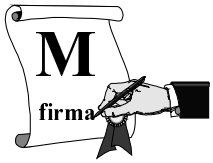
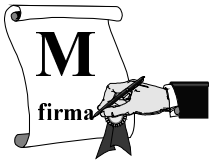
## Firma Digitale




Equivalente alla firma convenzionale



## Firma Digitale

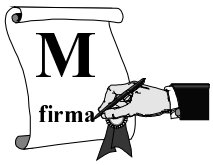



Equivalente alla firma convenzionale

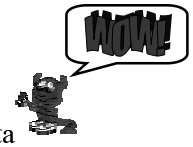
Soluzione naive:
incollare firma digitalizzata



## Firma Digitale




Equivalente alla firma convenzionale




Soluzione naive:
incollare firma digitalizzata



## Desiderata 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



## RSA

- Proposto da **R**ivest, **S**hamir, ed **A**dleman, nel 1978
- Sicurezza basata sulla difficoltà di fattorizzare



## Chiavi RSA

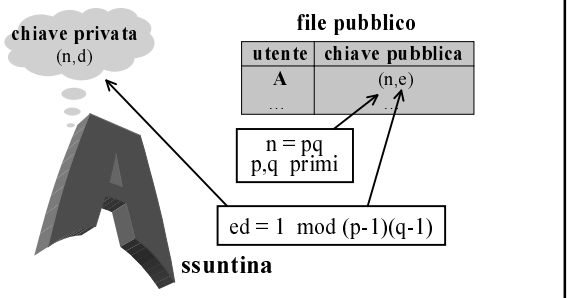
**chiave privata**
(n,d)

**ssuntina**

**file pubblico**

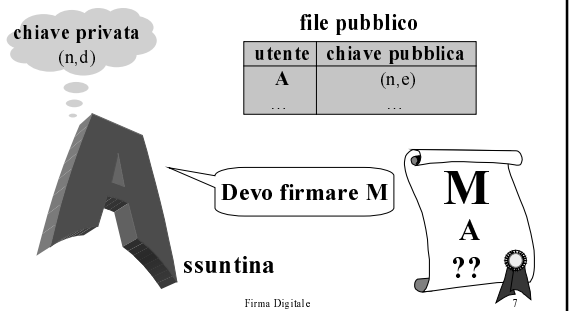
| utente | chiave pubblica |
|---|---|
| **A** | (n,e) |
| … | … |

