Firma digitale
Profili tecnici

Prof. ing. Pierluigi Ridolfi

- **Un po' di storia**
  - Metodi simmetrici (DES)
- **Sistemi sicuri**
  - Metodi asimmetrici (RSA)
- **Riservatezza, autenticità, integrità**
- **Certificazione**
- **Procedimento di Firma**
- **Sistemi a doppia cifratura**

Bibliografia

- Berardi, Beutelspacher: "Crittologia", F.Angeli 1996
- Ridolfi "Firma digitale e sicurezza informatica", F.Angeli 1998
- Giustozzi, Monti, Zimuel: "Crittografia: storia, tecniche, aspetti giuridici", Apogeo 1999
- Singh: "Codici & segreti", Rizzoli 2001
- Ferragina, Luccio: "Crittografia", Bollati Boringhieri 2001

Scritture segrete

Hanno lo scopo di riservare solo al destinatario la facoltà di comprendere il significato di un messaggio.

- **Steganografia**

  occultamento del messaggio

- **Crittografia**

  trasformazione del messaggio in un *criptogramma*

Steganografia

- Scritture simpatiche
- Microfotografie
- Palline cinesi
- Metodo di Istieo
- Scitala spartana

La scìtala spartana (1)

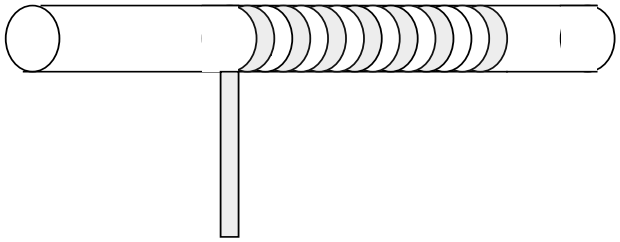
Plutarco nella *Vite parallele* scrive che gli efori (i magistrati di Sparta) inviarono a Lisandro una ***scìtala*** con l'ordine di tornare in patria. E spiega: "La scitala consiste in questo. Gli efori, all'atto di spedire all'estero un generale, prendono due pezzi di legno rotondi e perfettamente uguali, sia in lunghezza sia in larghezza, di dimensioni cioè corrispondenti. Di questi pezzi di legno, che si chiamano scitale, uno lo conservano loro, l'altro lo consegnano al partente. In seguito, allorché vogliono comunicare qualche cosa di grande importanza e che nessuno altro deve sapere, tagliano un rotolo di papiro lungo e stretto come una cinghia e l'avvolgono attorno alla scitala in loro possesso, coprendone tutt'intorno la superficie del legno col papiro, senza lasciare il minimo interstizio.

La scìtala spartana (2)

Compiuta questa operazione, scrivono sul papiro così come si trova disteso sulla scitala ciò che vogliono, e una volta scritto, tolgono il papiro e glielo mandano senza il bastone. Il generale, quando lo riceve, non può leggere le lettere di seguito, poiché non hanno alcun legame tra loro e rimangono sconnesse, finché anch'egli non prende la sua scitala e vi avvolge in giro la striscia di papiro. Così la spirale torna a disporsi nel medesimo ordine in cui fu scritta, e le lettere si allineano via via, di modo che l'occhio può seguire la lettura attorno al bastone e ritrovare il senso compiuto del messaggio. La striscia di papiro è chiamata scitala al pari del legno".

Schema della scìtala

Un messaggio scritto longitudinalmente diventa illeggibile sulla cinghia svolta



Terminologia

+ **Crittografia**

  messaggio $\Leftrightarrow$ *crittogramma*

  ◊ Codifica / Decodifica

  ◊ Cifratura / Decifrazione

+ **Crittoanalisi**

  crittogramma $\Rightarrow$ *? messaggio*

  ◊ Decrittazione

= **Crittologia**

Crittografia

Metodi di trasposizione:

- Metodo di Cesare
- Metodo di Ballaso

Metodi di sostituzione:

- Codice (livello parole)
- Cifra (livello lettere)

Metodo di Cesare (1)

Svetonio nella *Vita del Divo Giulio*:

"… se vi era qualche questione riservata egli usava scrivere in cifra, e questa cifra consisteva in una disposizione apparentemente caotica delle lettere, sicché era impossibile ricostruire la parola originale. Chi voglia scoprirne il senso e decifrarla sappia che bisogna sostituire a ogni lettera la terza che segue nell'alfabeto; vale a dire dove è scritto A bisogna leggere D e così di seguito."

Metodo di Cesare (2)

1 2 3 4 5 6 7 8 9 10 11 12 ..

A B C D E F G H I L M N ..

Per cifrare: chiave = 2

CADE ⇒ ECFG

Per decifrare: chiave = -2

Metodo di Bellaso

Chiave	**P**	**I**	**S**	**A**
	N	E	L	*
Testo in	M	E	Z	Z
chiaro	O	*	D	E
	L	*	C	A
	M	M	I	N

Testo cifrato

*ZEAN EE**M NMOLM LZDCI

Metodi di sostituzione

- **Mediante codici**
  - sistemi basati su nomenclature:

    Elenchi di parole (o frasi) ognuna codificata con numeri.

    Primi nomenclatori: a. 1326; molto sviluppati nei secoli successivi, da soli o in associazione con altri metodi.

    es. *5 = comprare, 6 = vendere*
  - sistemi basati su frasi:

    es. "*I lunghi singhiozzi dei violini d'autunno*" ⇒ sbarco in Normandia
- **Mediante cifra**
  - corrispondenza diretta
  - corrispondenza indiretta

Cifratura mediante corrispondenza diretta (1)

alfabeto chiaro e alfabeto cifrante

A B C D E F G H I L M …

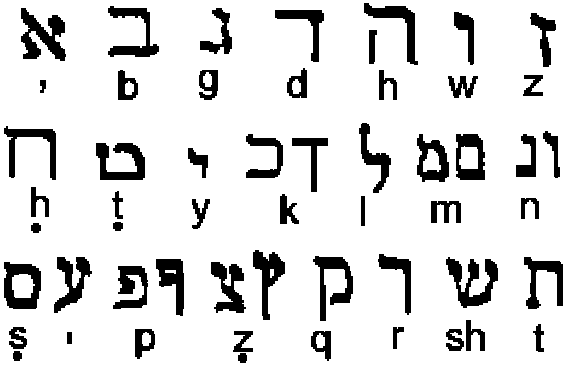
C I R U G Z V S T B N …

CADE ⇒ RCUG

Per decifrare: procedimento inverso.

Cifratura mediante corrispondenza diretta (2)

L'**Atbash**: un caso particolare con alfabeto invertito.



La prima lettera dell'alfabeto ebraico, *aleph*, viene sostituita con l'ultima, *taw*, e la seconda, *beth*, con la penultima, *shin*. Da qui il nome Atbash.

Nella Bibbia, Geremia, 25:
"… il re di *Sesac*"; si tratta invece del re di *Babel*.

Cifratura mediante corrispondenza diretta (3)

Variante Vernam (1917):

sostituzione con numeri
e aggiunta di una chiave

```
A  B  C  D  E  F  G  H …
1  2  3  4  5  6  7  8 …

es.:          C A D E
              3 1 4 5
chiave:       6 7 8 9
cifrato:      9 8 2 4
```

Per decifrare: procedimento inverso.

