benchmarks

- routine assembly language per aritmetica su interi

	bit chiave	firma	Firma con precomputazione	verifica
RSA	1024	1,48		0,07
DSA	1024	0,45	0,42	0,52
RSA	2048	6,05		0,16

millisecondi/operazione

esponente pubblico RSA: 17

<http://www.cryptopp.com/benchmarks.html> (marzo 2009)

# Prestazioni implementazioni

OpenSSL

openssl speed (giugno 2009)

Athlon X2 4000+ 2.8 Ghz Ubuntu

	sign	verify	sign/s	verify/s
rsa 512 bits	0.000208s	0.000013s	4808.0	79869.1
rsa 1024 bits	0.000688s	0.000030s	1453.2	32913.7
rsa 2048 bits	0.003529s	0.000091s	283.4	11026.4
rsa 4096 bits	0.020983s	0.000294s	47.7	3399.5
	sign	verify	sign/s	verify/s
dsa 512 bits	0.000135s	0.000140s	7393.3	7138.5
dsa 1024 bits	0.000299s	0.000341s	3339.4	2929.3
dsa 2048 bits	0.000863s	0.001027s	1158.6	973.8

Amd X2 6000+ 64bit Ubuntu

	sign	verify	sign/s	verify/s
rsa 512 bits	0.000201s	0.000012s	4966.7	82286.3
rsa 1024 bits	0.000650s	0.000029s	1537.6	34431.7
rsa 2048 bits	0.003313s	0.000086s	301.8	11581.0
rsa 4096 bits	0.019880s	0.000277s	50.3	3607.9
	sign	verify	sign/s	verify/s
dsa 512 bits	0.000130s	0.000134s	7692.9	7461.1
dsa 1024 bits	0.000286s	0.000331s	3502.0	3025.0
dsa 2048 bits	0.000819s	0.000973s	1221.7	1028.0

# Che parametri scegliere?

Bisogna tener conto dell'  
expected security life

Table 4: Recommended algorithms and minimum key sizes

Algorithm security lifetimes	Symmetric key algorithms (Encryption & MAC)	FFC (e.g., DSA, D-H)	IFC (e.g., RSA)	ECC e.g., ECDSA)
Through 2010 (min. of 80 bits of strength)	2TDEA <sup>23</sup>  3TDEA  AES-128  AES-192  AES-256	Min.:  $L = 1024$ ; $N = 160$	Min.:  $k = 1024$	Min.:  $f = 160$
Through 2030 (min. of 112 bits of strength)	3TDEA  AES-128  AES-192  AES-256	Min.:  $L = 2048$ $N = 224$	Min.:  $k = 2048$	Min.:  $f = 224$
Beyond 2030 (min. of 128 bits of strength)	AES-128  AES-192  AES-256	Min.:  $L = 3072$ $N = 256$	Min.:  $k = 3072$	Min.:  $f = 256$

NIST SP 800-57,  
"Recommendation for Key Management, Part 1: General (Revised)", Marzo 2007

# Che parametri scegliere?

Bisogna tener conto dell'  
*expected security life*

Esempi:

- Fatto nel 2005
- Expected security life = 5 anni →
  
- Fatto nel 2005
- Expected security life = 6 anni →

Table 4: Recommended algorithms and minimum key sizes

Algorithm security lifetimes	Symmetric key algorithms (Encryption & MAC)	FFC (e.g., DSA, D-H)	IFC (e.g., RSA)	ECC e.g., ECDSA)
Through 2010 (min. of 80 bits of strength)	2TDEA <sup>23</sup> 3TDEA AES-128 AES-192 AES-256	Min.: $L = 1024$ ; $N = 160$	Min.: $k = 1024$	Min.: $f = 160$
Through 2030 (min. of 112 bits of strength)	3TDEA AES-128 AES-192 AES-256	Min.: $L = 2048$ $N = 224$	Min.: $k = 2048$	Min.: $f = 224$
Beyond 2030 (min. of 128 bits of strength)	AES-128 AES-192 AES-256	Min.: $L = 3072$ $N = 256$	Min.: $k = 3072$	Min.: $f = 256$

NIST SP 800-57,

"Recommendation for Key Management, Part 1: General (Revised)", Marzo 2007

# Firma digitale

## alcune problematiche per l'utilizzo

- Certezza legame chiave pubblica ed utente
- Legislazione e valore legale (in Italia)
- Firme multiple e formati
- Conservazione ed utilizzo chiave privata
- Otttenere firma digitale

# Firma digitale

## alcune problematiche per l'utilizzo

- Certezza legame chiave pubblica ed utente
    - Certificati, PKI (lo vedremo in seguito)
  - Legislazione e valore legale (in Italia)
- 
- Fime multiple e formati
- 
- Conservazione ed utilizzo chiave privata
- 
- Otttenere firma digitale



# Legislazione firma digitale in Italia

## Codice dell'Amministrazione Digitale (CAD)

Decreto legislativo 7 marzo 2005 n. 82

Modifiche successive:

- Decreto legislativo 4 aprile 2006, n. 159
- Decreto legge n. 185/2008, convertito in Legge n. 2/2009
- Legge 18 giugno 2009, n. 69
- Legge 3 agosto 2009, n. 102
- Decreto legislativo 30 dicembre 2010, n. 235
- Decreto legge 21 giugno 2013 n. 69, convertito con modificazioni dalla L. 9 agosto 2013, n. 98

# Codice dell'Amministrazione Digitale

## Definizioni nell'Articolo 1

**Firma elettronica** "L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica"

**Firma elettronica avanzata** insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati.

**Firma elettronica qualificata** "la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca autenticazione informatica, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma, quale l'apparato strumentale usato per la creazione della firma elettronica"

**Firma digitale** "Un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici"

# Codice dell'Amministrazione Digitale

## Definizioni nell'Articolo 1

**Firma elettronica** "L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica"  
password, PIN, tecniche biometriche

**Firma elettronica avanzata** insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati.

Firma su tablet,  
firma grafometrica

**Firma elettronica qualificata** "la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca autenticazione informatica, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma, quale l'apparato strumentale usato per la creazione della firma elettronica"

**Firma digitale** "Un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici"

# Firma grafometrica

Firma elettronica avanzata ottenuta dal rilevamento dinamico dei dati calligrafici (ritmo, pressione, velocità, inclinazione penna,...) della firma tramite penna elettronica

Alcuni punti delle soluzioni esistenti:

Per privacy:

- Dati firma calligrafica cifrati (con chiave pubblica)
- Chiave privata presso notaio o pubblico ufficiale
- Dati non cifrati cancellati e sovrascritti



Per integrità:

- Hash (dati firma calligrafica || Hash documento)

Sicurezza postazione acquisizione



# Firma grafometrica

Firma elettronica avanzata ottenuta dal rilevamento dinamico dei dati calligrafici (ritmo, pressione, velocità, inclinazione penna,...) della firma tramite penna elettronica

Alcuni punti delle soluzioni esistenti:

Per privacy:

- Dati firma calligrafica cifrati (con chiave pubblica)
- Chiave privata presso notaio o pubblico ufficiale
- Dati non cifrati cancellati e sovrascritti



Per integrità:

- Hash (dati firma calligrafica || Hash documento)

Sicurezza postazione acquisizione



In caso di contenzioso: analisi calligrafica



# Firma grafometrica

Firma elettronica avanzata ottenuta calligrafici (ritmo, pressione, velocità tramite penna elettronica

Alcuni punti delle soluzioni esistenti:

Per privacy:

- Dati firma calligrafica cifrati (con chiave pubblica)
- Chiave privata presso notaio o pubblico ufficiale
- Dati non cifrati cancellati e sovrascritti

Per integrità:

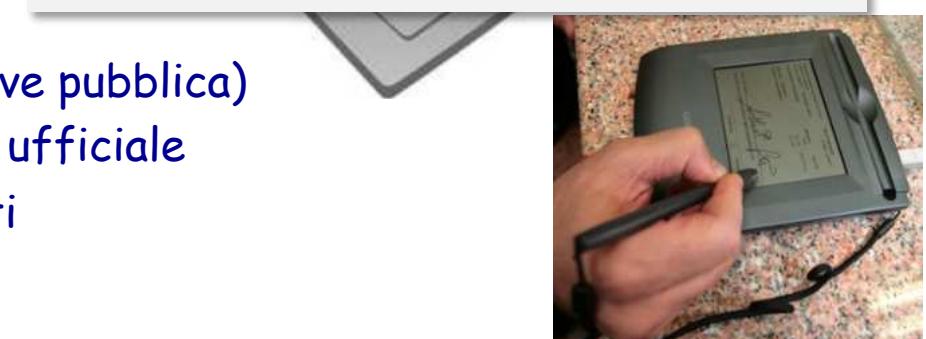
- Hash (dati firma calligrafica || Hash documento)

Sicurezza postazione acquisizione



In caso di contenzioso: analisi calligrafica

**ISO/IEC 19794-7 (2014)** specifies data interchange formats for signature/sign behavioural data captured in the form of a multi-dimensional time series using devices such as digitizing tablets or advanced pen systems.



# Codice dell'Amministrazione Digitale

## Definizioni nell'Articolo 1

**Firma elettronica** "L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica"  
password, PIN, tecniche biometriche

**Firma elettronica avanzata** insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati.  
Firma su tablet,  
firma grafometrica

**Firma elettronica qualificata** "la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca autenticazione informatica, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma, quale l'apparato strumentale usato per la creazione della firma elettronica"  
token, smart card

**Firma digitale** "Un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici"

# Valore legale firma digitale in Italia

## Firma elettronica

Riconosciuto dall'ordinamento come forma scritta  
La sua efficacia probatoria può essere liberamente  
valutata dal giudice.

## Firma elettronica avanzata

Medesima efficacia probatoria della scrittura privata  
(quella prevista dall'art. 2702 del Codice Civile,  
tranne che per i contratti immobiliari nel caso si usi  
la Firma Elettronica Avanzata).