## Chiavi RSA



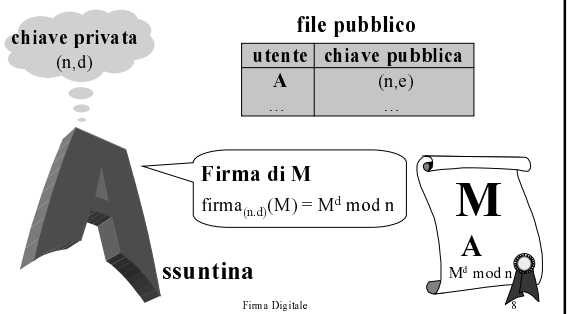

Firma Digitale 6

## Firma RSA



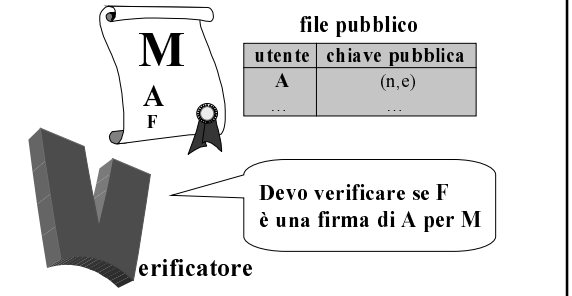

Firma Digitale 7

## Firma RSA




Firma Digitale 8

## Verifica firma RSA

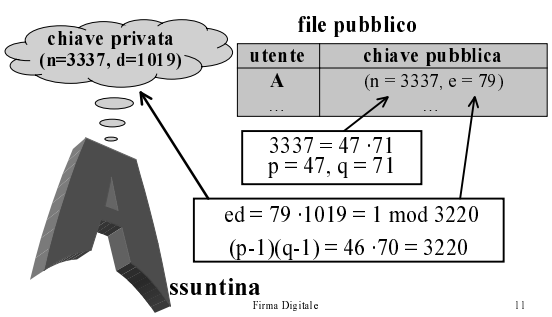



Firma Digitale 9

## Verifica firma RSA

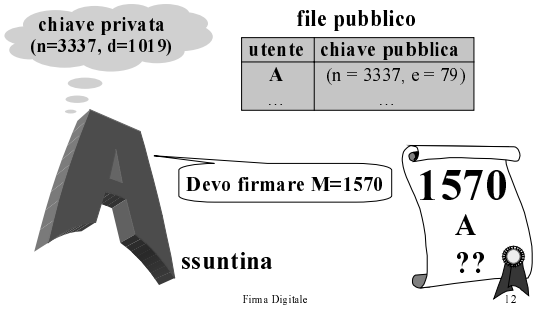

Firma Digitale 10

## "Piccolo" esempio: Chiavi RSA



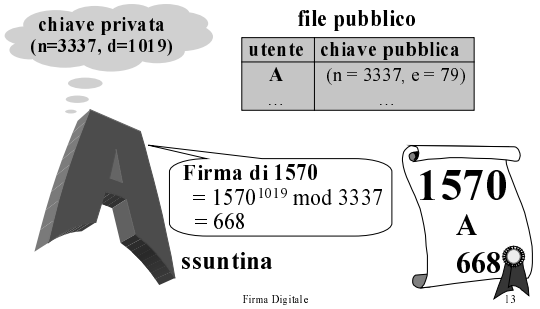

Firma Digitale 11

## "Piccolo" esempio: Firma RSA



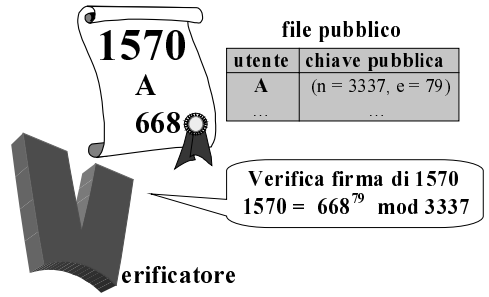



## "Piccolo" esempio: Firma RSA






## "Piccolo" esempio: Verifica firma






## Correttezza verifica firma RSA

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

$= M^{ed} \bmod n$

$= M \bmod n$

$= M$

$ed = 1 \bmod (p-1)(q-1)$

$x \in Z_n^* \Rightarrow x^{(p-1)(q-1)} = 1 \bmod n$

poichè $0 \le M < n$

**Prova per tutti gli x mediante il teorema del resto cinese**

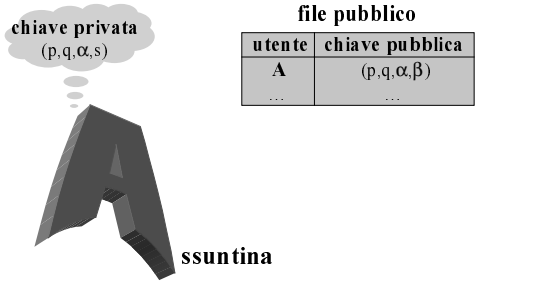


## Digital Signature Standard (DSS)

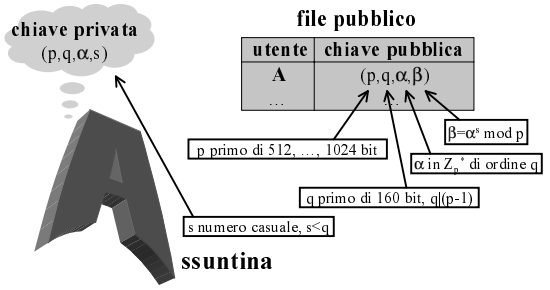
- Proposto nell'agosto del 1991 dal National Institute of Standard and Technology (NIST)
  - Digital Signature Algorithm (DSA)
  - Digital Signature Standard (DSS)
- Standard rivisto nel 1993, in risposta alle critiche
- Modifica ingegnosa dello schema di El Gamal
- Firme DSS sempre di 320 bit (buone per smart card)
- Sicurezza basata sulla difficoltà del logaritmo discreto