Limiti

- Difficile ricordare gli alfabeti cifranti:

  $\Rightarrow$ metodi generativi

- "Facile" da decrittare:

  $\Rightarrow$ crittoanalisi

- Sicurezza dipendente dalla segretezza della chiave.

Metodi per generare un alfabeto cifrante

- Si prende una "frase chiave".

  es: `sempre caro mi fu quest'ermo colle`

- Si eliminano spazi e lettere ripetute.

  es: `semprcaoifuqtl`

- Si affianca la stringa risultante all'alfabeto chiaro a partire da una certa posizione (*es. la 6*) e si riempiono quelle mancanti con le lettere rimaste.

  es:
  ```
  abcdefghilmnopqrstuvz
        semprcaoifuqtl
  ghnvz               bd
  ```

Metodi per scegliere la chiave

- Si prende come riferimento un'*opera* già pubblicata.
- Si trasmette o si concorda preventivamente come "pre-chiave" un certo numero *n.*
- Si assume come chiave la prima frase che appare nell'*opera* alla pagina *n.*

Crittoanalisi

- Tecniche per ricostruire il "messaggio" dato il solo crittogramma.
- Nel caso del metodo della corrispondenza diretta si può utilizzare la frequenza delle lettere.
- al-Kindi (IX sec.): "Sulla decifrazione dei messaggi criptati".
- Caso letterario:
  E.A. Poe: "Lo scarabeo d'oro".

Frequenze delle lettere nella lingua italiana

lettera	frequenza
A	11,7
B	0,9
C	4,5
D	3,7
E	11,8
F	0,9
G	1,6
H	1,5
I	11,3
L	6,5
M	2,5

lettera	frequenza
N	6,9
O	9,8
P	3,0
Q	0,5
R	6,4
S	5,0
T	5,6
U	3,0
V	2,1
Z	0,5

N.B.: le frequenze dipendono dal contesto.

Artifici per ostacolare la crittoanalisi

- **Inserire lettere inesistenti**
  *es: ne?l ^mez?z^o *de?l^*
- **Inserire errori ortografici**
  es: nelmezo del gamin
- **Usare codifica plurima per la stessa lettera**
  es. 12 modi diversi per codificare la a, in modo da "uniformare" le frequenze di tutte le lettere
- **Passare dalla cifratura alla parziale codifica**
  es: Ω = *oggi*, Δ = *domani*
- **Utilizzare più di un alfabeto**

Metodi basati su più di un alfabeto (1)

- **Metodo di Leon B. Alberti**
  - 2 alfabeti cifranti usati alternativamente.

```
abcdefghilmnopqrstuvz
zvustrqponmlihgfedcba
mlihgfedcbazvustrqpon
```

es: ROMA ⇒ FVMM

Metodi basati su più di un alfabeto (2)

- **Metodo di Vegenère**
  - 26 alfabeti in chiaro sfalsati, con chiave; si cifra ogni lettera in progressione con l'alfabeto relativo alla corrispondente lettera della chiave.

```
abcdefghilmnopqrstuvz
bcdefghilmnopqrstuvza
cdefghilmnopqrstuvzab
defghilmnopqrstuvzabc
efghilmnopqrstuvzabcd
```

es: chiave = *cade*

ROMA ⇒ TOPE

Cifratura mediante corrispondenza indiretta

Un'estensione del metodo di Vegenère

	A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**L**	**M**
indice											
A	C	I	R	U	G	Z	V	S	T	B	N
B	S	T	U	V	B	C	N	I	R	Z	G
C	R	Z	G	S	C	T	U	B	N	I	V
D	……										
R	T	B	N	I	V	R	Z	G	S	C	U
Z	……										

Chiave = ***ABRACADABRA***
Messaggio = BACCA
Codifica = I S NRR

Per decifrare: procedimento inverso.

Metodi "misti"

Trasposizione e sostituzione

- ADFGVX
- Macchine cifranti
  - Enigma

Metodo ADFGVX (1)

Metodo adottato in Germania nel 1918.

Qualunque messaggio viene tradotto in una sequenza delle lettere ADFGVX, poi trasmessa per telegrafo.

Le 6 lettere scelte sono quelle che meno facilmente si possono confondere tra loro con il codice Morse.

A . –	D – . .	F . . – .
G – – .	V . . . –	X – . . –

Metodo ADFGVX (2)

1a fase: sostituzione.

	A	**D**	**F**	**G**	**V**	**X**
A	p	g	1	4	m	e
D	f	5	j	b	z	8
F	2	l	q	o	d	t
G	h	a	v	7	s	k
V	u	9	x	c	i	y
X	0	n	r	w	3	6

Messaggio: 2 m a r z o

Crittogramma parziale: FA AV GD XF DV FG

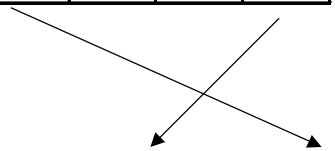
Metodo ADFGVX (3)

2a fase: trasposizione.

Crittogramma parziale: FA AV GD XF DV FG

Chiave: P I S A

P	**I**	**S**	**A**
F	A	A	V
G	D	X	F
D	V	F	G



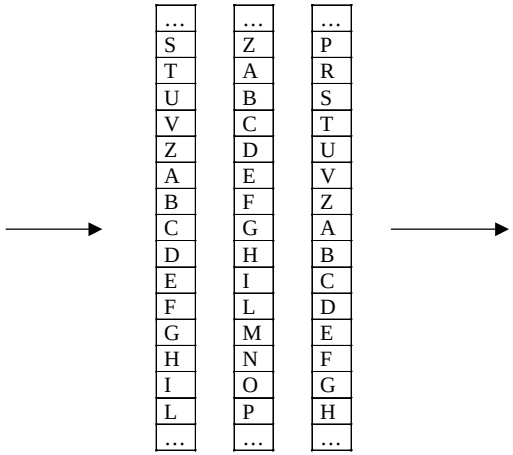
Crittogramma finale: **VFG ADV FGD AXF**

Macchine cifranti

- **Dischi alfabetici rotanti:**
  - Leon B. Alberti (1470)
- **Sistemi autocifranti a più dischi:**
  - “Enigma” di Scherbius (1918)

Schema di Enigma

(1)



3 dischi con 26 lettere
26 x 26 x 26 = 17.576 combinazioni

Schema di Enigma

(2)

- Tastiera per l'immissione delle lettere, una alla volta, e visore per mostrare le lettere cifrate.
- Ad ogni immissione le ruote si muovono.
- Ogni giorno cambio della posizione delle ruote.
- 3 ruote su 5 + pannello per sostituzione di 6 coppie di lettere portano le combinazioni a $\approx 10^{17}$

Tecniche per decrittare

- **Cifratura con corrispondenza indiretta**
  - Metodo considerato invulnerabile, se il messaggio è corto e la chiave è lunga.
- **ADFGVX**
  - Vari tentativi prima sulla lunghezza della chiave, poi sulle sequenze, poi sulla frequenza delle coppie.
  - Oggi con un computer sarebbe relativamente semplice.
- **ENIGMA**
  - Esistevano degli esemplari di Enigma, clonati in numerose copie che venivano fatti funzionare in parallelo.

