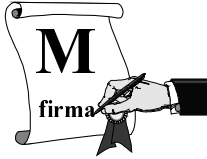


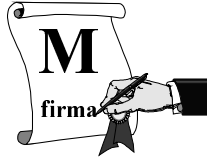
Firma Digitale



Equivalente alla firma
convenzionale

Firma Digitale 0

Firma Digitale




Equivalente alla firma
convenzionale


Soluzione naive:
incollare firma digitalizzata

Firma Digitale 1

Firma Digitale



Equivalente alla firma
convenzionale



Soluzione naive:
incollare firma digitalizzata

Firma Digitale 2

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 

Firma Digitale 3

RSA

- Proposto da Rivest,
Shamir, ed Adleman, nel 1978
- Sicurezza basata sulla
difficoltà di fattorizzare




Firma Digitale 4

Chiavi RSA

chiave privata
(n,d)

file pubblico	
utente	chiave pubblica
A	(n,e)
...	...



ssuntina

Firma Digitale 5

Chiavi RSA

chiave privata (n,d)

file pubblico

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

$n = pq$
p,q primi

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

ssuntina

Firma Digitale 6

Firma RSA

chiave privata (n,d)

file pubblico

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

Devo firmare M

ssuntina

M
A
??

Firma Digitale 7

Firma RSA

chiave privata (n,d)

file pubblico

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

Firma di M
 $\text{firma}_{(n,d)}(M) = M^d \pmod n$

ssuntina

M
A
 $M^d \pmod n$

Firma Digitale 8

Verifica firma RSA

file pubblico

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

Devo verificare se F è una firma di A per M

erificatore

Firma Digitale 9

Verifica firma RSA

file pubblico

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

Verifica firma di M
vera se $M = F^e \pmod n$
falsa altrimenti

erificatore

Firma Digitale 10

“Piccolo” esempio: Chiavi RSA

chiave privata (n=3337, d=1019)

file pubblico

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

$3337 = 47 \cdot 71$
p = 47, q = 71

$ed = 79 \cdot 1019 = 1 \pmod{3220}$
 $(p-1)(q-1) = 46 \cdot 70 = 3220$

ssuntina

Firma Digitale 11

“Piccolo” esempio: Firma RSA

chiave privata (n=3337, d=1019)

file pubblico	
utente	chiave pubblica
A	(n = 3337, e = 79)
...	...

Devo firmare M=1570

1570
A
??

ssuntina

Firma Digitale 12

“Piccolo” esempio: Firma RSA

chiave privata (n=3337, d=1019)

file pubblico	
utente	chiave pubblica
A	(n = 3337, e = 79)
...	...

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

1570
A
668

ssuntina

Firma Digitale 13

“Piccolo” esempio: Verifica firma

file pubblico	
utente	chiave pubblica
A	(n = 3337, e = 79)
...	...

1570
A
668

Verifica firma di 1570
 $1570 = 668^{79} \bmod 3337$

erificatore

Firma Digitale 14

Correttezza verifica firma RSA

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

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

$$= M \bmod n$$

$$= M$$

$ed = 1 \bmod (p-1)(q-1)$
 $x \in \mathbb{Z}_n^* \Rightarrow x^{(p-1)(q-1)} = 1 \bmod n$

poichè $0 \leq M < n$

Prova per tutti gli x mediante il teorema del resto cinese

Firma Digitale 15

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

Firma Digitale 16

Chiavi DSA

chiave privata (p, q, α, s)

file pubblico	
utente	chiave pubblica
A	(p, q, α, β)
...	...

ssuntina

Firma Digitale 17

Chiavi DSA

chiave privata (p,q,α,s)

file pubblico	
utente	chiave pubblica
A	(p,q,α,β)
...	...

p primo di 512, ..., 1024 bit
 q primo di 160 bit, q|(p-1)
 α in Z_{p-1}^* di ordine q
 β = α^s mod p
 s numero casuale, s < q

ssuntina

Firma Digitale 18

Chiavi DSA ("piccolo" esempio)

chiave privata (7879,101,170,75)

file pubblico	
utente	chiave pubblica
A	(7879,101,170,4567)
...	...

p = 7879 primo
 q = 101 primo, p = 78q + 1
 α = 170 ∈ Z_{7879}^* di ordine 101
 4567 = 170⁷⁵ mod 7879
 s = 75 numero casuale

ssuntina

Firma Digitale 19

Firma DSA

chiave privata (p,q,α,s)

file pubblico	
utente	chiave pubblica
A	(p,q,α,β)
...	...