## Chiavi DSA

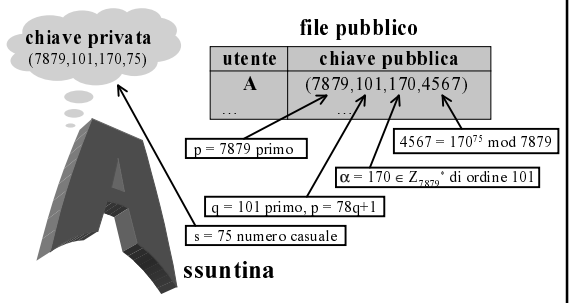


## Chiavi DSA



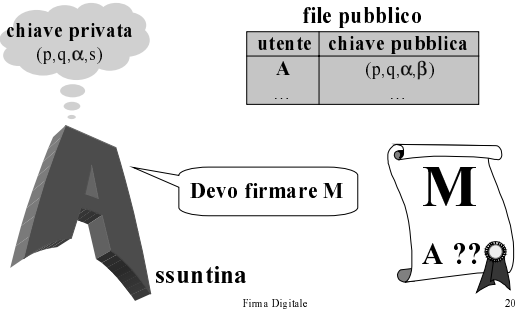

Firma Digitale 18

## Chiavi DSA ("piccolo" esempio)



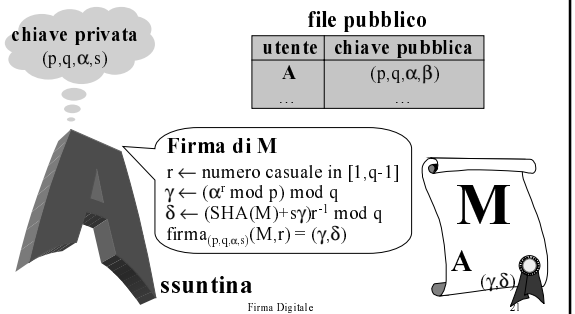

Firma Digitale 19

## Firma DSA




Firma Digitale 20

## Firma DSA

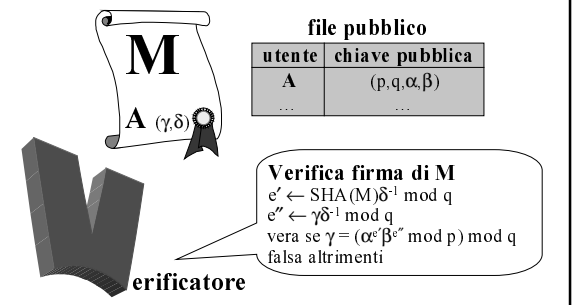



Firma Digitale 21

## Verifica firma DSA


Firma Digitale 22

## Verifica firma DSA




Firma Digitale 23

## Efficienza firma DSA

**Firma_DSA**(M,p,q,α,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 = 320 bit
- Computazioni off-line: r, $s\gamma$, $r^{-1} \bmod q$
- Computazioni on-line: SHA(M), +, ·



## Verifica firma DSA

**Verifica_firma_DSA**(M,γ,δ,p,q,α,β)
$e' \leftarrow SHA(M)\delta^{-1} \bmod q$
$e'' \leftarrow \gamma\delta^{-1} \bmod q$

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

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



## Correttezza verifica firma DSA

$(\alpha^{e'}\beta^{e''} \bmod p) \bmod q$
$e' = SHA(M)\delta^{-1} \bmod q$
$e'' = \gamma\delta^{-1} \bmod q$
$\beta = \alpha^s \bmod p$
$= (\alpha^{SHA(M)\delta^{-1} \bmod q}\ \alpha^{s\gamma\delta^{-1} \bmod q} \bmod p) \bmod q$
$\alpha$ è di ordine q
$= (\alpha^{SHA(M)\delta^{-1}+s\gamma\delta^{-1}} \bmod p) \bmod q$
$\delta^{-1}(SHA(M)+s\gamma) = r \bmod q$
$= (\alpha^r \bmod p) \bmod q$
$= \gamma$



## Generazione di p e q

Scegli p
Scegli q di 160 bit tale che q|(p-1)



## Generazione di p e q

Scegli p
Scegli q di 160 bit tale che q|(p-1)



## Generazione di p e q

- Scegli un primo q di 160 bit
- Scegli un primo p di 512/1024 bit tale che q|(p-1)
  - Scegli X di 512 bit (oppure … 1024 bit)
  - $p \leftarrow X - ((X \bmod 2q)-1)$ 2q|(p-1)
  - se p è primo e $p \geq 2^{511}$ esci altrimenti riprova

## Scelta di un elemento di ordine q

- Ordine di $\alpha \in Z_n^*$ = il più piccolo intero positivo r tale che $\alpha^r = 1 \bmod n$
- p,q primi tali che $q|(p-1)$

**Scegli_ordineq** (p,q)
1. g ← elemento scelto a caso in $Z_p^*$
2. $\alpha \leftarrow g^{(p-1)/q} \bmod p$
3. **if** $\alpha \neq 1$ **then return** $\alpha$ **else** go to **1.**