## Firma digitale

"La scrittura privata fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritta, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa è legalmente considerata come riconosciuta"

# Regolamento eIDAS

(electronic IDentification Authentication and Signature)

## Gazzetta ufficiale L 257 dell'Unione europea



Edizione  
in lingua italiana

Legislazione

57° anno

28 agosto 2014

Sommario

I Atti legislativi

### REGOLAMENTI

- ★ Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE ..... 73

# Regolamento eIDAS

## Articolo 25 Effetti giuridici delle firme elettroniche

1. A una firma elettronica non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti per firme elettroniche qualificate.
2. Una firma elettronica qualificata ha effetti giuridici equivalenti a quelli di una firma autografa.
3. Una firma elettronica qualificata basata su un certificato qualificato rilasciato in uno Stato membro è riconosciuta quale firma elettronica qualificata in tutti gli altri Stati membri.

# Regolamento eIDAS

## Articolo 3 Definizioni

- 11) «firma elettronica avanzata», una firma elettronica che soddisfi i requisiti di cui all'articolo 26;
- 12) «firma elettronica qualificata», una firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche;

## Articolo 26 Requisiti di una firma elettronica avanzata

Una firma elettronica avanzata soddisfa i seguenti requisiti:

- a) è connessa unicamente al firmatario;
- b) è idonea a identificare il firmatario;
- c) è creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo; e
- d) è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati.

# Conservazione ed utilizzo chiave privata

- Computer
- Smart card
- Token USB



# Ottenerne firma digitale

- Certificatori
- Autorità di Registrazione
- Kit di firma
  - Smart card e lettore / token usb
  - Software per generazione firma
- Identificazione per ottenere il kit di firma
- Per la firma l'utente ha:
  - Smart card / token usb
  - PIN (Personal Identification Number)



# Software di verifica

Ultimo aggiornamento 10 Novembre 2015

La **verifica della firma digitale** e la successiva estrazione degli oggetti firmati può essere effettuata con qualsiasi software in grado di elaborare file firmati in modo conforme alla Deliberazione CNIPA 21 maggio 2009, n. 45.

I produttori dei seguenti **software** rendono disponibili per il download i propri prodotti gratuitamente:

- [Digital Signature Service](#) ↗
- [DigitalSign Reader](#) ↗
- [Firma OK!](#) ↗
- [PkNet](#) ↗
- [DIKE](#) ↗
- [Firma Certa](#) ↗
- [DSTK](#) ↗
- [View2Sign](#) ↗
- [MnlSignVerifier](#) ↗

La verifica della firma elettronica digitale può essere effettuata anche grazie ad **applicazioni** messe a disposizioni online rispettivamente da:

- [AgID](#) - applicazione DSS per la verifica di firme europee
- [AndXor](#) ↗ - verifica anche le firme PDF (PAdES) e le firme basate su certificati rilasciati da certificatori qualificati stabiliti nell'Unione Europea
- [Consiglio Nazionale del Notariato](#) ↗
- [Infocert](#) ↗ - verifica anche le firme PDF (PAdES)
- [Postecom](#) ↗
- [DigitaSign Cloud](#) ↗ - verifica anche le firme PDF (PAdES) e XAdES (XML), consente di aprire e verificare le Fatture PA con gli appropriati fogli di stile
- [Namirial](#) ↗ - verifica anche le firme PDF (PAdES) e le firme basate su certificati rilasciati da certificatori qualificati stabiliti nell'Unione Europea

<http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/firme-elettroniche/software-verifica>



Agenzia per l'Italia Digitale  
Presidenza del Consiglio dei Ministri

# Firma multiple

Firme multiple dello stesso documento?



# Formato Firma

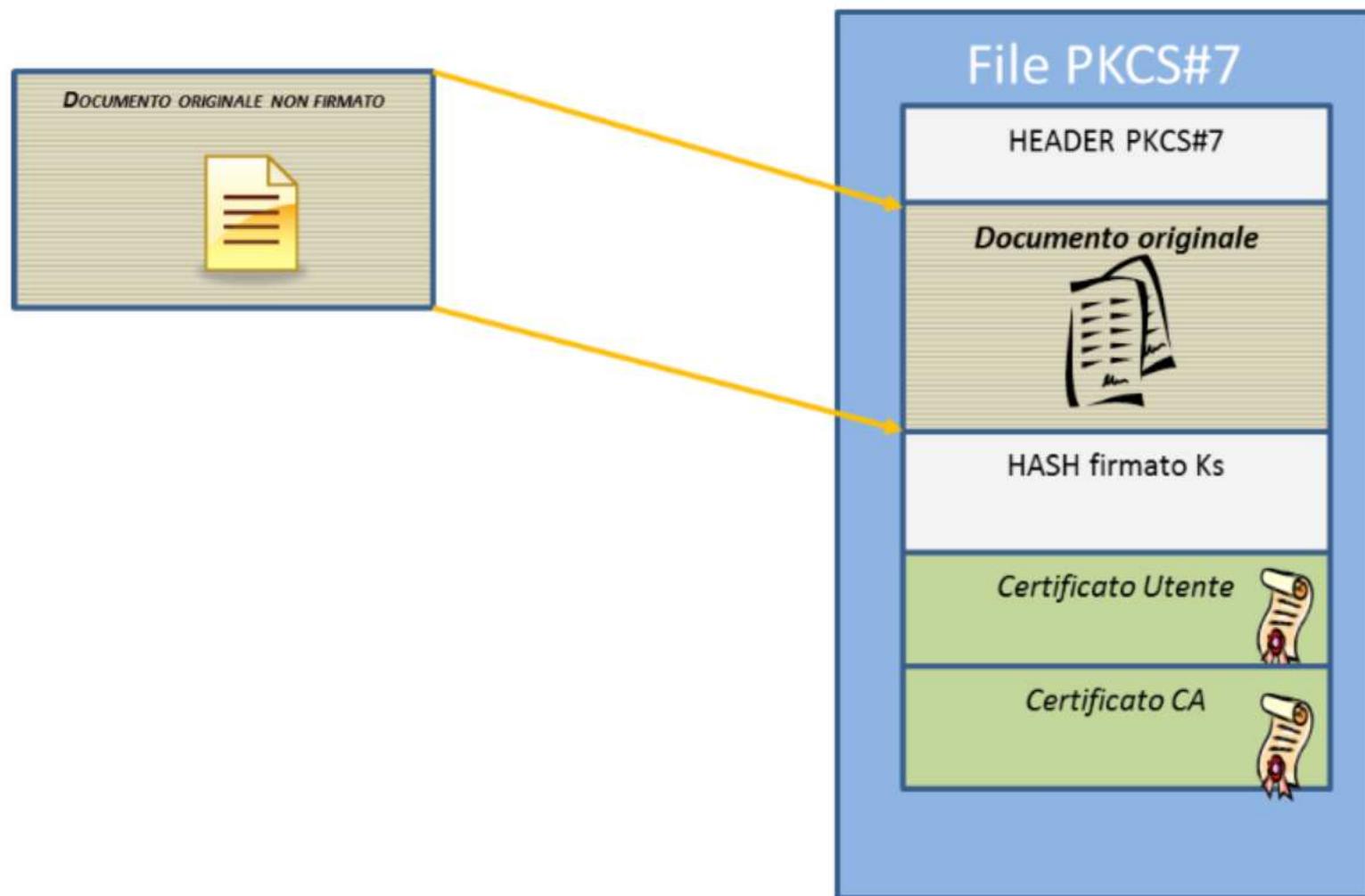
## Firma CAdES

- CMS Advanced Electronic Signatures
- Cryptographic Message Syntax
  - Standard di IETF che si basa su
  - PKCS #7 Cryptographic Message Syntax Standard
- File con estensione .p7m
- Si possono firmare file Word, Excel, OpenOffice, jpeg, gif, png, pdf, ...
- Occorre software specifico
- Non si può visualizzare il file

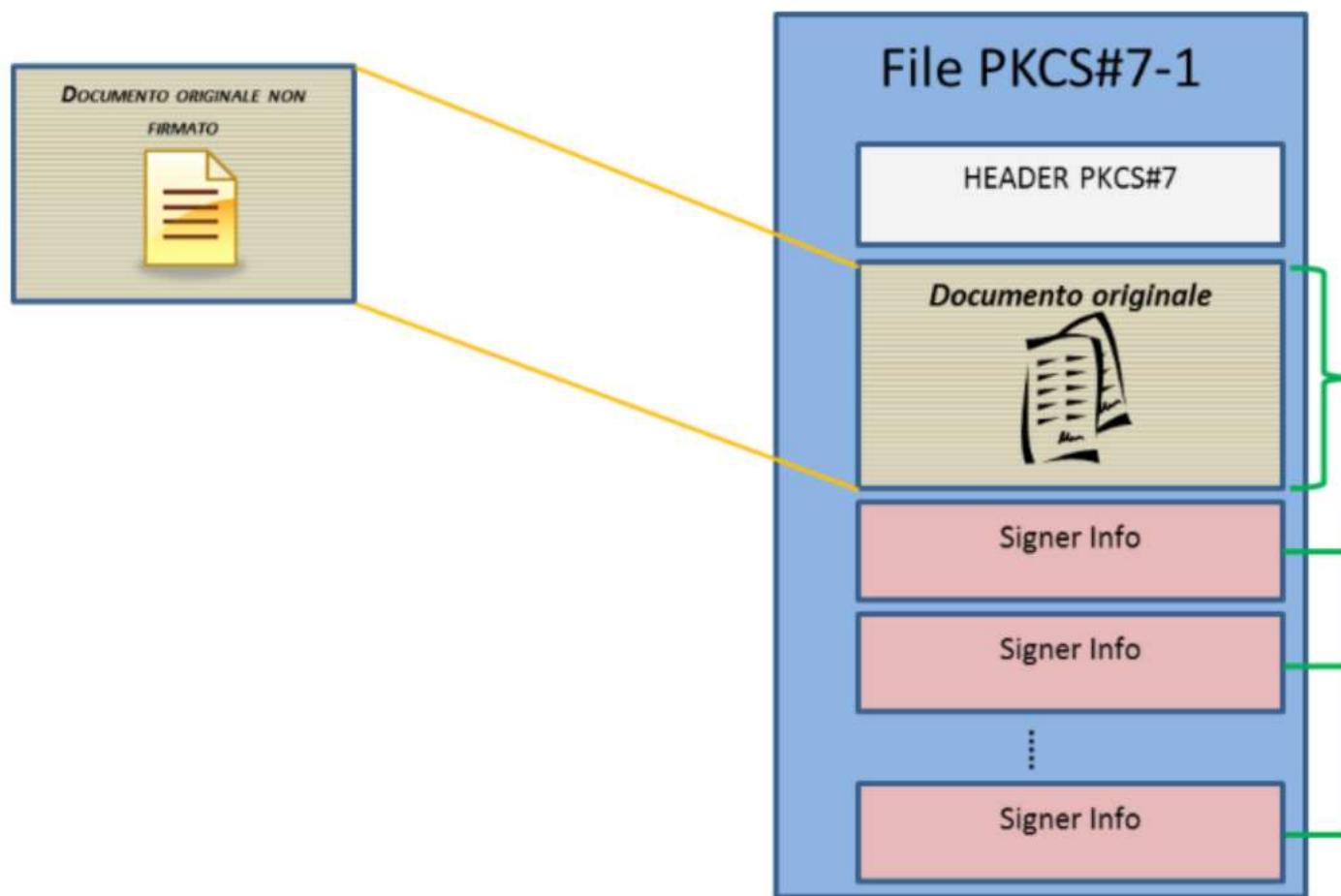
## Firma PAdES

- PDF Advanced Electronic Signatures
- ETSI TS 102 778, Standard ISO/IEC 32000
- File con estensione .pdf
- Si possono firmare solo i file pdf
- Occorre qualunque reader pdf

