



INTRODUZIONE

Lo sviluppo dell'e-business oggi ha bisogno di **garanzie** per quanto riguarda **l'inviolabilità** dei dati trasmessi.

La garanzia della **riservatezza** dei dati in rete e di transazioni commerciali **sicure** sono diventate un **obiettivo strategico** per la crescita di internet.

Prof. G. Chiumeo Crittografia e firma digitale 2 / 44

INTRODUZIONE

La crittografia è la tecnica che consente di rendere visibili le informazioni **soltanto alle persone a cui esse sono destinate.**

In una comunicazione i messaggi trasmessi tra gli interlocutori vengono **crittografati** per renderli **illeggibili** tranne che agli interlocutori stessi.

Prof. G. Chiumeo Crittografia e firma digitale 3 / 44

INTRODUZIONE

- La crittografia è nota fin dall'antichità e si è sviluppata, nel corso del tempo, soprattutto in campo militare
- La paternità è attribuita Giulio Cesare (!)
- Si basa generalmente su algoritmi matematici



INTRODUZIONE

Un po' di terminologia:

- **Testo in chiaro**: è il messaggio che può essere letto da tutti
- **Testo cifrato**: è il testo in chiaro trasformato in messaggio illeggibile
- **Codifica (cifratura)**: tecnica che trasforma testo in chiaro → testo cifrato
- **Decodifica (decifrazione)**: tecnica che trasforma testo cifrato → testo in chiaro

INTRODUZIONE

La CODIFICA e la DECODIFICA sono eseguite da uno o più

ALGORITMI CRITTOGRAFICI

che utilizzano:

- Una o più funzioni matematiche
- Una o più chiavi per operazioni di cifratura o decifrazione

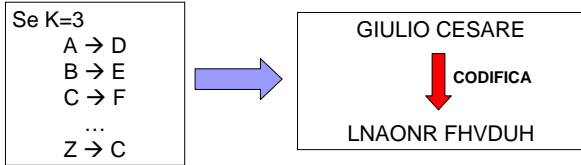


INTRODUZIONE

Esempio 1

Algoritmo di Giulio Cesare

Data una chiave k numerica
sostituire ogni lettera di una frase con la k-ma successiva
dell'alfabeto



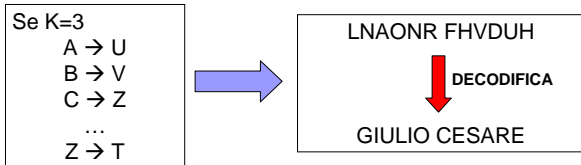
INTRODUZIONE

Cifrario a sostituzione

Esempio 1

Algoritmo di Giulio Cesare

Data una chiave k numerica
sostituire ogni lettera di una frase con la k-ma successiva
dell'alfabeto



INTRODUZIONE

Esempio 2

Sia data una frase:
*La cavalleria deve
attaccare sull'ala sinistra*
Sia data una chiave k di tipo stringa
K= VINCE

- Dividere la frase in tante colonne quante sono le lettere della chiave k scrivendola in orizzontale
- Ordinare le colonne in base all'ordine alfabetico della chiave k e spedirle

V	I	N	C	E
L	A	C	A	V
A	L	L	E	R
I	A	D	E	V
E	A	T	T	A
C	C	A	R	E
S	U	L	L	A
L	A	S	I	N
I	S	T	R	A



LA CRITTOGRAFIA SIMMETRICA

- Sistema di codifica convenzionale
- Usa **una sola chiave** per cifrare e decifrare
- Mittente e destinatario usano la **stessa chiave**

Esempio: Algoritmo di Giulio Cesare!!
 Esempio: Algoritmo a trasposizione!!
 Esempio: Doppio operatore XOR...