## Correttezza di Scegli_ordineq

**Scegli_ordineq** (p,q)
1. g ← elemento scelto a caso in $Z_p^*$
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

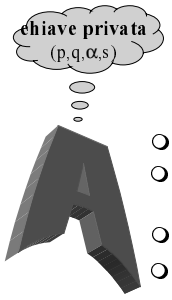


## Probabilità successo singola iterazione

- Se g è un generatore allora $g^{(p-1)/q} \neq 1 \bmod p$
- Probabilità successo ≥ Probabilità che g è generatore $> 1/(6\ln\ln(p-1))$
- Numero medio di iterazioni $< 6\ln\ln(p-1)$
- Esempio: 512 bit $6\ln\ln(2^{512}) \approx 35{,}23$
  1024 bit $6\ln\ln(2^{1024}) \approx 39{,}38$



## Chiavi globali ed individuali



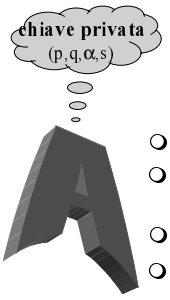

**file pubblico**

| utente | chiave pubblica |
|---|---|
| A | (p,q,α,β) |
| … | … |

- **Sicurezza basata sul valore privato s**
- **I valori p,q,α possono essere gli stessi per un gruppo di utenti**
- **Un'autorità sceglie p,q,α**
- **Il singolo utente sceglie solo s,β**



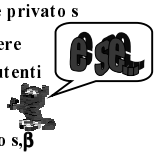
## Chiavi globali ed individuali




**file pubblico**

| utente | chiave pubblica |
|---|---|
| A | (p,q,α,β) |
| … | … |

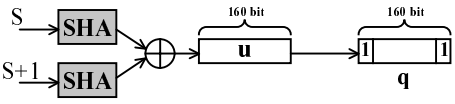
- **Sicurezza basata sul valore privato s**
- **I valori p,q,α possono essere gli stessi per un gruppo di utenti**
- **Un'autorità sceglie p,q,α**
- **Il singolo utente sceglie solo s,β**





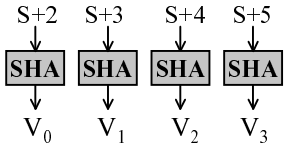
## Generazione di q

- Scegli a caso S di ≥160 bit



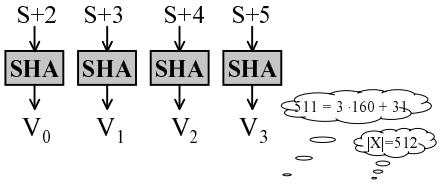

- Scegli un nuovo S finchè q è primo
- S è un testimone della validità di q

## Generazione di p (512 bit)





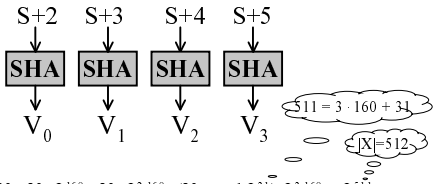

## Generazione di p (512 bit)




$X \leftarrow V_0+V_1 \cdot 2^{160}+ V_2 \cdot 2^{2 \cdot 160}+(V_3 \bmod 2^{31}) \cdot 2^{3 \cdot 160}+2^{511}$



## Generazione di p (512 bit)



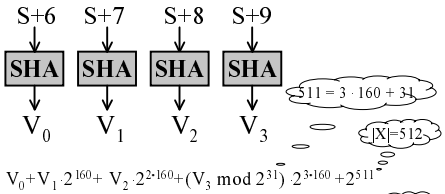

$X \leftarrow V_0+V_1 \cdot 2^{160}+ V_2 \cdot 2^{2 \cdot 160}+(V_3 \bmod 2^{31}) \cdot 2^{3 \cdot 160}+2^{511}$

$p \leftarrow X - ((X \bmod 2q)-1)$ 2q|(p-1)

se p è primo e $p \geq 2^{511}$ esci altrimenti …



## Generazione di p (512 bit)




$X \leftarrow V_0+V_1 \cdot 2^{160}+ V_2 \cdot 2^{2 \cdot 160}+(V_3 \bmod 2^{31}) \cdot 2^{3 \cdot 160}+2^{511}$

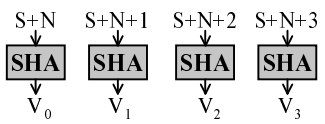
$p \leftarrow X - ((X \bmod 2q)-1)$ 2q|(p-1)

se p è primo e $p \geq 2^{511}$ esci altrimenti …



## Generazione di p (512 bit)

N←2




$X \leftarrow V_0+V_1 \cdot 2^{160}+ V_2 \cdot 2^{2 \cdot 160}+(V_3 \bmod 2^{31}) \cdot 2^{3 \cdot 160}+2^{511}$