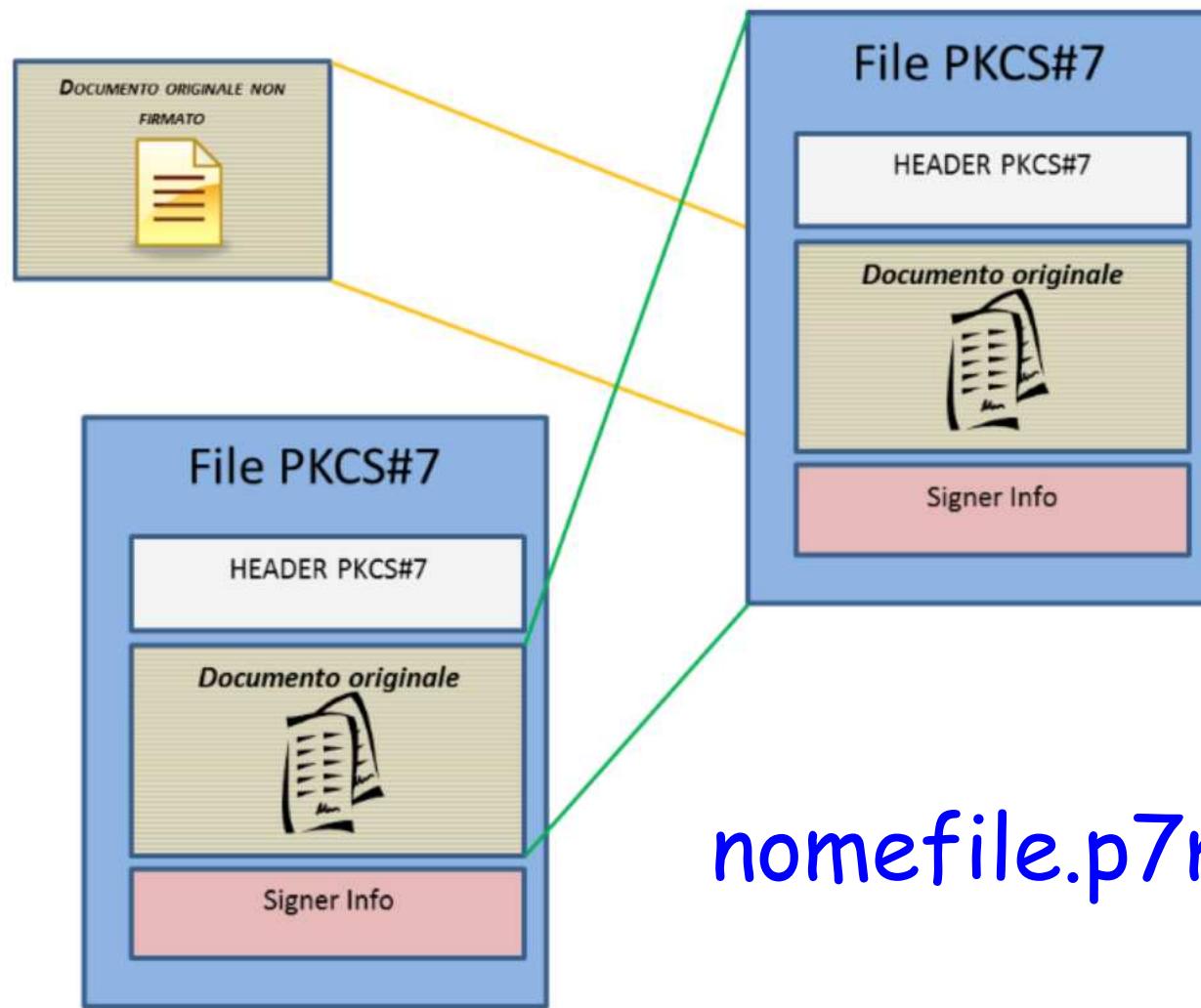
# Firma



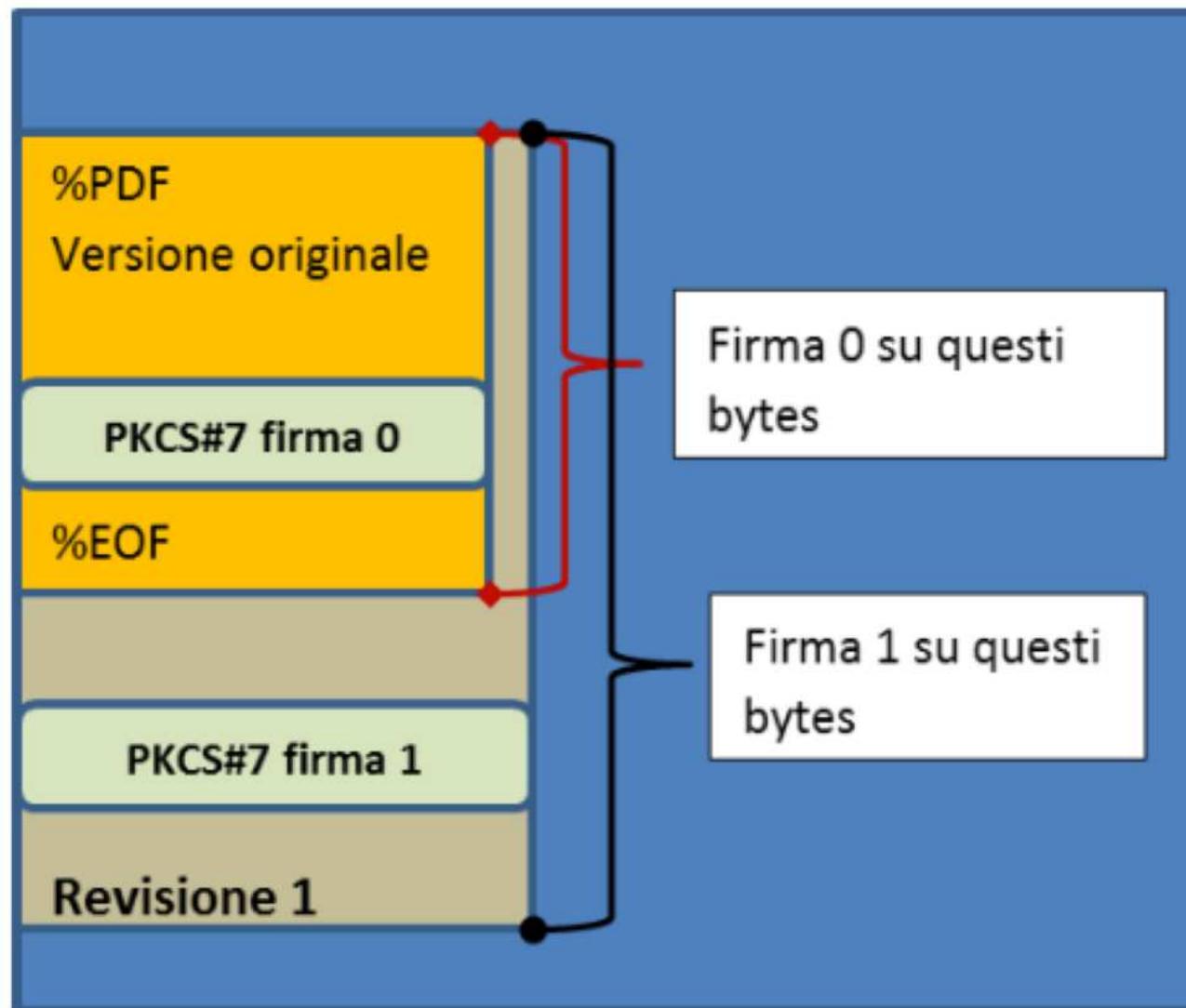
# Firme congiunte CAdES



# Firma a matriosca CAdES

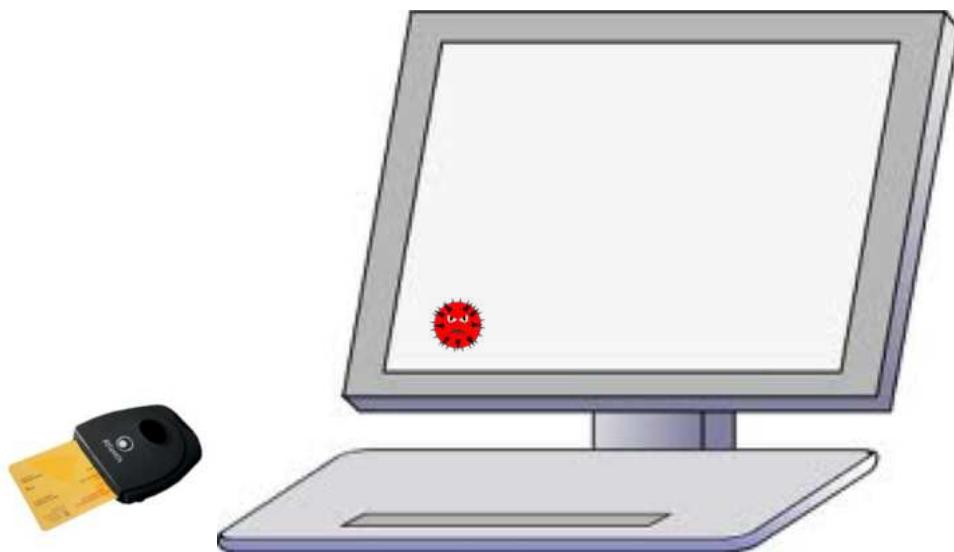


# Firme multiple PAdES



# Vulnerabilità processo firma digitale

Sicurezza piattaforma



# Vulnerabilità processo firma digitale

Documenti possono incorporare macro-istruzioni o codice eseguibile

- Esempio: Macro dei documenti Word, Javascript nei documenti PDF

Può cambiare la visualizzazione del documento

- Esempio: contratto con prezzo in base alla data (o altre variabili)



# Vulnerabilità processo firma digitale

Documenti possono incorporare macro-istruzioni o codice eseguibile

- Esempio: Macro dei documenti Word, Javascript dei documenti PDF

Può cambiare la visualizzazione del documento

- Esempio: contratto con prezzo in base alla data (o altre variabili)



Come si evita?