Crittografia in campo binario

- Particolare struttura dei documenti e dei messaggi.
- Le elaborazioni si prestano in modo naturale al calcolo automatico.
- È la base per la moderna firma digitale e relative applicazioni.

Struttura di un documento/messaggio

- Un “documento” *d* è dato da una sequenza di caratteri (stringa di bit) di lunghezza qualunque.
- In genere è un testo, composto da più righe.
- Il documento viene spezzato in “messaggi” elementari *m*, ognuno di lunghezza fissa.
- $d = m_1 \mid m_2 \mid m_3 \mid \ldots \; m_n$

Metodo della somma

- Il messaggio elementare *m* sia di 64 bit.
- Si sceglie come “chiave” una costante $k < 64$ bit.
- Per cifrare, al valore numerico del messaggio si somma la chiave

$$m' = m + k$$

- Per decifrare: procedimento inverso.
- Il metodo è concettualmente simile a quello di Vernam.

2° Metodo di Vernam

(1)

Definizioni

- Operatore logico XOR (OR esclusivo)
- R, A, B siano grandezze binarie
- R = A.XOR.B
- R = 1 solo se A e B sono diversi

Proprietà

- A.XOR.B = B.XOR.A
- A = B.XOR.R
- B = A.XOR.R

2° Metodo di Vernam

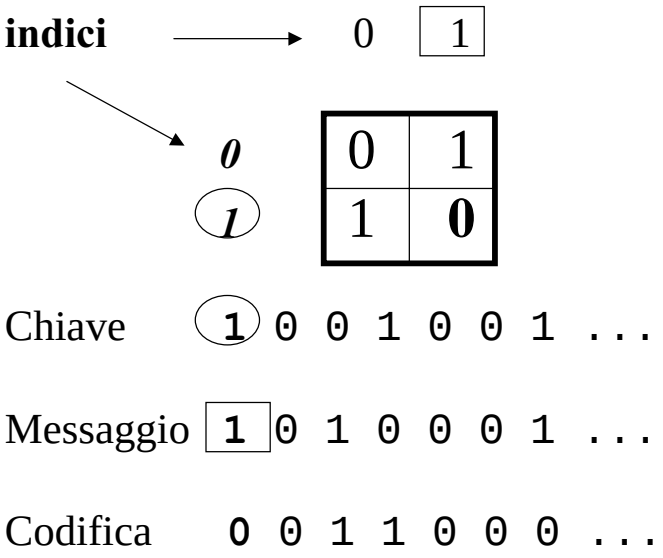
(2)

- Il messaggio da inviare sia M (binario).
- Si dispone di una chiave K (binaria) lunga quanto M.
- Il messaggio cifrato è dato da:

  C = M.XOR.K
- Per decifrare:

  M = C.XOR.K
- Numerosi metodi per ottenere la chiave K “lunga” (es.: sequenza di numeri a caso generati da una chiave “corta”, oppure sequenza parziale di una serie di cifre di un numero preassegnato).

Trasformazione indiretta a matrice di bit



Trasformazione indiretta a matrice di byte

- Sistema di cifratura simile al precedente ma basato su una matrice di byte (es.: 8 x 8)
- È la base di uno dei sistemi di cifratura più evoluti.

DES: Data Encryption Standard

- Sistema di cifratura basato su una chiave di 56 bit e su una complessa sequenza di trasposizioni e trasformazioni indirette, ripetuta 16 volte, più 2 permutazioni, secondo tabelle note, su blocchi di 8 byte.
- Un messaggio *m* espresso da 64 bit viene trasformato in un crittogramma di 64 bit.
- Approvato dal National Bureau of Standard nel ‘77: tuttora il più usato.
- Il procedimento di decifrazione è l’inverso di quello di cifratura.
- Algoritmo velocissimo per soluzioni Hw, relativamente lento in Sw.

Sicurezza del DES

- Decrittazione possibile solo per tentativi.
- Le possibili combinazioni per la chiave sono $2^{56} \approx 7{,}2 \bullet 10^{16}$
- Si tratta di un numero superiore a quello di tutte le parole pronunciate da tutte le persone del mondo negli ultimi duemila anni.
- Tentativi di rottura: DESCHALL.
- Miti e realtà.
- Comunque, è opinione corrente che il DES non sia abbastanza sicuro.

3DES (Triplo DES)

- Cifrario composto: tre operazioni DES consecutive con due chiavi diverse (complessivamente 128 bit).
- Detti:
  - C il processo di cifratura DES;
  - D il processo di decifrazione DES;
  - k_1 e k_2 le due chiavi;
  - m il messaggio da cifrare;
  - c il messaggio cifrato.
- 3DES cifra e decifra nel modo seguente:

$$c = C\{D[C(m,k_1),k_2],k_1\}$$
$$m = D\{C[D(c,k_1),k_2],k_1\}$$

- Si noti che se $k_1 = k_2 \Rightarrow$ 3DES ≡ DES

Nuovo standard

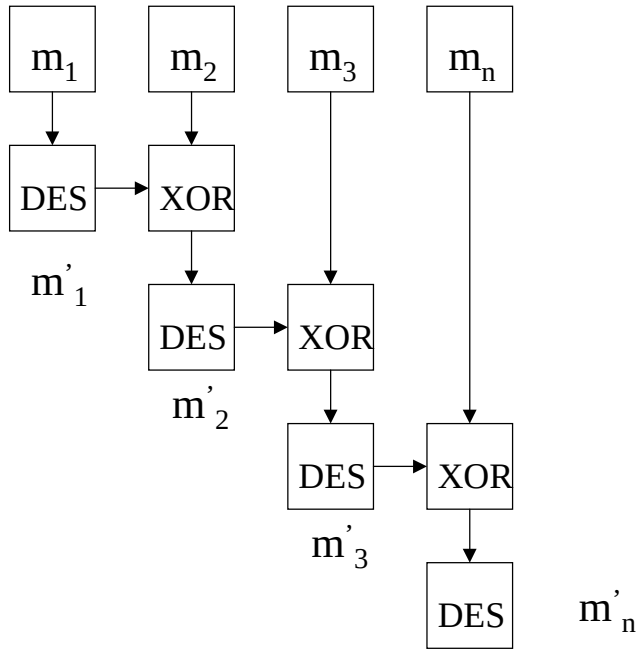
- 1977: iniziativa del NIST per sostituire il DES.
- AES: Advanced Encription Standard.
- 15 concorrenti, 5 finalisti.
- 2000: vincitore Rijndael (europeo!!!).
- Novembre 2001: definitavamente approvato come nuovo standard.
- Come il DES, l'algoritmo Rijndael opera per fasi (in numero variabile), per blocchi e con chiave di dimensioni variabili (da 128 a 256 bit).