Devo firmare M

M

A ??

ssuntina

Firma Digitale 20

Firma DSA

chiave privata (p,q,α,s)

file pubblico	
utente	chiave pubblica
A	(p,q,α,β)
...	...

Firma di M
 $r \leftarrow$ numero casuale in $[1, q-1]$
 $\gamma \leftarrow (\alpha^r \text{ mod } p) \text{ mod } q$
 $\delta \leftarrow (\text{SHA}(M) + s\gamma)r^{-1} \text{ mod } q$
 $\text{firma}_{(p,q,\alpha,s)}(M,r) = (\gamma,\delta)$

M

A (γ,δ)

ssuntina

Firma Digitale 21

Verifica firma DSA

M

file pubblico	
utente	chiave pubblica
A	(p,q,α,β)
...	...

A (γ,δ)

Devo verificare se (γ,δ) è una firma di A per M

erificatore

Firma Digitale 22

Verifica firma DSA

M

file pubblico	
utente	chiave pubblica
A	(p,q,α,β)
...	...

A (γ,δ)

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

erificatore

Firma Digitale 23

Efficienza firma DSA

Firma_DSA(M,p,q,α,s)
 $r \leftarrow$ numero casuale in $[1,q-1]$
 $\gamma \leftarrow (\alpha^r \text{ mod } p) \text{ mod } q$
 $\delta \leftarrow (\text{SHA}(M)+s\gamma)r^{-1} \text{ mod } q$
output firma_(p,q,α,s)(M,r) = (γ,δ)

- Lunghezza firma = 320 bit
- Computazioni off-line: r, sγ, r⁻¹ mod q
- Computazioni on-line: SHA(M), +, ·

Firma Digitale 24

Verifica firma DSA

Verifica_firma_DSA(M,γ,δ,p,q,α,β)
 $e' \leftarrow \text{SHA}(M)\delta^{-1} \text{ mod } q$
 $e'' \leftarrow \gamma\delta^{-1} \text{ mod } q$
 $\text{ver}_{(p,q,\alpha,\beta)}(M,\gamma,\delta) = \begin{cases} \text{vera} & \text{se } \gamma = (\alpha^{e'}\beta^{e''} \text{ mod } p) \text{ mod } q \\ \text{falsa} & \text{altrimenti} \end{cases}$
Output ver_(p,q,α,β)(M,γ,δ)

Firma Digitale 25

Correttezza verifica firma DSA

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

Firma Digitale 26


Generazione di p e q

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

Firma Digitale 27

Generazione di p e q

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



Firma Digitale 28

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)
 - ★ $p \leftarrow X - ((X \text{ mod } 2q) - 1)$ ○ ○ ○ $2q|(p-1)$
 - ★ se p è primo e $p \geq 2^{511}$ esci altrimenti riprova

Firma Digitale 29

Scelta di un elemento di ordine q

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

Scegli_ordineq (p,q)

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

Firma Digitale 30

Correttezza di Scegli_ordineq

Scegli_ordineq (p,q)

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

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

dal Teorema di Lagrange l'ordine di α divide q
Firma Digitale 31

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 $> 1/(6 \ln(p-1))$
- Numero medio di iterazioni $< 6 \ln(p-1)$

Esempio: 512 bit $6 \ln(2^{512}) \approx 35,23$
 1024 bit $6 \ln(2^{1024}) \approx 39,38$

Firma Digitale 32

Chiavi globali ed individuali

chiave privata
(p,q,α,s)

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

Firma Digitale 33

Chiavi globali ed individuali

chiave privata
(p,q,α,s)

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

Firma Digitale 34

Generazione di q

- Scegli a caso S di ≥ 160 bit

```

            S → [SHA] → ⊕ → [160 bit] → [160 bit]
            S+1 → [SHA] → ⊕ → [160 bit] → [160 bit]
            (The XOR result is labeled 'u', and the final result is labeled 'q')
        
```