Prof. G. Chiameo Crittografia e firma digitale 14 / 44

LA CRITTOGRAFIA SIMMETRICA

Esempio: ...doppio operatore XOR

(A xor K) xor K = A

A	B	A xor B
0	0	0
0	1	1
1	0	1
1	1	0

Alice → **Bob**

C = crittogramma

Messaggio A

C = A xor K

🔑 K = chiave

A = 110011010
 K = 101110001
C = 011101011
C xor K = 110011010

Messaggio C

A = C xor K

🔑 K = chiave

Più grande è K più difficile sarà infrangere C

Se K=10 bit → 2¹⁰ K distinte
 Se K=20 bit → 2²⁰ K distinte
 ...

Se K = 40 bit → 2⁴⁰ K distinte → 10¹² k distinte → se provo una chiave ogni millisecondo servirebbero 10⁹ secondi = 10⁸ giorni = 27,7 anni!
K = 128 bit è ritenuta SICURA

Prof. G. Chiameo Crittografia e firma digitale 15 / 44

LA CRITTOGRAFIA SIMMETRICA

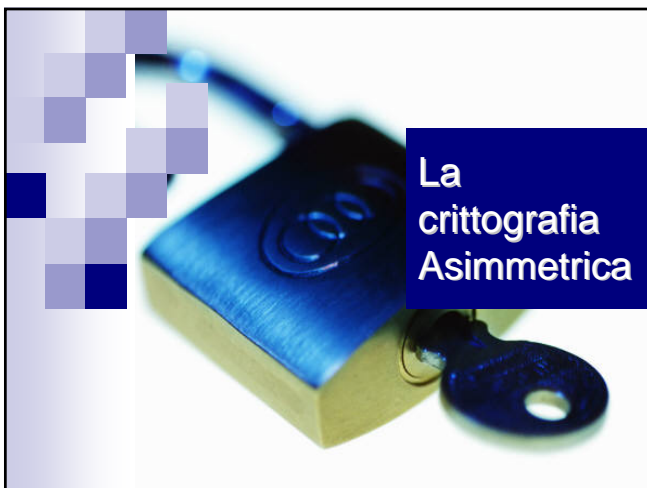
Sistemi crittografici

- DES (Data Encryption Standard): IBM 1974 → K = 56 bit
- 3DES → K maggiore
- CAST → sviluppato dalla *Nortel* → K = 128 bit
- IDEA (International Data Encryption Algorithm) → Svizzera 1990 → K = 128 bit

LA CRITTOGRAFIA SIMMETRICA

SVANTAGGI

- Difficoltà nel mantenere la chiave K segreta
- La segretezza dipende dai possessori di K
- Per N conoscenti bisognerebbe avere N chiavi distinte t.c. N° chiavi $K = (n-1)n/2$
- Difficoltà per la distribuzione sicura della chiave K, cioè dello scambio



LA CRITTOGRAFIA **A**SIMMETRICA

- Nasce nel 1975
- È chiamata anche “**Crittografia a chiave pubblica**”
- Risolvere il problema della **distribuzione sicura** delle chiavi
- Utilizza una coppia di chiavi



LA CRITTOGRAFIA **A**SIMMETRICA



- Le due chiavi sono **correlate MATEMATICAMENTE:**
i messaggi codificati con la chiave pubblica possono essere decodificati solo con la chiave privata e viceversa

■ La **particolarità** e la **forza** di questo sistema crittografico è che, anche conoscendo la chiave pubblica, **non è possibile** risalire alla corrispondente chiave privata se non con calcoli che richiedono tempi molto elevati

■ La coppia di chiavi viene generata da un **software opportuno**. Ogni persona che vuole ricevere i messaggi cifrati deve fornirsi di una coppia di chiavi:

- La chiave **PRIVATA** è mantenuta segreta
- La chiave **PUBBLICA** viene distribuita liberamente a tutte le persone con cui si vuole comunicare