# Vulnerabilità processo firma digitale

Documenti possono incorporare macro-istruzioni o codice eseguibile

- Esempio: Macro dei documenti Word, Javascript dei documenti PDF

Può cambiare la visualizzazione del documento

- Esempio: contratto con prezzo in base alla data (o altre variabili)

- Utente deve verificare presenza di macro o codice eseguibile
- Restringere formati permessi (ASCII, PDF/A, immagini)

i evita?

art. 3, comma 3 del DPCM 13 gennaio 2004 "Il documento informatico sottoscritto con firma digitale o altro tipo di firma elettronica avanzata basata su un certificato qualificato e generata mediante un dispositivo sicuro per la creazione di una firma non produce gli effetti di cui all'articolo 10, comma 3, del testo unico (ora art. 21 comma 2 del Codice dell'Amministrazione Digitale) se contiene macroistruzioni o codici eseguibili, tali da attivare funzionalità che possano modificare gli atti, i fatti o i dati nello stesso rappresentati"

# Vulnerabilità processo firma digitale

Documenti possono incorporare:

- Esempio: Macro dei documenti

Può cambiare la visualizzazione

- Esempio: contratto con prezzo

## PDF/A

- A sta per Archive
- Archiviazione lungo periodo
- Assicura che il file sarà visualizzato allo stesso modo nel futuro
- Contiene tutte le info senza link
- Vietati: javascript, invocazioni a codice eseguibile, cifratura, link a contenuti esterni
- PDF/A-1 Standard ISO 19005-1:2005
- PDF/A-2 Standard ISO 19005-2:2011
- PDF/A-3 Standard ISO 19005-3:2013

- Utente deve verificare presenza di macro o codice eseguibile 😞
- Restringere formati permessi (ASCII, PDF/A, immagini)

art. 3, comma 3 del DPCM 13 gennaio 2004 "Il documento informatico sottoscritto con firma digitale o altro tipo di firma elettronica avanzata basata su un certificato qualificato e generata mediante un dispositivo sicuro per la creazione di una firma non produce gli effetti di cui all'articolo 10, comma 3, del testo unico (ora art. 21 comma 2 del Codice dell'Amministrazione Digitale) se contiene macroistruzioni o codici eseguibili, tali da attivare funzionalità che possano modificare gli atti, i fatti o i dati nello stesso rappresentati"

i evita?



# Rubano la firma digitale e si intestano l'azienda di un ignaro imprenditore: scovati dalla Guardia di Finanza

26 marzo 2012 Commenti (6)



Rubano la firma digitale e si intestano l'azienda di un ignaro imprenditore: scovati dalla Guardia di Finanza

Il Sole 24 ORE

Si procurano una copia indebita della cosiddetta «firma digitale» e, con quella, scippano letteralmente l'azienda a un piccolo imprenditore. La truffa, prima nel suo genere, in Italia, è stata scoperta dagli 007 informatici del Gat, il Nucleo speciale frodi telematiche della Guardia di finanza, impegnati nelle indagini dirette dal procuratore aggiunto di Roma, Nello Rossi, e coordinate dal sostituto procuratore Eugenio Albamonte.

## La scena del crimine

Tutto è avvenuto all'interno del sistema informatico delle Camere di Commercio. Protagonisti, un commercialista, un consulente per la sicurezza sul lavoro, una fantomatica

società intestata a un'ottuagenaria defunta da circa un anno e facente capo in realtà a un soggetto sconosciuto al fisco da almeno 16 anni. Vittima, un imprenditore (vero, almeno lui), che riteneva di essere «protetto» dalla smart card obbligatoria per le comunicazioni societarie con il registro delle Imprese.

## I capi d'accusa

Dopo perquisizioni e sequestri effettuati a Roma e provincia, i tre indagati devono ora rispondere - in concorso tra loro e con la continuazione della condotta - dei reati di sostituzione di persona, false dichiarazioni o attestazioni al certificatore di firma elettronica sull'identità o qualità personali proprie o di altri, falsità in atti pubblici, in scritture private e in documenti informatici.

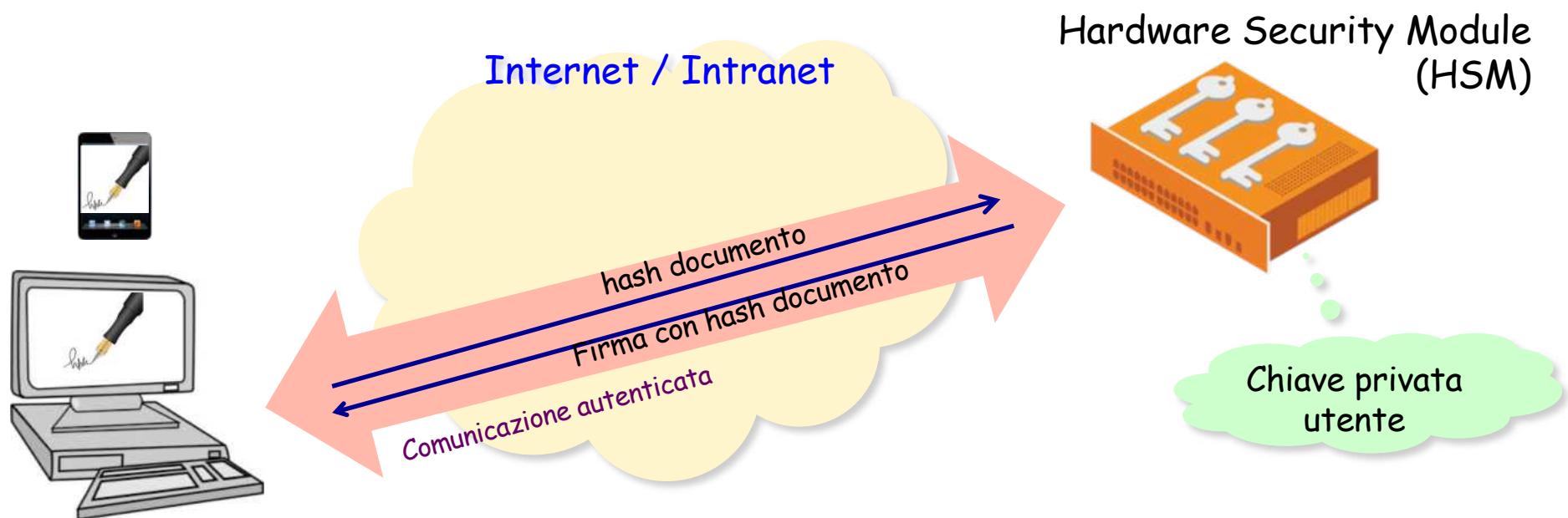
<http://www.ilsole24ore.com/art/notizie/2012-03-26/rubano-firma-digitale-intestano-181133.shtml>

# Firma digitale con smart card

## Problematiche

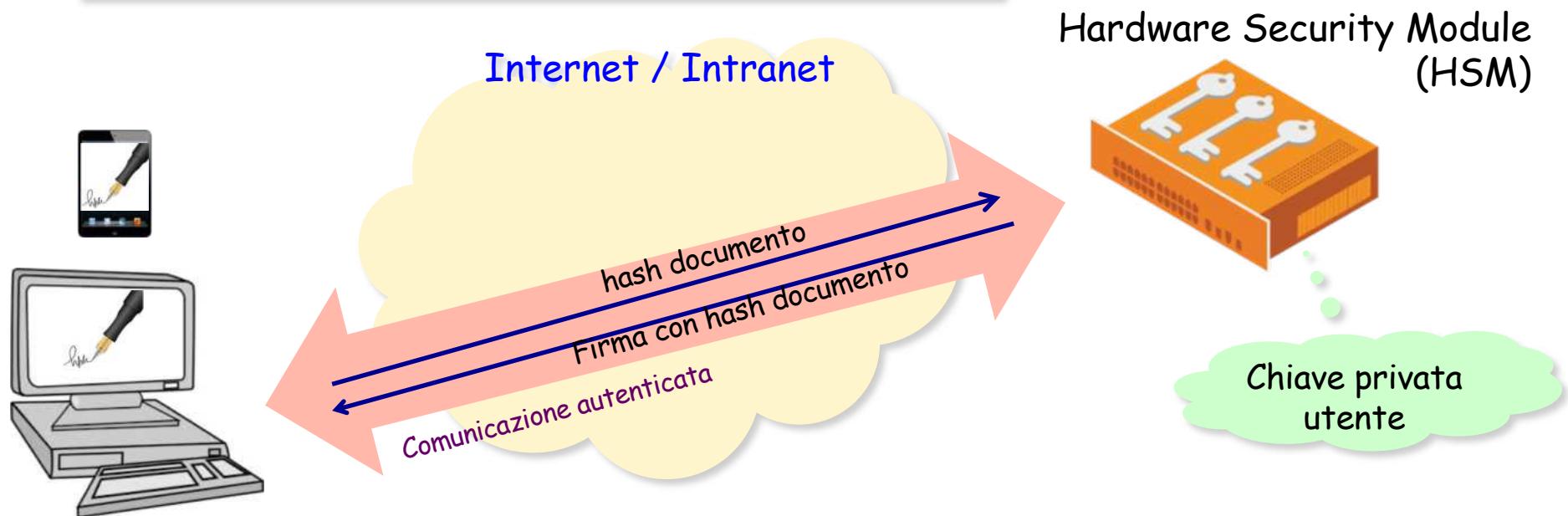
- Installare e aggiornare il software di firma
- Installare e configurare il driver del lettore di smart card
- Ripetere la procedura per ognuno dei computer utilizzati dallo stesso titolare
- Risolvere eventuali conflitti tra driver e applicazioni che richiedono un controllo esclusivo della smart card...
- Ricordarsi di avere sempre con sé non solo la smart card ma anche il lettore e/o necessari dispositivi per effettuare la firma
- Ricordarsi di gestire il rinnovo dei certificati digitali entro la data di scadenza
- Gestire la procedura di sostituzione in caso di furto, smarrimento dei vari dispositivi utilizzati