DES
per messaggi lunghi

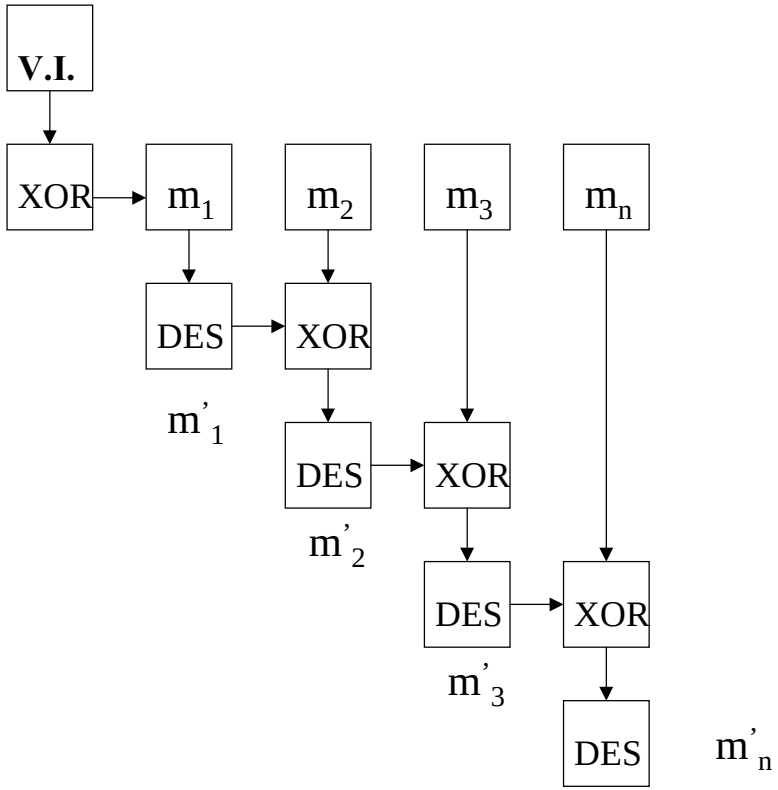
- Se $d = m_1 | m_2 | m_3 | \ldots m_n$

  il procedimento di cifratura DES va ripetuto per ognuno degli *m.*
- Anche se *d* è molto lungo questa procedura non crea problemi pratici di elaborazione.
- Spesso, per aumentare la sicurezza, la cifratura di ogni *m* avviene dopo aver compiuto un'operazione XOR con l'*m* precedente, già cifrato (CBC = Cipher Block Chaining).

Schema del CBC
(Cipher Block Chaining)



Schema del CBC con Valore Iniziale dato



Osservazioni sul CBC

- La sicurezza è data dall'insieme della Chiave e del V.I.
- In m'_n c'è il contributo di tutti gli *m* che compongono *d*.
- Se la Chiave e il V.I. assumono valori standard, m'_n diventa una caratteristisca di *d* (*impronta di d*).
- Dalla sequenza degli *m'*, nota la Chiave e il V.I., si ricava la sequenza degli *m*, cioè *d*.
- Dal solo m'_n non si può risalire a *d*.

Sistemi simmetrici

- Sono tutti quelli visti finora.
- Si chiamano così perché il metodo di decifrazione è “simmetrico” a quello di cifratura.
- La chiave per la cifratura è la stessa utilizzata per la decifrazione.
- I sistemi sono sempre reversibili.

I pilastri della sicurezza nella cifratura simmetrica

- **Metodo**

  presunto / noto
- **Cifrario**

  riservato / noto
- **Chiave**

  segreta

Motivo della insicurezza nella cifratura simmetrica

Tutti i sistemi simmetrici sono intrinsicamente **non sicuri** in quanto vi è sempre un momento in cui **la chiave transita** tra persone diverse e, pertanto, è suscettibile di intercettazione.

Alla ricerca di sistemi più sicuri

Nuovi schemi di cifratura

- Schema dei due lucchetti.
- Schema delle due cifrature.
- Aritmetica dei moduli.
- Metodo di Diffie e Hellman.

Schema dei due lucchetti

A	B
1	
Prepara il messaggio *m*, lo inserisce in uno scrigno, chiude lo scrigno con un lucchetto α (di cui possiede l'unica chiave), lo invia a B.	**2**
	Riceve lo scrigno, lo chiude una seconda volta con un lucchetto β (di cui possiede l'unica chiave), lo rimanda ad A.
3	
Riceve lo scrigno, apre il lucchetto α, invia nuovamente lo scrigno a B.	**4**
	Riceve lo scrigno, apre il lucchetto β, apre lo scrigno, legge il messaggio *m*.

Se le chiavi in possesso di A e di B sono veramente in un unico esemplare, B ha la sicurezza che quanto riceve da A non è stato alterato.

Schema delle due cifrature

A	B
1	
Prepara il messaggio *m*, lo cifra con il metodo α (a lui solo noto), lo invia a B.	**2**
	Riceve il messaggio cifrato, lo cifra una seconda volta con il metodo β (a lui solo noto), lo restituisce ad A.
3	
Riceve il messaggio, applica il metodo α', inverso di α, invia il risultato a B.	**4**
	Riceve questo risultato, applica il metodo β', inverso di β, legge il messaggio *m*.

La successione corretta dovrebbe essere: α β β'α'.
Invece è: α β α' β'. Le successioni sono equivalenti solo per particolari metodi α e β (ad es. quello di Cesare).

Alla ricerca di nuovi metodi

Quali metodi α e β adottare?

⇓

Aritmetica dei moduli.

Aritmetica dei moduli

Definizione:

N^{α} (mod M) = resto della divisione di N^{α} per M

Proprietà:

$$[N^{\alpha} \pmod M]^{\beta} \pmod M =$$
$$= [N^{\beta} \pmod M]^{\alpha} \pmod M$$

Esempio:

N = 7 **M** = 11
α = 3 β = 4

$[7^3 \pmod{11}]^4 \pmod{11} =$
$[343 \pmod{11}]^4 \pmod{11} =$
$[2]^4 \pmod{11} = 16 \pmod{11} =$ **5**

$[7^4 \pmod{11}]^3 \pmod{11} =$
$[2.401 \pmod{11}]^3 \pmod{11} =$
$[3]^3 \pmod{11} = 27 \pmod{11} =$ **5**

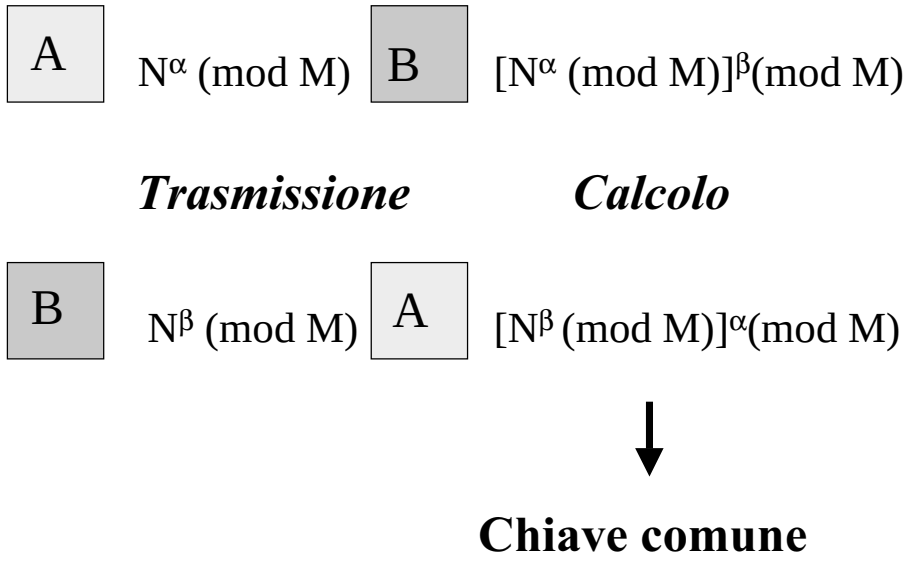
Metodo di Diffie e Hellman (1)

- Inventato nel 1975
- A e B trasmettono messaggi tra loro con il metodo DES.
- La chiave di cifratura/decifrazione viene generata all'insaputa di entrambi e senza che avvenga alcun scambio.