LA CRITTOGRAFIA **A**SIMMETRICA



Diverse combinazioni di chiave pubblica e privata determinano

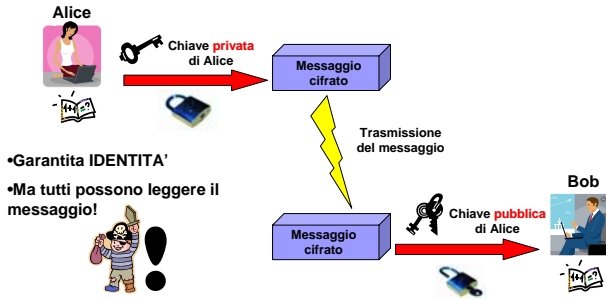
DIVERSI LIVELLI DI SICUREZZA

nella comunicazione dei messaggi

Analizziamoli...

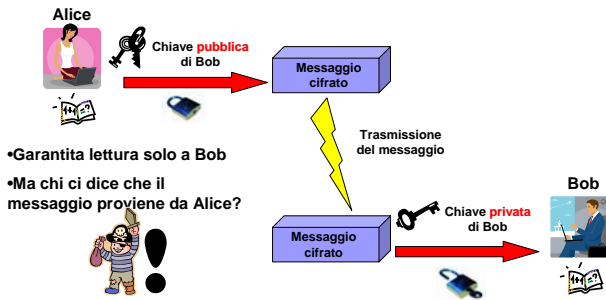
LA CRITTOGRAFIA ASIMMETRICA

A) Garanzia IDENTITA' del mittente



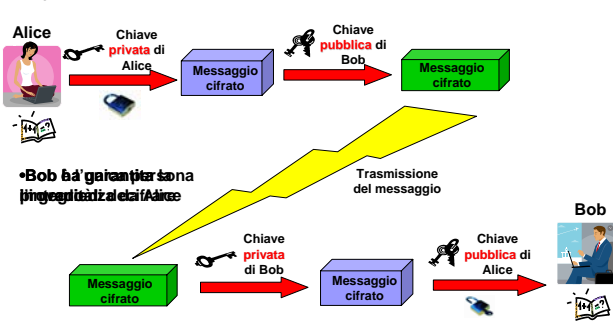
LA CRITTOGRAFIA ASIMMETRICA

B) Garanzia di SEGRETEZZA



LA CRITTOGRAFIA ASIMMETRICA

C) Garanzia IDENTITA' del mittente + SEGRETEZZA + INTEGRITA'



LA CRITTOGRAFIA **A**SIMMETRICA

Considerazioni finali:

- Alice e Bob non devono condividere una chiave segreta
- I mittenti devono solo conoscere la chiave pubblica del destinatario
- La chiave privata deve essere solo conservata dal destinatario

Prof. G. Chiameo Crittografia e firma digitale 25 / 44

Approfondimento

LA CRITTOGRAFIA **A**SIMMETRICA RSA (Rivest, Shamir, Adleman – 1978)

- Si basa sulla difficoltà di fattorizzare numeri molto grandi (10³⁰⁰ cifre!)
- Chiave **pubblica** di 2 numeri: $K_{pub}=(pub,n)$
- Chiave **privata** di 2 numeri: $K_{pri}=(pri,n)$
- Per **cifrare** un messaggio:
 - $c = m^{pub} \bmod n$
 - m = carattere oppure un blocco del messaggio trasformato in binario
 - C = crittogramma
 - mod = calcola il resto della divisione
- Per **decifrare** un messaggio:
 - $m = c^{pri} \bmod n$

Prof. G. Chiameo Crittografia e firma digitale 26 / 44

Approfondimento

LA CRITTOGRAFIA **A**SIMMETRICA RSA (Rivest, Shamir, Adleman – 1978)

- Come costruire $K_{pub}=(pub,n)$ e $K_{pri}=(pri,n)$?
 1. Scelgo due numeri **primi** **a** e **b** molto grandi
t.c. $n = a*b \rightarrow$ (secondo numero delle chiavi)
 2. Determino $z = (a-1)*(b-1)$
e scelgo le chiavi:

Funzioni
ONE-WAY
Con trapdoor

 - A. *pri* t.c. non abbia fattori comuni con z
 - B. *pub* t.c. soddisfi l'equazione:
 $(pub*pri) \bmod z = 1$

Prof. G. Chiameo Crittografia e firma digitale 27 / 44

LA CRITTOGRAFIA ASIMMETRICA RSA (Rivest, Shamir, Adleman – 1978)

Esempio (1/5):

Scegliamo 2 numeri primi a e b (piccoli per comodità):

- $a=17$ $n = a*b = 17*5 = 85$
- $b=5$ $z = (a-1)*(b-1) = 16*4 = 64$

Scegliamo $pri=5$ perché non ha fattori comuni con z

Scegliamo $pub=13$ perché soddisfa l'eq.ne: $(pub*5) \bmod 64 = 1$

- $K_{pub}=(pub,n)=(13,85)$
- $K_{pri}=(pri,n)=(5,85)$

LA CRITTOGRAFIA ASIMMETRICA RSA (Rivest, Shamir, Adleman – 1978)

Esempio (2/5):

Testo in chiaro	m	m^{13}	$c = m^{13} \bmod 85$
E	5	1220703125	20
U	19	42052983462257059	49
R	16	4503599627370496	16
O	13	302875106592253	13
P	14	793714773254144	39
A	1	1	1

EUROPA $\xrightarrow{c = m^{pub} \bmod n}$ 20, 49, 16, 13, 39, 1
Testo cifrato

LA CRITTOGRAFIA ASIMMETRICA RSA (Rivest, Shamir, Adleman – 1978)

Esempio (3/5):

- $K_{pub}=(pub,n)=(13,85)$
- $K_{pri}=(pri,n)=(5,85)$

Decifriamo il crittogramma 20, 49, 16, 13, 39, 1 applicando la formula, numero x numero:

$$m = c^{pri} \bmod n = c^5 \bmod 85$$

Soltanto chi possiede la chiave privata (5, 85) può decifrare il messaggio

LA CRITTOGRAFIA ASIMMETRICA RSA (Rivest, Shamir, Adleman – 1978)

Esempio (4/5):

Testo cifrato	c^5	$m = c^5 \text{ mod } 85$	Testo in chiaro
20	3200000	5	E
49	282475249	19	U
16	1048576	16	R
13	371293	13	O
39	90224199	14	P
1	1	1	A

20, 49, 16, 13, 39, 1 $\xrightarrow{m = c^5 \text{ mod } 85}$ EUROPA

LA CRITTOGRAFIA ASIMMETRICA RSA (Rivest, Shamir, Adleman – 1978)

Esempio (5/5):

Nelle applicazioni pratiche i numeri utilizzati per le **chiavi** sono molto più **grandi** e la codifica **non** avviene **carattere per carattere**, ma per **blocchi**.

LA CRITTOGRAFIA IBRIDA

Essendo

- Cifrari SIMMETRICI → veloci ma n^k molto elevato + problema dello scambio di k
- Cifrari ASIMMETRICI → lenti ma efficienti

ALLORA

si utilizza un cifrario **IBRIDO**:

- Cifrario SIMMETRICO per la comunicazione
- Cifrario ASIMMETRICO per lo scambio di chiavi k

LA CRITTOGRAFIA IBRIDA

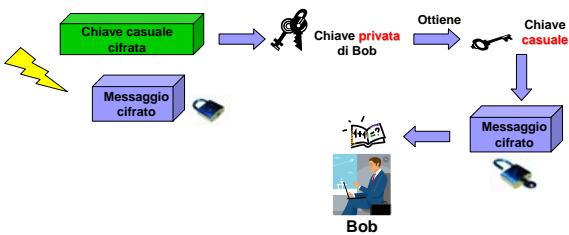
■ Il messaggio viene crittografato con un algoritmo a **chiave simmetrica**, in cui la **chiave** è generata **casualmente**.