# Firma digitale remota

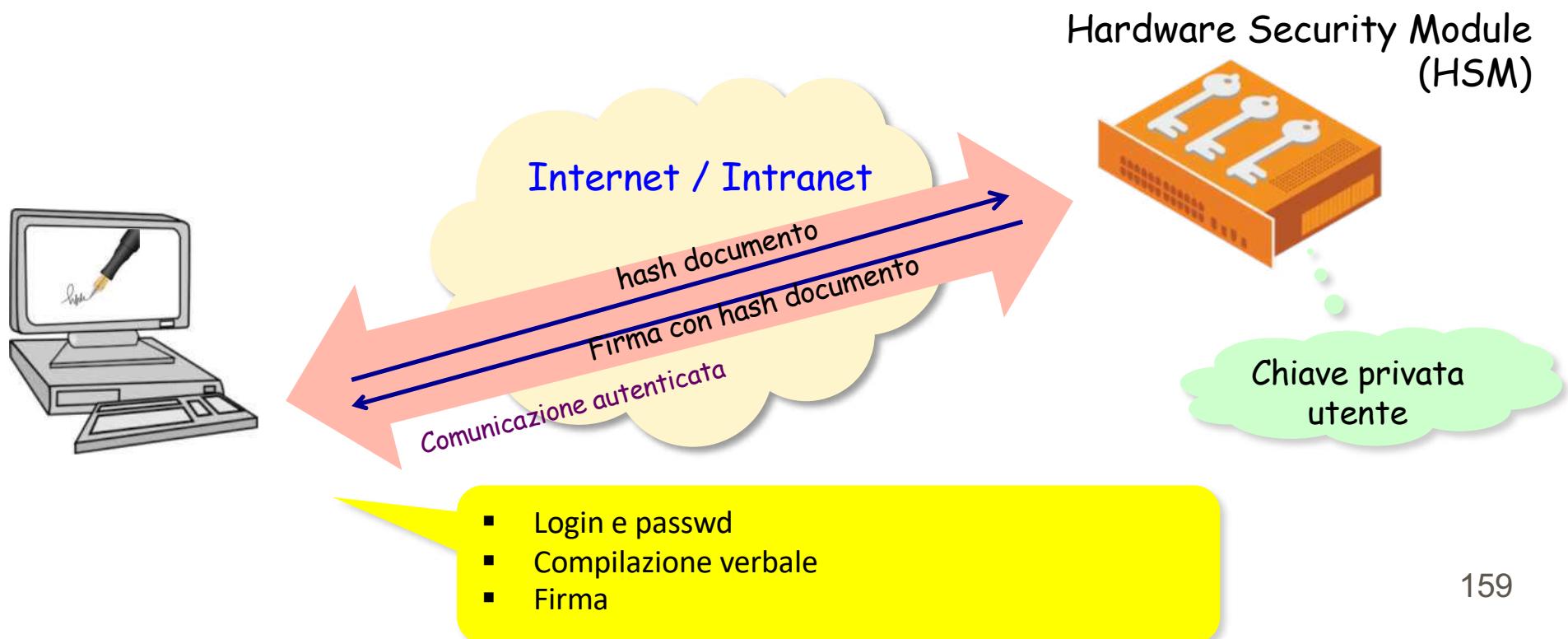


# Firma digitale remota

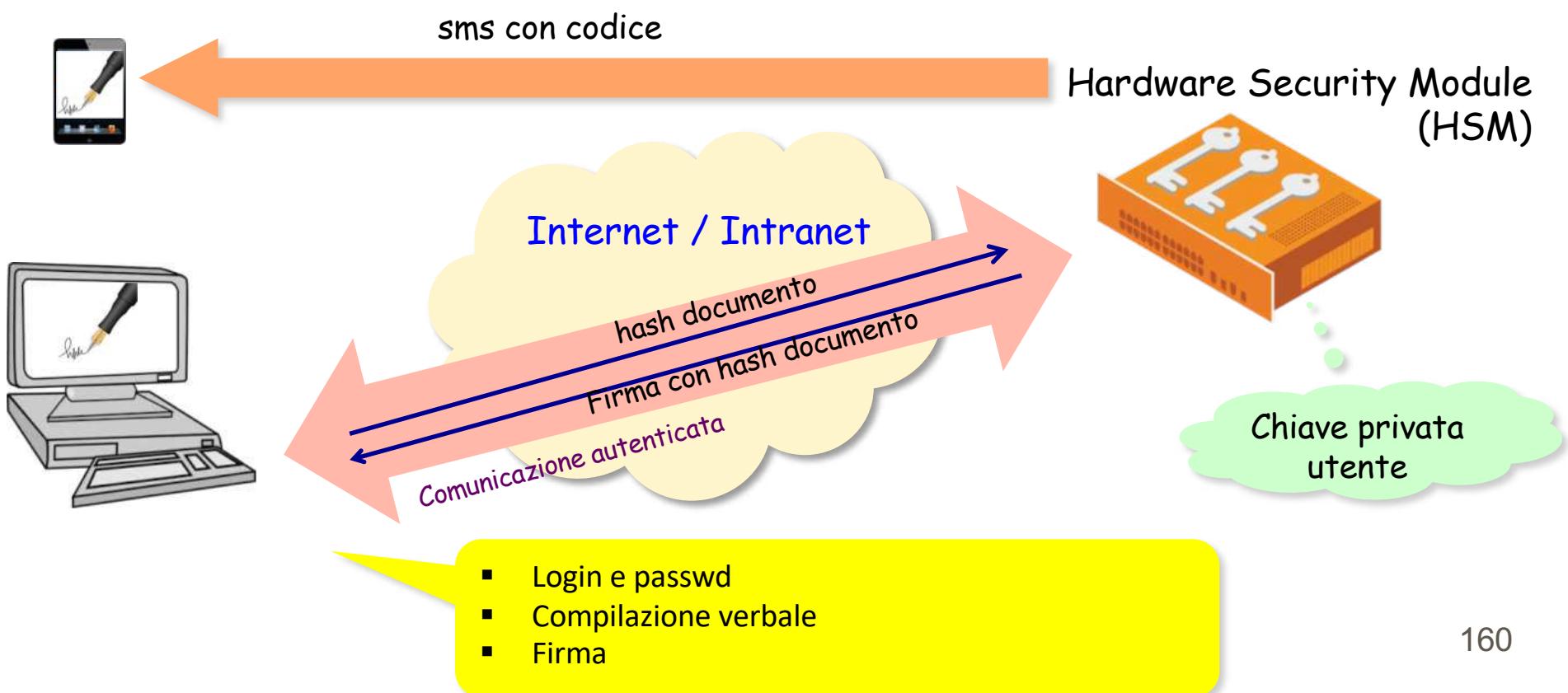
- Generazione, memorizzazione e gestione chiavi
- Protezione logica e fisica informazioni
  - Es., audit e log
- Business continuity
- High availability: messi in cluster
- Alcuni hanno anche acceleratori crittografici
  - Es., anche 7000 firme RSA 1024 bit al secondo



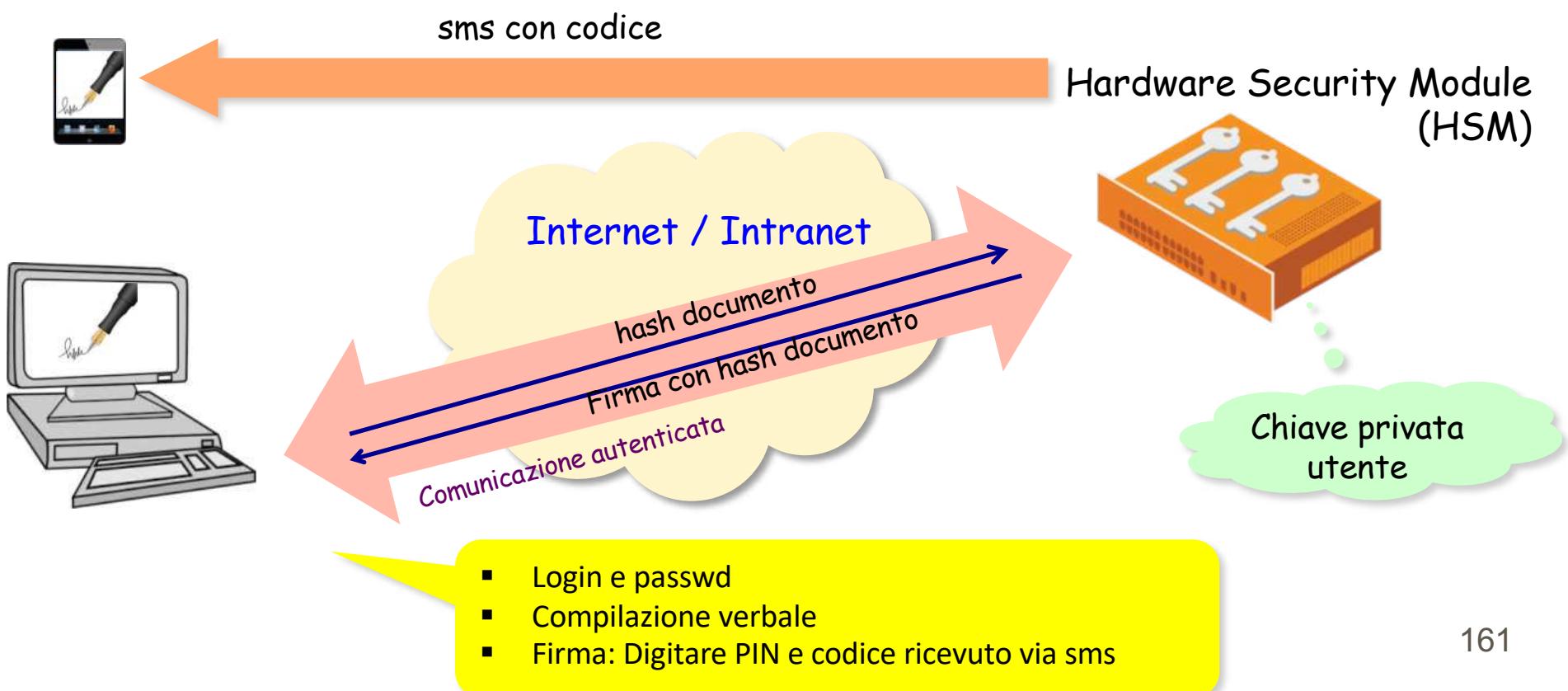
# Firma digitale esami Esse3



# Firma digitale esami Esse3



# Firma digitale esami Esse3



# Valore giuridico firma remota in Italia

Ma non era necessario che l'utente e nessun altro avesse accesso alla chiave privata?