$p \leftarrow X - ((X \bmod 2q)-1)$ 2q|(p-1)

se p è primo e $p \geq 2^{511}$ allora esci S,(N-2)/4 sono testimoni

altrimenti N←N+4 e ripeti (per ≤4096 volte) numero iterazioni



## Generazione di p e q

```
Seleziona_pq(L)
(1) Computa interi n e b tali che L-1=160n+b
(2) repeat
(3)     repeat
(4)         S ← sequenza casuale di almeno 160 bit
(5)         g ← |S|
(6)         U ← SHA(S)⊕ SHA((S+1) mod 2^g)
(7)         Forma q da U ponendo il MSB ed il LSB ad 1
(8)     until q primo
(9)     C ← 0
(10)    N ← 2
(11)    repeat
(12)        for k=0 to n do V_k ← SHA(S+N+k) mod 2^g
(13)        W ← V_0+V_1·2^160+...+V_n-1·2^160(n-1)+(V_n mod 2^b)·2^160n
(14)        X ← W+2^L-1
(15)        p ← X-((X mod 2q)-1)
(16)    until (p primo) or (p<2^L-1)
(17)    if p<2^L-1
(18)        then C ← C+1
(19)           N ← N+n+1
(20)           if C<4096 then goto step (12)
(21)                     else Help ← falso
(22)        else Help ← vero
(23) until Help
(24) return p,q,S,C
```

## Confronto tempi firme RSA e DSA

| | DSS | RSA | DSS con p,q,a 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 eseguite su 80386 a 33MHz



## Certificati

- **Certificato**: struttura dati composta da
  - dati (in chiaro): almeno una chiave pubblica ed una stringa identificativa (subject entity)
  - firma di una autorità che *lega* chiave e identità


- **Autorità di Certificazione**: Terza parte fidata la cui firma *garantisce* il legame tra chiave ed identità
- Esempi di altri dati di un certificato:
  - periodo di validità chiave pubblica
  - numero seriale o identificatore chiave
  - info addizionali su subject entity (ad es., indirizzo fisico o rete)
  - info addizionali su chiave (ad es., algoritmi ed utilizzo)
  - stato della chiave pubblica (revoca certificati)



## Revoca Certificati

- **Data scadenza dentro un certificato**
- **Notifica manuale**
- **File pubblico di chiavi revocate**
  - **Certificate Revocation List** (CRL)
- **Certificato di revoca**



## Certificate Revocation List (CRL)

- Lista firmata da CA contenenti i numeri seriali dei certificati emessi revocati (ma non ancora scaduti), quando è avvenuta la revoca, ed altro (per es., motivi)
  - la data della CRL indica quanto sia aggiornata
- **Distribuzione CRL**:
  - modello **pull**: download da CA quando necessario
  - modello **push**: CA la invia ad intervalli regolari
  - approccio **ibrido**: CA la invia a repository intermediari da cui il verificatore fa il download quando necessario



## Certificati X.509

Definiti nel 1988 ITU-T recommendation, ISO/IEC 9594-8
- modificati nel 1993 (versione 2)
- estensioni aggiunte nel 1995 (versione 3)
  - identificatori chiave, uso chiave, policy, attributi…

Standard X.509 supportato da molti protocolli (PKCS, SSL)

**Campi di un certificato X.509**

1. version
2. serial number
3. signature algorithm ID
4. issuer name
5. validity period
6. subject name
7. subject public key information
8. issuer unique identifier (ver 2,3)
9. subject unique identifier (ver 2,3)
10. extensions (ver 3)
11. firma dei precedenti campi



## Legislazione italiana

Legge 15 marzo 1997 n. 59 "Bassanini 1" art. 15 comma 2: *gli atti, i dati e i documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici e telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici e telematici, sono validi e rilevanti ad ogni effetto di legge*

Regolamento attuativo DPR 513/97, G.U. n° 60 13/3/1998

Regolamento tecnico *"Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici..."* Decreto del Presidente del Consiglio dei Ministri, G.U. n° 87 del 15/4/1999


Regolamento Tecnico
I. Regole di base
RSA, DSS, chiave ≥1024 bit, SHA-1, RIPEMD-160
II. Regole per la certificazione delle chiavi
III. Regole per la validazione temporale e per la protezione dei documenti informatici
IV. Regole tecniche per le Pubbliche Amministrazioni
V. Disposizioni finali
Firma Digitale
48