Metodo di Diffie e Hellman (2)

- A e B si accordano preventivamente su 2 valori N e M (non segreti).
- A sceglie un valore α a caso (segreto).
- B sceglie un valore β a caso (segreto).
- A invia a B il valore
  $x = N^{\alpha} \pmod M$
- B invia a A il valore
  $y = N^{\beta} \pmod M$
- A calcola $w = y^{\alpha} \pmod M$
- B calcola $z = x^{\beta} \pmod M$
- Risulterà $w = z$, da usare come chiave per la cifratura DES.

Schema del metodo



Valore “strategico”

- Nel metodo di Diffie e Hellman i trasferimenti sono 3 (2 per ottenere la chiave comune e 1 per il trasferimento del messaggio).
- Il sistema è macchinoso: in pratica non può funzionare.
- È comunque importante perché ha aperto la strada alla cifratura a due chiavi.

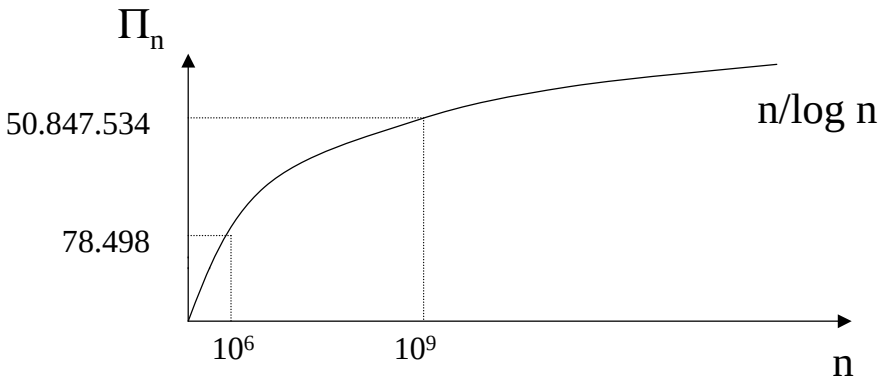
Tipi di cifratura

- **Cifratura simmetrica**
  - un metodo per cifrare;
  - il metodo inverso per decifrare;
  - **una chiave** per la cifratura e la stessa per la decifrazione.
- **Cifratura asimmetrica**
  - **due chiavi** e due metodi diversi per cifrare e decifrare.

Metodi asimmetrici:
indice degli argomenti

- Basi matematiche.
  - Numeri primi.
  - Teorema di Fermat-Eulero.
- Sistema RSA.
  - Processo di funzionamento.
  - Principio delle due chiavi.
  - Fondamento della sicurezza.
- Riservatezza.
- Autenticità.
- Integrità.

Numeri primi



Verifica della primalità di un numero *n*

- Non vi sono formule.
- Metodo diretto: crivello di Eratostene ⇒ divisioni successive fino alla radice quadrata di *n*.
- Metodo indiretto: criteri probabilistici.

Teorema di Fermat

Se ***a*** e ***n*** sono due numeri primi fra loro, il resto della divisione tra la potenza a^{n-1} e l'esponente ***n*** è sempre **= 1**, cioè:

$$a^{n-1} \pmod{n} = 1$$

Esempi

$\Rightarrow$ $a = 2 \quad n = 5 \quad a^{n-1} = 16$

$16 : 5 = 3$ con resto 1

$\Rightarrow$ $a = 3 \quad n = 7 \quad a^{n-1} = 729$

$729 : 7 = 104$ con resto 1

Teorema di Eulero

È una rielaborazione del Teorema di Fermat nel caso che *n* non sia un numero primo ma il prodotto di più numeri primi.

Se ***a*** è primo e $n = p \cdot q$ (***p*** e ***q*** primi), il resto della divisione della potenza $a^{(p-1)\cdot(q-1)}$ per ***n*** è sempre = **1**, cioè:

$$a^{(p-1)\cdot(q-1)} \pmod{n} = 1$$

Es: $p = 3 \quad q = 5 \quad a = 2$

$a^{(p-1)(q-1)} = 2^8 = 256$

$256:15 \Rightarrow$ resto = 1

Sistema RSA

- **R**ivest, **S**hamir, **A**dleman.
- MIT, 1977.
- Algoritmo basato sul Teorema di Fermat-Eulero.
- Hardy: “Teoria dei numeri completamente inutile”.
- RSA Co. venduta per 200 M$.

Principio di funzionamento del Sistema RSA (1)

- Le chiavi sono due:
  - una è **pubblica** (non segreta), ***h***;
  - l’altra è **privata** (segreta), ***j***.
- C’è un Ente centrale E che genera le due chiavi. Come? Per ogni utente:

1) vengono scelti due numeri primi p e q, e si calcola il prodotto $n = p \bullet q$
2) viene assegnato, come **chiave pubblica**, un numero a caso ***h***.
3) la corrispondente **chiave privata** ***j*** viene calcolata in modo che

$$[h \cdot j] \pmod{[(p-1)\cdot(q-1)]} = 1.$$

Principio di funzionamento del Sistema RSA (2)

- Se:
  $m' = m^{h} \pmod{n}$

  $m'' = m'^{j} \pmod{n}$

- Si dimostra che:

  $m'' = m$

- Conseguenze:

  $m \Rightarrow m'$ = messaggio cifrato
  $m' \Rightarrow m'' = m$ = messaggio decifrato

Esempio

- $p = 3, \quad q = 5 \Rightarrow n = 15$
- $\Rightarrow (p-1) \cdot (q-1) = 8$
- se $h = 11 \Rightarrow j = 3$
- verifica: $(h \cdot j) : 8 \Rightarrow$ resto = 1

$m = 2$

$m' \Rightarrow m^{h} = 2^{11} = 2048$

$\Rightarrow : 15 \Rightarrow$ resto = 8 = m'

$m'' \Rightarrow m'^{j} = 8^{3} = 512$

$\Rightarrow : 15 \Rightarrow$ resto = 2 = m

Traccia della dimostrazione

* $R[a^{(p-1)(q-1)} : n] = 1$
- $\Rightarrow a^{(p-1)(q-1)} = k\,n + 1$
* $R[(h \cdot j) : [(p-1)(q-1)]] = 1$
- $\Rightarrow h \cdot j - 1 = k\,[(p-1)(q-1)]$

- $m' = R[\, m^{h} : n]$
- $\Rightarrow m' = m^{h} - k\,n$
- $m'' = R[\, m'^{j} : n\,]$
- $= R[\, [\, m^{h \cdot j} + n(\ldots)\,] : n\,]$
- $= R[\, m^{h \cdot j} : n\,]$
- $= R[\, m\, m^{h \cdot j - 1} : n]$

  $= R[\, m\, m^{k(p-1)(q-1)} : n]$

  $= R[\, m : n\,] = m$

Il motivo della invulnerabilità

- È noto n, che si sa essere il prodotto dei due primi p e q, ma non sono noti né p né q, né è possibile ricavarli da n (si tratta di scomporre in fattori un numero grandissimo, operando solo per tentativi).
- Non è pertanto possibile calcolare $(p-1) \cdot (q-1)$.
- Dunque, noto h, non è possibile calcolare j.