L'HSM genera anche la coppia di chiavi!  
Chi e come gestisce l'HSM?



# Decreto del Presidente del Consiglio dei Ministri 30 marzo 2009

Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici (GU n. 129 del 6-6-2009 )

## Articolo 7

Conservazione delle chiavi e dei dati per la creazione della firma

1. E' vietata la duplicazione della chiave privata e dei dispositivi che la contengono.
2. Per fini particolari di sicurezza, è consentito che le chiavi di certificazione vengano esportate, purchè ciò avvenga con modalità tali da non ridurre il livello di sicurezza e di riservatezza delle chiavi stesse.
3. Il titolare della coppia di chiavi:
  - a)assicura la custodia del dispositivo di firma in conformità all'art. 32, comma 1, del codice, in ottemperanza alle indicazioni fornite dal certificatore;
  - b)conserva le informazioni di abilitazione all'uso della chiave privata separatamente dal dispositivo contenente la chiave;
  - c)richiede immediatamente la revoca dei certificati qualificati relativi alle chiavi contenute in dispositivi di firma difettosi o di cui abbia perduto il possesso, o qualora abbia il ragionevole dubbio che essi siano stati usati abusivamente da persone non autorizzate;
  - d)mantiene in modo esclusivo la conoscenza o la disponibilità di almeno uno dei dati per la creazione della firma.

codice  
PIN

# Decreto del Presidente del Consiglio dei Ministri

## 22 febbraio 2013

**Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, (GU n. 117 del 21-5-2013)**

### Articolo 3 Disposizioni generali

4. La firma remota ... è generata su un HSM custodito e gestito, sotto la responsabilità, dal certificatore accreditato ...

Articolo 12 Ulteriori requisiti per i dispositivi sicuri per la generazione della firma 1. La certificazione di sicurezza dei dispositivi sicuri per la creazione di una firma elettronica qualificata, anche remota o automatica, prevista dall'art. 35 del Codice è effettuata secondo criteri non inferiori a quelli previsti: a) dal livello EAL 4+ della norma ISO/IEC 15408, in conformità ai profili di protezione indicati nella decisione della Commissione europea 14 luglio 2003 e successive modificazioni; b) dal livello EAL 4+ della norma ISO/IEC 15408, in conformità ai profili di protezione o traguardi di sicurezza giudicati adeguati ai sensi dell'art. 35, commi 5 e 6 del Codice e successive modificazioni.

### Articolo 35 Piano per la sicurezza

1. Il certificatore definisce un piano per la sicurezza nel quale sono contenuti almeno i seguenti elementi: ... t) misure di sicurezza per la protezione dei dispositivi di firma remota, ivi comprese le modalità di custodia; u) limitatamente a quanto previsto all'art. 11, comma 3, modalità con cui è assicurato il controllo esclusivo delle chiavi private custodite sui dispositivi di firma remota; v) le misure procedurali e tecniche applicate per la distruzione dei dispositivi HSM e delle chiavi che contengono in caso di guasto del dispositivo HSM che non consente l'applicazione delle funzionalità di sicurezza certificate implementate dai dispositivi medesimi.

## Prestatori di servizi fiduciari attivi in Italia

Ragione sociale	Indirizzo della sede legale	Rappresentante legale	Man. oper. certificatore	Data iscrizione	Man. oper. sottoscritta AgID
<a href="#">Actualis S.p.A.</a>	Via S. Clemente, 53 - 24036 Ponte San Pietro (BG), IT	Cecconi Giorgio	<a href="#">Link</a>	28/03/2002	<a href="#">Manuali Operativi</a> Data: 11/03/2019
<a href="#">Aruba Posta Elettronica Certificata S.p.A.</a>	Via San Clemente n. 53 - 24036 Ponte San Pietro (BG)	Cecconi Giorgio	<a href="#">Link</a>	06/12/2007	<a href="#">Manuali Operativi</a> Data: 11/03/2019
<a href="#">Banca d'Italia</a>	Via Nazionale, 91 - 00184 Roma, IT	il Governatore pro tempore	<a href="#">Link</a>	23/01/2008	<a href="#">Manuali operativi</a>
<a href="#">Cedacri S.p.A. (già Cedacrinord S.p.A.)</a>	via del Conventino, 1 - 43044 Callecchia (PR), IT	Renato Dalla Riva, Presidente	<a href="#">Link</a>	15/11/2001	<a href="#">Manuali operativi</a>
<a href="#">Comando C4 Difesa - Stato Maggiore della Difesa</a>	Via Stresa, 31/B - 00135 Roma, IT	Generale B. Calogero Massara, Comandante C4 Difesa	<a href="#">Link</a>	20/09/2006	<a href="#">Manuali operativi</a>
<a href="#">Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili</a>	Piazza della Repubblica, 59 - 00185 Roma, IT	Il Presidente pro tempore	<a href="#">Link</a>	10/07/2008	<a href="#">Manuali operativi</a>
<a href="#">Consiglio Nazionale del Notariato</a>	via Flaminia, 160 - 00196 Roma, IT	Il Presidente pro tempore	<a href="#">Link</a>	12/09/2002	<a href="#">Manuali operativi</a>
<a href="#">InTeSA S.p.A.</a>	Strada Pianezza, 289 - 10151 Torino IT	Nicola Losito, Amministratore Delegato	<a href="#">Link</a>	22/03/2001	<a href="#">Manuali operativi</a>
<a href="#">InfoCert S.p.A.</a>	Piazza Sallustio, 9 - 00187 Roma, IT	Daniele Vaccarino, Presidente CdA	<a href="#">Link</a>	19/07/2007	<a href="#">Manuali operativi</a> Data: 15/02/2019
<a href="#">Intesa Sanpaolo S.p.A. (già Sanpaolo IMI S.p.A. e Banca Intesa S.p.A.)</a>	Piazza San Carlo, 156 - 10126 Torino, IT	Messina Carlo, Consigliere delegato e CEO	<a href="#">Link</a>	07/04/2004	<a href="#">Manuali operativi</a>
<a href="#">Intesi Group S.p.A.</a>	Via Torino, 4B - 20123 Milano, IT	Paolo Sironi	<a href="#">Link</a>	19/01/2018	<a href="#">Manuale operativo</a>
<a href="#">Lombardia Informatica S.p.A.</a>	via Don Minzoni, 24 - 20158 Milano, IT	Francesco Ferri, Presidente	<a href="#">Link</a>	16/12/2010	<a href="#">Manuali operativi</a>

# Prestatori di servizi fiduciari attivi in Italia

<https://www.agid.gov.it/it/piattaforme/firma-elettronica-qualificata/prestatori-di-servizi-fiduciari-attivi-in-italia>



Agenzia per l'Italia Digitale

Presidenza del Consiglio dei Ministri

<a href="#">Lottomatica Holding S.r.l.</a>	Via del Campo Boiano, 56/d 00154 - Roma	Fabio Attilio Cairoli	<a href="#">Link</a>	20/11/2018 <a href="#">Manuali operativi</a> Data: 30/11/2018
<a href="#">Namirial S.p.A.</a>	Via Caduti sul Lavoro, 4 - 60019 Senigallia (AN), IT	Davide Ceccucci, Amministratore Delegato.	<a href="#">Link</a>	03/11/2010 <a href="#">Manuali operativi</a>
<a href="#">NexiPayments S.p.A.</a>	Corsa Semiponte 55 - 20149 Milano, IT	Marco Bassilichi, Presidente	<a href="#">Link</a>	01/07/2018 <a href="#">Manuali operativi</a> Data: 01/07/2018
<a href="#">Poste Italiane S.p.A.</a>	Viale Europa, 190 - 00144 Roma IT	Matteo Del Fante	<a href="#">Link</a>	29/03/2017 <a href="#">Manuali operativi</a>
<a href="#">Telecom Italia Trust Technologies S.r.l.</a>	S.S. 148 Pontina - Km 29,100 - 00040 Pomezia (RM), IT	Salvatore Nappi, Amministratore Delegato	<a href="#">Link</a>	01/01/2014 <a href="#">Manuali operativi</a> Data: 18/03/2019
<a href="#">Zucchetti S.p.A.</a>	Via Selvettino, 1 - 26900 Lodi	Alessandro Zucchetti, Amministratore delegato	<a href="#">Link</a>	22/10/2015 <a href="#">Manuali operativi</a>