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

Firma Digitale 35

Generazione di p (512 bit)

$S+2 \rightarrow \text{SHA} \rightarrow V_0$
 $S+3 \rightarrow \text{SHA} \rightarrow V_1$
 $S+4 \rightarrow \text{SHA} \rightarrow V_2$
 $S+5 \rightarrow \text{SHA} \rightarrow V_3$

Firma Digitale 36

Generazione di p (512 bit)

$S+2 \rightarrow \text{SHA} \rightarrow V_0$
 $S+3 \rightarrow \text{SHA} \rightarrow V_1$
 $S+4 \rightarrow \text{SHA} \rightarrow V_2$
 $S+5 \rightarrow \text{SHA} \rightarrow V_3$

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

Firma Digitale 37

Generazione di p (512 bit)

$S+2 \rightarrow \text{SHA} \rightarrow V_0$
 $S+3 \rightarrow \text{SHA} \rightarrow V_1$
 $S+4 \rightarrow \text{SHA} \rightarrow V_2$
 $S+5 \rightarrow \text{SHA} \rightarrow V_3$

$X \leftarrow V_0 + V_1 \cdot 2^{160} + V_2 \cdot 2^{2 \cdot 160} + (V_3 \bmod 2^{31}) \cdot 2^{3 \cdot 160} + 2^{511}$
 $p \leftarrow X - ((X \bmod 2q) - 1)$
 se p è primo e $p \geq 2^{511}$ esci altrimenti ...

Firma Digitale 38

Generazione di p (512 bit)

$S+6 \rightarrow \text{SHA} \rightarrow V_0$
 $S+7 \rightarrow \text{SHA} \rightarrow V_1$
 $S+8 \rightarrow \text{SHA} \rightarrow V_2$
 $S+9 \rightarrow \text{SHA} \rightarrow V_3$

$X \leftarrow V_0 + V_1 \cdot 2^{160} + V_2 \cdot 2^{2 \cdot 160} + (V_3 \bmod 2^{31}) \cdot 2^{3 \cdot 160} + 2^{511}$
 $p \leftarrow X - ((X \bmod 2q) - 1)$
 se p è primo e $p \geq 2^{511}$ esci altrimenti ...

Firma Digitale 39

Generazione di p (512 bit)

$N \leftarrow 2$

$S+N \rightarrow \text{SHA} \rightarrow V_0$
 $S+N+1 \rightarrow \text{SHA} \rightarrow V_1$
 $S+N+2 \rightarrow \text{SHA} \rightarrow V_2$
 $S+N+3 \rightarrow \text{SHA} \rightarrow V_3$

$X \leftarrow V_0 + V_1 \cdot 2^{160} + V_2 \cdot 2^{2 \cdot 160} + (V_3 \bmod 2^{31}) \cdot 2^{3 \cdot 160} + 2^{511}$
 $p \leftarrow X - ((X \bmod 2q) - 1)$
 se p è primo e $p \geq 2^{511}$ allora esci $S_i(N-2)/4$ sono testimoni
 altrimenti $N \leftarrow N+4$ e ripeti (per ≤ 4096 volte) numero iterazioni

Firma Digitale 40

Generazione di p e q

```

Selezione 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 29)
(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 Vk ← SHA(S+n+k) mod 29
(13)    W ← V0+V1·2160+...+Vn-1·2160(n-1)+(Vn mod 2b)·2160n
(14)    X ← W+2511
(15)    p ← X-((X mod 2q)-1)
(16)  until (p primo) or (p < 2511)
(17)  if p < 2511
(18)    then C ← C+1
(19)         N ← N+n+1
(20)         if C < 4096 then goto step (12)
(21)         else Help ← falso
(22)  until Help
(23)  return p,q,S,C
    
```

Firma Digitale 41

Confronto tempi firme RSA e DSA

	DSA	RSA	DSA 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

Firma Digitale 42

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)

Firma Digitale 43

Revoca Certificati

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

Firma Digitale 44

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

Firma Digitale 45

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

Firma Digitale 46

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

Firma Digitale 47



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