Esempio

- Lunghezza di n: 128 bit
  - Max $n = 2^{127} \approx 10^{38}$
  - Metodo di Eratostene
  - $\sqrt{n} \approx 10^{19}$
  - $\Pi\ (10^{19}) \approx 10^{17}$
- 10^9 divisioni/secondo

$\Rightarrow 10^8$ secondi ≈ 3 anni

Soluzioni realizzative

In pratica si preferisce:

- utilizzare come chiave pubblica (sempre identificata da ***h***) la grandezza fin qui chiamata **n**, cioè il prodotto dei due numeri primi;
- assumere la grandezza fin qui chiamata **h** come caratteristica della "comunità" alla quale appartiene questo particolare utente.

Confronto di metodi

- Diffie e Hellman
  - α e β sono totalmente indipendenti.
  - Il metodo esige tre trasferimenti.
- RSA
  - *h* e *j* sono derivate dalla stessa coppia *p* e *q*.
  - Il trasferimento è diventato uno solo.

Basi della sicurezza nella cifratura asimmetrica

Numero di bit dell'esponente

Segretezza della chiave privata

I tre pilastri della crittografia

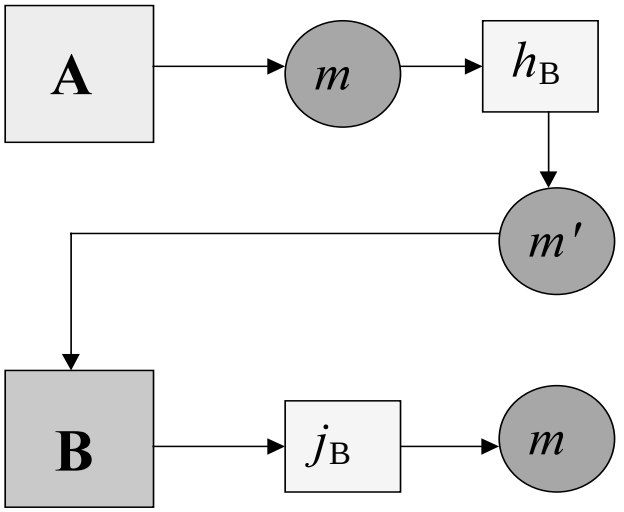
- **Riservatezza**

  ⇒ certezza che il testo può essere letto solo dal destinatario.
- **Autenticità** (o **Provenienza**)

  ⇒ certezza del mittente.
- **Integrità**

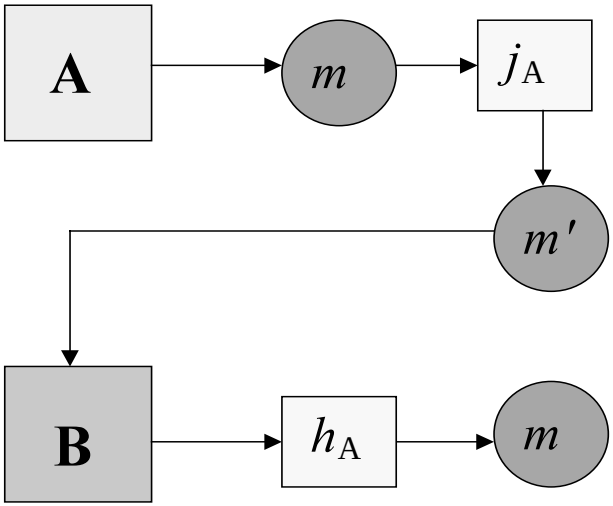
  ⇒ certezza del messaggio.

Garanzia della riservatezza



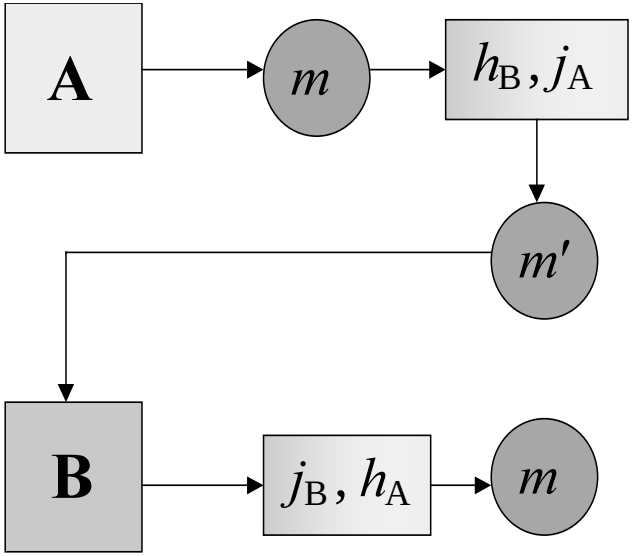
A cifra ***m*** con la chiave pubblica di B
e ottiene ***m'*** che invia a B; B lo decifra
con la propria chiave privata riottenendo ***m***.

Garanzia della autenticità



A cifra ***m*** con la propria chiave privata
e ottiene ***m'*** che invia a B; B lo decifra
con la chiave pubblica di A riottenendo ***m.***

Schema del processo di riservatezza e autenticità



Principio della doppia cifratura

Caso di messaggi lunghi

- Se $d = m_1 | \ m_2 | m_3 | \ldots \ m_n$

  i processi precedenti vanno ripetuti per ognuno degli *m.*

- Il metodo di cifratura RSA è molto lento.

- Se *d* è “lungo”, l’elaborazione può risultare molto onerosa.

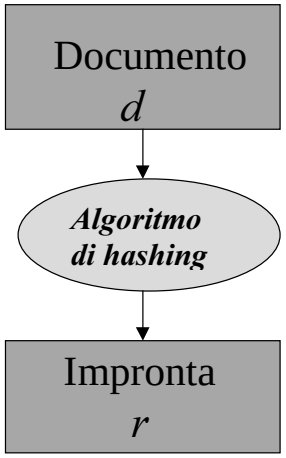
Integrità

- Il processo di autenticità garantisce indirettamente anche l’integrità del messaggio trasmesso, però:

  $\Rightarrow$ se *d* è lungo la sua cifratura con RSA può risultare onerosa;
  $\Rightarrow$ solo in pochi casi pratici valgono criteri di riservatezza per i quali occorra cifrare *d.*

Concetto di impronta (“hash”)

Campo di lunghezza fissa (in genere 160 bit) ricavato dal documento *d* mediante una procedura ben determinata e fissa.