## Prestatori di servizi fiduciari cessati in Italia

Ragione sociale	Data iscrizione	Data cessazione	Certificatore sostitutivo
<a href="#">Banca di Roma S.p.A.</a>	08/09/2004	13/02/2008	nessuno
<a href="#">Banca Intesa S.p.A.</a>	08/09/2004		Intesa San Paolo S.p.A.
<a href="#">Banca Monte dei Paschi di Siena S.p.A.</a>	03/04/2008	31/08/2015	no 'Contenuto nei certificati'
<a href="#">BNL Multiservizi S.p.A.</a>	29/03/2000	30/11/2003	Actalis
<a href="#">Cedacrinord S.p.A.</a>	14/11/2001		Cedacri S.p.A.
<a href="#">Centro Tecnico per la RUPA</a>	14/03/2001		confluito nel CNIPA
<a href="#">CNIPA</a>	14/03/2001	31/08/2009	nessuno
<a href="#">Comando C4 - IEW (dal 10/04/2003 - Nuova denominazione Comando Trasmissioni e Informazioni Esercito) Comando Trasmissioni e Informazioni Esercito</a>	09/04/2003	21/09/2007	nessuno
<a href="#">Consiglio Nazionale Forense</a>	10/12/2003	01/07/2014	Nessuno 'Contenuto nei certificati'
<a href="#">Consorzio Certicomm</a>	22/06/2005	15/12/2008	CNDCEC
<a href="#">ENELIT S.p.A.</a>	16/05/2001	31/12/2004	nessuno
<a href="#">Finital S.p.A.</a>	12/04/2000	31/12/2003	nessuno
<a href="#">I.T. Telecom S.p.A. (già Saritel S.p.A.)</a>	05/02/2003	31/12/2004	I.T. Telecom S.r.l.
<a href="#">I.T. Telecom S.r.l.</a>	13/01/2005	31/12/2013	Telecom Italia Trust Technologies S.r.l. 'Contenuto nei certificati'
<a href="#">ICBPI - Istituto Centrale delle Banche Popolari Italiane S.p.A. (Cambio denominazione)</a>	17/12/2012	10/11/2017	NEXI S.p.A. 'Contenuto nei certificati'
<a href="#">Infocamere S.c.p.A.</a>	05/04/2000	15/12/2007	Infocert
<a href="#">Lombardia Integrata S.p.A. Servizi Infotelematici per il Territorio</a>	16/08/2004	21/04/2011	Lombardia Informatica S.p.A. 'Contenuto nei certificati'

# Prestatori di servizi fiduciari cessati in Italia

<https://www.agid.gov.it/it/piattaforme/firma-elettronica-qualificata/prestatori-di-servizi-fiduciari-attivi-in-italia>



Agenzia per l'Italia Digitale  
Presidenza del Consiglio dei Ministri

<a href="#">Lottomatica S.p.A. (in cessazione)</a>	26/07/2017	30/11/2018
<a href="#">NEXI S.p.A.</a>	10/11/2017	01/07/2018
<a href="#">NexiPayments S.p.A.</a>		
<a href="#">Postecom S.p.A.</a>	20/04/2000	01/04/2017
		'Contenuto nei certificati'
<a href="#">S.I.A. S.p.A.</a>	26/01/2000	01/03/2003
<a href="#">Actalis</a>		
<a href="#">Sanpaolo IMI S.p.A. (società fusa per incorporazione in Banca Intesa)</a>	07/04/2004	
<a href="#">Saritel S.p.A. (società fusa per incorporazione nella I.T. Telecom S.p.A.)</a>	19/04/2000	
<a href="#">Seceti S.p.A.</a>	05/07/2000	31/07/2003
<a href="#">Actalis</a>		
<a href="#">SOGEI S.p.A.</a>	26/02/2004	20/02/2013
		'Contenuto nei certificati'
<a href="#">SSB S.p.A.</a>	19/04/2000	01/01/2003
<a href="#">Actalis</a>		
<a href="#">Trust Italia S.p.A.</a>	06/06/2001	20/02/2008
<a href="#">Aruba PEC S.p.A.</a>		

# Common Criteria for Information Technology Security Evaluation

Standard ISO/IEC 15408 per certificazione di Computer Security

## ➤ Target Of Evaluation (TOE)

Prodotto o sistema da valutare

## ➤ Protection Profile (PP)

Documento con requisiti di sicurezza, relate ad uno scopo specifico o relate ad un caso d'uso

### ➤ Security Target (ST)

Documento con proprietà di sicurezza del target of evaluation

### ➤ Security Functional Requirements (SFRs)

Specifica funzioni di sicurezza fornite da un prodotto

### ➤ Security Assurance Requirements (SARs)

Misure prese durante sviluppo e valutazione del prodotto

# Evaluation Assurance Level

EAL1 - functionally tested

EAL2 - structurally tested

EAL3 - methodically tested and checked

EAL4 - methodically designed, tested, and reviewed

EAL5 - semiformally designed and tested

EAL6 - semiformally verified design and tested

EAL7 - formally verified design and tested

# Tamper Security (in general)

Tamper = alterazione, manomissione

- Tamper Evidence
- Tamper Detection
- Tamper Resistance

# Tamper Security

Tamper = alterazione, manomissione

## ➤ Tamper Evidence

- Unauthorized access easily detected
- having one or more indicators or barriers to entry which, if breached or missing, can reasonably be expected to provide visible evidence that tampering has occurred.
- The tamper evident feature should be designed from material not readily available to everybody. Therefore, it can't be easily duplicated.
- Example: seal, tamper sticker may be tamper indicating

## ➤ Tamper Detection

## ➤ Tamper Resistance



# Tamper Security

Tamper = alterazione, manomissione

➤ Tamper Evidence

➤ Tamper Detection

- ability of a device to sense that an active attempt to compromise the device integrity or the data associated with the device is in progress; the detection of the threat may enable the device to initiate appropriate defensive actions.
- Example: suite of sensors each specialized on a single threat type, some of which may be physical penetration, hot or cold temperature extremes, input voltage variations, input frequency variations, x-rays, and gamma rays.

➤ Tamper Resistance

# Tamper Security

Tamper = alterazione, manomissione

- Tamper Evidence
- Tamper Detection
- Tamper Resistance
  - Example: screws difficult to remove without the special matching screwdrivers



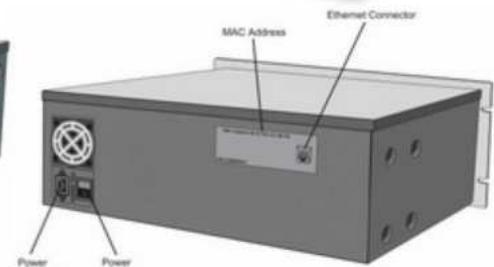
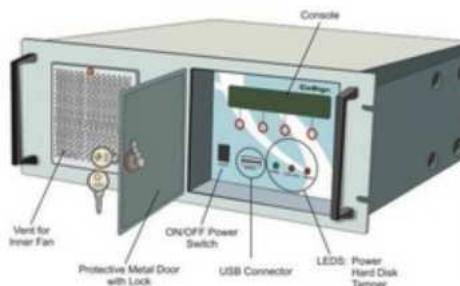
# Tamper Security in HSM



- Epoxy potting of sensitive electronics
  - Protects sensitive electronic components from impact, shock, vibration, heat, conductivity, moisture, chemicals, and visual inspection
- Multi-layered intrusion detection systems
  - Detection of mechanical penetration
  - Detection of chemical penetration
- Custom designed chassis and enclosures to prevent probing attacks
- Real-time monitoring of environmental conditions such as temperature and power

# HSM

- Generazione, memorizzazione e gestione chiavi
- Protezione logica e fisica informazioni
  - Es., audit e log
- Business continuity
- High availability: messi in cluster
- Alcuni hanno anche acceleratori crittografici
  - Es., anche 7000 firme RSA 1024 bit al secondo



# HSM accertati (maggio 2020)

**ORGANISMO**

**LABORATORI**

**ASSISTENTI**

**FORMAZIONE**

**DOCUMENTAZIONE**

**ELENCHI CERTIFICAZIONI**

**DISPOSITIVI DI FIRMA**

- Procedura di Accertamento
- Dispositivi accertati
- In corso di accertamento

**EVENTI**

**DOMANDE FREQUENTI**

**Dispositivi di firma per i quali è stato rilasciato l'Attestato di Conformità**

Sono stati rilasciati da questo Organismo Accertamenti di Conformità per i seguenti dispositivi di firma.

**QSCD**

Dispositivi per la creazione di una firma elettronica qualificata e di un sigillo elettronico qualificato accertati ai sensi del Regolamento (UE) n. 910/2014 (eIDAS).

[Espandi tutto](#) | [Chiudi tutto](#)

**nShield Connect 500+, nShield Connect 1500+, nShield Connect 6000+ (v11.72.03)**

Fornitore: nCipher Security Limited  
Data emissione attestato: 28 novembre 2019  
Attestato di Conformità: [ac\\_rda\\_eidas\\_nshield\\_2019\\_v1.0.pdf](#)  
Traguardo di Sicurezza: [st\\_ncipher\\_nshield\\_v1.1\\_public.pdf](#)

**distributed remote Qualified Signature Creation Device (drQSCD) v1.0**

Fornitore: I4P-informatikai Kft. (I4P Ltd.)  
Data emissione attestato: 25 luglio 2019  
Attestato di Conformità: [ac\\_rda\\_eidas\\_drqscd\\_10\\_v1.0.pdf](#)  
Traguardo di Sicurezza: [st\\_drqscd\\_v1.2\\_public.pdf](#)

**ADSS Server SAM Appliance v6.0**

Fornitore: Ascertia Ltd.  
Data emissione attestato: 1 luglio 2019  
Attestato di Conformità: [ac\\_rda\\_eidas\\_adss\\_sam\\_60\\_v1.0.pdf](#)  
Traguardo di Sicurezza 1: [st\\_adss\\_sam\\_60\\_v18.pdf \(SAM\)](#)  
Traguardo di Sicurezza 2: [st\\_cryptoserver\\_cp5\\_v200\\_lite.pdf \(CM\)](#)

**J-SIGN v1.8.9**

Fornitore: STMicroelectronics, S.r.l.  
Data emissione attestato: 21 gennaio 2019  
Attestato di Conformità: [ac\\_rda\\_eidas\\_jsign\\_189\\_v1.0.pdf](#)  
Traguardo di Sicurezza: [st\\_stmicro\\_jsign\\_189\\_public.pdf](#)

**SafeNet Luna® PCI-E Cryptographic Module used as an embedded device in Luna® SA**

Fornitore: SafeNet Canada, Inc.  
Data emissione attestato: 12 giugno 2018  
Attestato di Conformità: [ac\\_rda\\_eidas\\_luna\\_pcie\\_v1.0.pdf](#)  
Traguardo di Sicurezza: [st\\_safenet\\_luna\\_pcie\\_rev23.pdf](#)

**DocuSign Signature Appliance v8.4**

Fornitore: DocuSign, Inc.  
Data emissione attestato: 21 febbraio 2018  
Attestato di Conformità: [ac\\_rda\\_eidas\\_docsign\\_84\\_v1.0.pdf](#)  
Traguardo di Sicurezza: [st\\_docsign\\_84\\_v2.13.pdf](#)

**nShield Connect 500, nShield Connect 500+, nShield Connect 1500, nShield Connect 1500+, nShield Connect 6000, nShield Connect 6000+**

Fornitore: Thales e-Security  
Data emissione attestato: 5 febbraio 2018  
Attestato di Conformità: [ac\\_rda\\_eidas\\_nshield\\_v1.0.pdf](#)  
Traguardo di Sicurezza: [st\\_thales\\_nshield\\_v1.0\\_public.pdf](#)

**CoSign v8.2**

Fornitore: ARX  
Data emissione attestato: 7 febbraio 2017  
Attestato di Conformità: [ac\\_rda\\_eidas\\_cosign\\_82\\_v1.0.pdf](#)  
Traguardo di Sicurezza: [st\\_arx\\_cosign\\_82\\_v2.6.pdf](#)

**SSCD**

Dispositivi sicuri di firma accertati ai sensi della Direttiva 1999/93/CE.