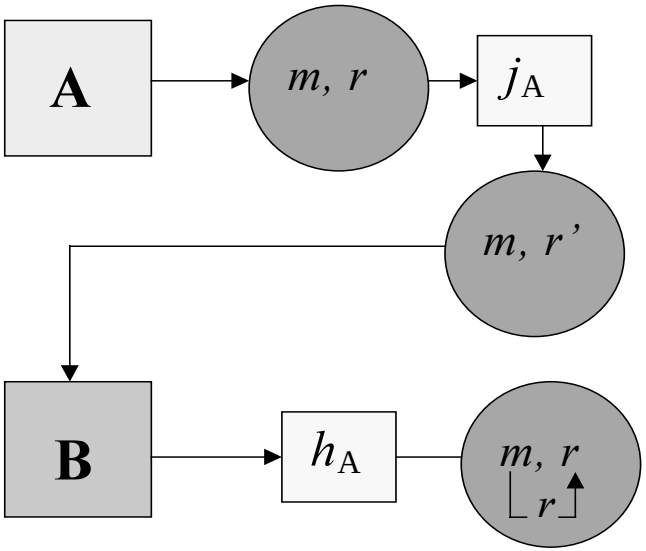


È praticamente impossibile risalire dall’impronta a un documento che generi quell’impronta.

Proprietà dell’impronta

- L’algoritmo utilizzato per ottenere l’impronta è concettualmente simile a quello del DES con CBC, con blocchi diversi.
- È praticamente impossibile risalire dall’impronta a un documento che generi quell’impronta.
- La probabilità che due documenti abbiano la stesa impronta è di $2^{-160} \approx 10^{-53}$.
- Se ogni persona al mondo per il prossimo miliardo di anni producesse un miliardo di documenti al giorno, non si arriverebbe a 10^{31} documenti.

Garanzia dell'integrità



A calcola ***r***, lo cifra con la propria chiave privata, ottiene ***r'*** che invia a B insieme a ***m***; B decifra ***r'*** con la chiave pubblica di A riottenendo ***r***, poi ricalcola l'***r*** dell'***m*** ricevuto; se le due impronte coincidono significa che ***m*** non è stato alterato.

In questo caso concettualmente $d \equiv m$.

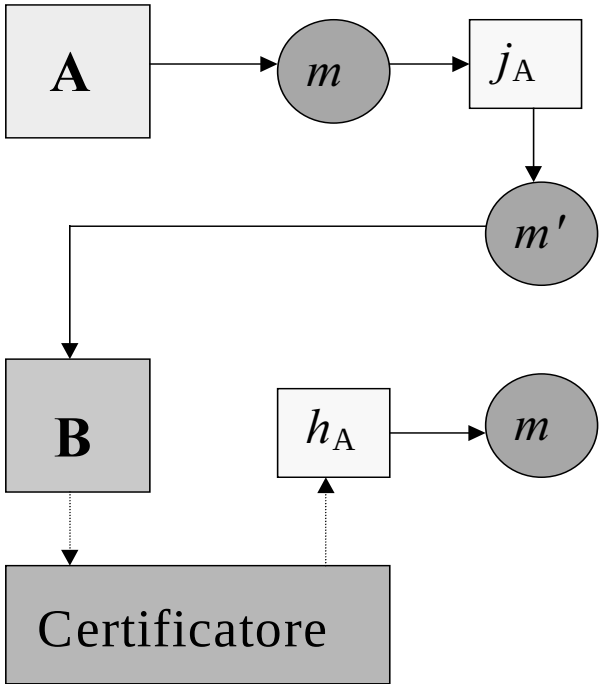
Certificazione

- Garantisce la correttezza formale e sostanziale del mittente.
- Viene ottenuta con particolari procedure informatiche e organizzative.
- Viene assicurata dai Certificatori.

I Certificatori

- Concetto di Comunità.
- I Certificatori:
  - possiedono le chiavi pubbliche di ogni membro della Comunità;
  - le forniscono a richiesta;
  - hanno una struttura tecnica ed etica a prova di frode;
- Generazione delle chiavi.

Processo “teorico” di certificazione



Vantaggi della certificazione

- Non è necessario che B conosca la chiave pubblica di ognuno dei suoi corrispondenti A: basta rivolgersi al Certificatore C.
- Se C risponde fornendo a B la chiave di A, implicitamente garantisce a B che A “esiste”.
- Un uso fraudolento delle chiavi può essere bloccato da A con una segnalazione a C.

Firma digitale

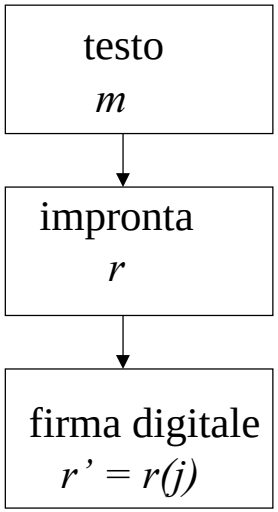
“Il risultato della procedura informatica basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al sottoscrittore tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la **provenienza e l’integrità** di un documento informatico …”

Realizzazione della firma digitale

firma digitale

⇓

impronta di
un testo
cifrata con la
chiave privata
del mittente



Caratteristiche della firma digitale

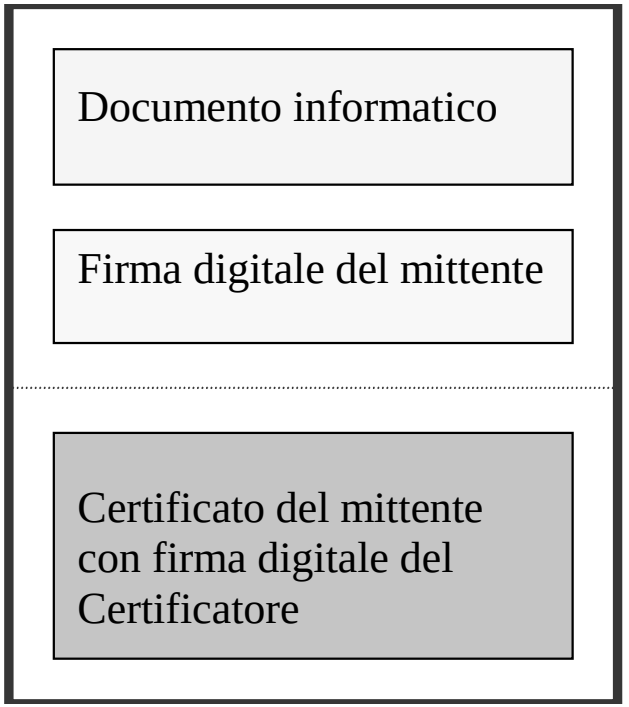
- La firma digitale dipende dal testo e dal mittente.
- Testi uguali, sottoscritti da soggetti diversi, hanno firme digitali diverse.
- Testi diversi, sottoscritti dallo stesso soggetto, hanno firme digitali diverse.

Certificato

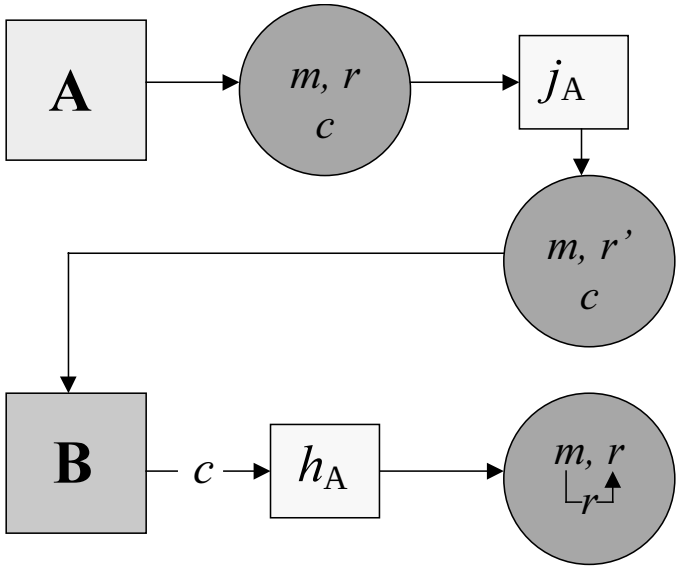
- Il Certificatore emette un certificato per ogni chiave pubblica di ogni persona nella sua attività di “mittente”.
- Il certificato contiene:
  - l’identificativo del Certificatore;
  - un numero progressivo;
  - l’identificativo del mittente;
  - la chiave pubblica del mittente;
  - eventuali “qualifiche” del mittente;
  - il periodo di validità.
- È firmato dal Certificatore.
- È in possesso del mittente.
- Va allegato al documento da inviare.

Struttura del messaggio completo

Busta elettronica



Schema d'uso del certificato



Validità di un certificato

- Elenco dei numeri dei certificati non più validi.
  - *Sospensione*: valore provvisorio.
  - *Revoca*: valore definitivo.
- Sono considerati validi tutti i certificati emessi da un certificatore, non scaduti e non inclusi nell'elenco di quelli sospesi o revocati.
- Responsabilità del Certificatore.

Processo “reale” di certificazione

- Al documento, firmato dal mittente, va allegato il certificato.
- Il destinatario trova direttamente nel certificato la chiave pubblica del mittente.
- Se il destinatario “si fida”, procede alla verifica dell’integrità del documento e alla sua lettura.
- Se “non si fida”, verifica presso il Certificatore che il certificato non sia incluso nell’elenco di quelli sospesi o revocati.

Dispositivo di firma

- Formato carta di credito, con chip; va inserito in un apposito lettore collegato a un PC.
- Capace di generare - una volta sola - una coppia di chiavi asimmetriche.
- Dotato di memoria per contenere la chiave privata.
- In grado - tutte le volte che si deve firmare un documento - di generare la firma digitale.

Modus operandi del Certificatore

- Registrazione dell'Utente
- Attivazione del servizio
- Gestione del servizio

Registrazione

- Operazione periferica.
- Responsabilità del Certificatore.
- Attribuzione di un codice.
- Consegna all'Utente di:
  - dischetto con programma per PC;
  - lettore di smart card;
  - smart card "vergine" (*dispositivo di firma*).

Attivazione

- L’Utente installa sul proprio PC il lettore di smart card e il programma ricevuti.
- Si collega al Certificatore, inserisce nel PC il proprio codice e il dispositivo di firma “vergine”.
- All’interno del dispositivo viene generata una coppia di chiavi: quella privata resta all’interno del dispositivo, quella pubblica viene inviata al Certificatore.
- Il Certificatore, fatti i dovuti controlli, genera il certificato e lo invia all’Utente che lo registra nel dispositivo di firma.

Gestione

- La firma viene gestita dal programma ricevuto dall’Utente.
- La codifica dell’impronta viene effettuata all’interno del dispositivo di firma: la chiave privata non esce mai.
- Alla firma viene associato automaticamente il certificato.
- Il Certificatore tiene disponibile in linea l’elenco dei certificati, in particolare tiene tempestivamente aggiornato l’elenco di quelli revocati o sospesi.

Generazione di *h* e *j* all'interno della card

- Ottenimento della coppia *p* e *q*
  - Generazione di numeri binari casuali molto grandi (*metodo dell'orologio, dell'angolo del disco, del rumore di fondo*).
  - Verifica della loro (probabile) "primalità" (*metodi vari*).
- Calcolo di ***h***
- Calcolo di ***j***

Sistemi ibridi

- **Sistemi simmetrici**
  - Una sola chiave
  - Operazione di cifratura semplice
  - Messaggio di lunghezza qualunque
  - Possibilità di intercettazione
  - Standard: DES e successori
- **Sistemi asimmetrici**
  - Due chiavi
  - Operazione di cifratura complessa
  - Messaggio "corto"
  - Sicurezza elevatissima
  - Standard: RSA

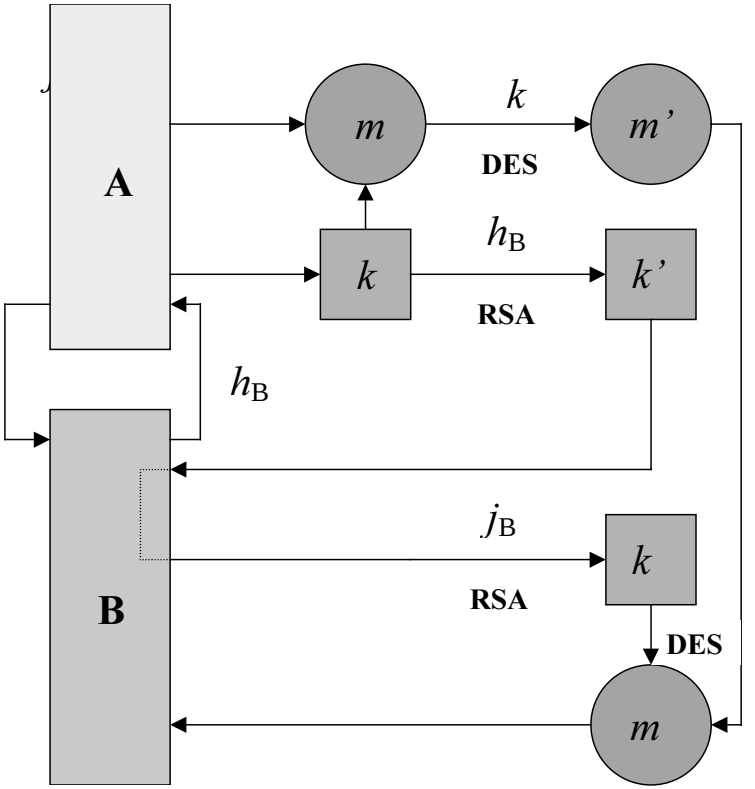
⇒**Sistemi a doppia cifratura**

- Si utilizzano per cifrare messaggi "lunghi"
- Si cifra il messaggio con il DES
- Si cifra la chiave del DES con RSA

Principio della doppia cifratura

- A deve inviare a B un messaggio *m*, non breve.
- A sceglie a caso una chiave *k*, di 64 bit.
- A cifra (con il DES) *m* mediante la chiave $k \Rightarrow m'$.
- A cifra *k* con $h_B \Rightarrow k'$
- A invia a B *m'* e *k'*
- B decifra *k'* con $j_B \Rightarrow k$
- B decifra (con il DES) *m'* con $k \Rightarrow m$

Schema di funzionamento



Sicurezza delle transazioni

- I **sistemi a due chiavi** offrono le maggiori garanzie, ma richiedono elaborazioni complesse: è difficile applicarli se il messaggio è lungo.
- I **sistemi a una chiave** offrono minori garanzie, ma richiedono elaborazioni semplici: la lunghezza del messaggio è in pratica ininfluente.
- L'utilizzo combinato di entrambi i sistemi ("**doppia cifratura**") offre il massimo della sicurezza insieme a una relativa semplicità di elaborazione, qualunque sia la lunghezza del messaggio.