**CoSign v8.2**

Fornitore: ARX  
Data emissione attestato: 12 settembre 2016  
Attestato di Conformità: [ac\\_rda\\_cosign\\_82\\_v1.0.pdf](#)  
Traguardo di Sicurezza: [st\\_arx\\_cosign\\_82\\_v2.6.pdf](#)

**nShield HSM Family v11.72.02**

Fornitore: Thales e-Security  
Data emissione attestato: 6 aprile 2016  
Attestato di Conformità: [ac\\_rda\\_nshield\\_v1.0.pdf](#)  
Traguardo di Sicurezza: [st\\_thales\\_nshield\\_v1.0\\_public.pdf](#)

**CoSign v7.5**

Fornitore: ARX  
Data emissione attestato: 6 ottobre 2015  
Attestato di Conformità: [ac\\_rda\\_cosign\\_75\\_v1.0.pdf](#)  
Traguardo di Sicurezza: [st\\_arx\\_cosign\\_75\\_v1.23.pdf](#)

**CoSign v7.1**

Fornitore: ARX  
Data emissione attestato: 30 settembre 2014  
Data revisione: 23 luglio 2015  
Attestato di Conformità: [ac\\_rda\\_cosign\\_v1.1.pdf](#)  
Traguardo di Sicurezza: [tds\\_arx\\_cosign\\_1.19.pdf](#)

**Luna® PCI Configured for Use in Luna® SA 4.5.1 (RF)**

Fornitore: SafeNet  
Data emissione attestato: 18 marzo 2014  
Attestato di Conformità: [ac\\_rda\\_safenet\\_rf\\_v1.0.pdf](#)  
Traguardo di Sicurezza: [st\\_luna\\_pci\\_cr-3636\\_5.pdf](#)

**Luna® PCI Configured for Use in Luna SA 4.1**

Fornitore: SafeNet  
Data emissione attestato: 12 dicembre 2012  
Attestato di Conformità: [ac\\_rda\\_safenet\\_v1.0.pdf](#)  
Note interpretative: [note\\_rda\\_safenet\\_v10.pdf](#)  
Traguardo di Sicurezza: [st\\_luna\\_pci\\_cr-2386\\_11.pdf](#)

<http://www.ocsi.isticom.it/index.php/dispositivi-di-firma/dispositivi-accertati>

# HSM in fase di accertamento

**OCSI**  
Organismo di Certificazione della Sicurezza Informatica



cerca nel sito...

home | contatti | cerca | mappa

**ORGANISMO**

**LABORATORI**

**ASSISTENTI**

**FORMAZIONE**

**DOCUMENTAZIONE**

**ELENCHI CERTIFICAZIONI**

**DISPOSITIVI DI FIRMA**

- **Procedura di Accertamento**
- **Dispositivi accertati**
- **In corso di accertamento**

**EVENTI**

**DOMANDE FREQUENTI**

**Dispositivi di firma in corso di Accertamento**

---

Non sono attualmente in corso presso questo Organismo processi di Accertamento di Conformità di dispositivi di firma.

<http://www.ocsi.isticom.it/index.php/dispositivi-di-firma/in-corso-di-accertamento>

# Numero firme attive in Italia

Periodo di rilevamento	Certificati qualificati di firma digitale attivi (cumulativo a fine periodo)		Numero di firme digitali remote generate nel periodo
	Totale	<i>di cui con firma remota (%)</i>	
Avvio - Mag 14	5.319.800	n.d.	n.d.
Giu 14 - Lug 15	8.104.615	55,00%	n.d.
Lug 15 - Apr 16	11.170.257	60,00%	n.d.
Mag 16 - Dic 16	14.400.872	60,00%	665.206.174
Gen 17 - Giu 17*	18.880.320	72,35%	804.513.324
Lug 17 - Dic 17	18.657.725	81,48%	1.071.865.899
Gen 18 - Giu 18	20.690.513	82,74%	971.137.425
Lug 18 - Dic 18	20.288.382	81,96%	1.034.548.974
Gen 19 - Giu 19	20.652.065	80,40%	1.429.713.138
Lug 19 - Dic 19	22.067.401	81,41%	1.681.406.616

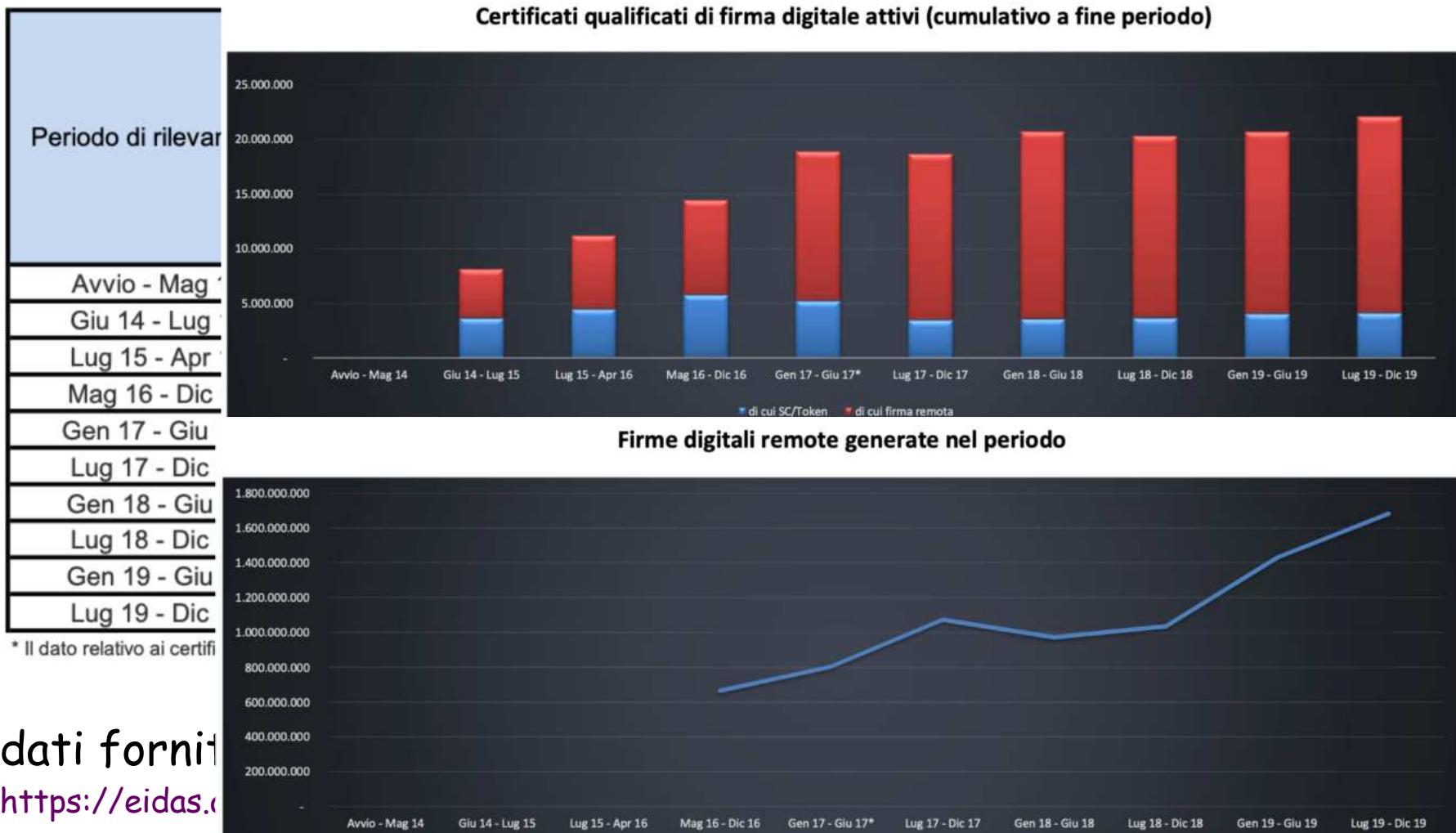
\* Il dato relativo ai certificati qualificati di firma digitale attivi si riferisce al 31 luglio 2017

dati forniti dai certificatori accreditati Agid  
<https://eidas.agid.gov.it/Statistiche/Diffusione.pdf>



Agenzia per l'Italia Digitale  
Presidenza del Consiglio dei Ministri

# Numero firme attive in Italia



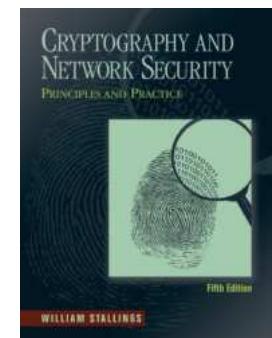
dati forniti da  
<https://eidas.eu>

# Bibliografia

## ➤ Cryptography and Network Security

by W. Stallings, 2010

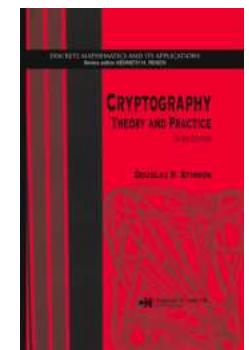
➤ cap. 13 (DSS)



## ➤ Tesina di Sicurezza su reti

➤ Firme digitali

## ➤ Cryptography: Theory and Practice, by D. Stinson (2005)



# Domande?