■ La **chiave casuale** generata per cifrare il messaggio, viene **crittografata** mediante la chiave pubblica del destinatario.

LA CRITTOGRAFIA IBRIDA

■ Il destinatario, mediante la sua chiave privata, decifra la chiave usata per codificare il messaggio e quindi il messaggio stesso





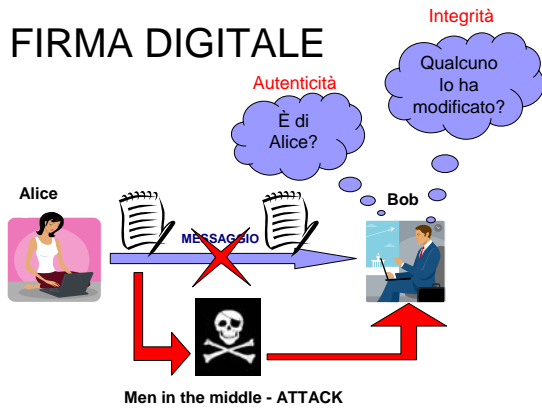
LA FIRMA DIGITALE

È un metodo elettronico che permette ad una persona di apporre un suo segno distintivo ai documenti digitali.

Tramite la **firma digitale** chiunque può verificare:

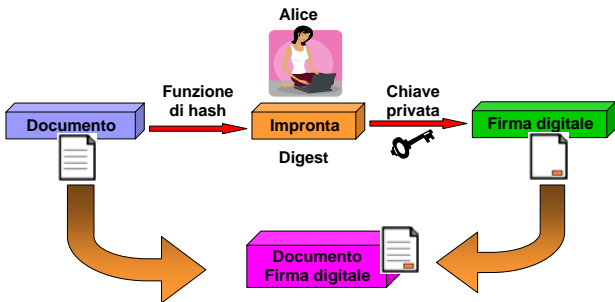
- **Autenticità** del messaggio
- **Integrità** del messaggio

LA FIRMA DIGITALE



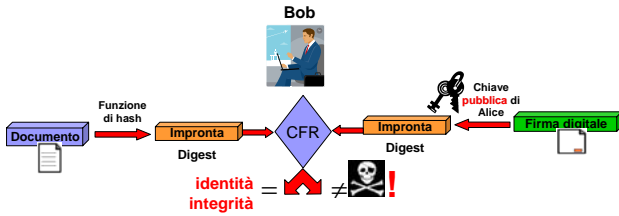
LA FIRMA DIGITALE: invio

La firma digitale viene realizzata usando i sistemi di **CRITTOGRAFIA ASIMMETRICA**.



LA FIRMA DIGITALE: **verifica**

Chi vuole controllare l'**identità** e l'**integrità** del messaggio deve usare sia la **funzione Hash** sia la **chiave pubblica del mittente**.



ATTENZIONE: dopo l'apposizione della firma digitale, ogni modifica al documento comporta una modifica nell'impronta associata!

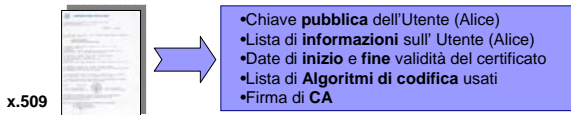
Questo significa che: **la firma digitale è diversa per ogni documento**

LA FIRMA DIGITALE

La coppia di chiavi pubblica e privata deve essere rilasciata da un

**Ente di certificazione
Certification Authority**

che garantisce l'identità del possessore della chiave (ovvero la validità della chiave pubblica)



LA FIRMA DIGITALE: **conclusioni**

La può **generare solo una persona** (colui che conosce $k_{U[priv]}$ cioè Alice.

Non è **riutilizzabile / copiabile / falsificabile**: in quanto è funzione del documento su cui è apposta.

Il **documento** su cui è apposta **non è modificabile**: in quanto anche la firma andrebbe nuovamente generata.

Non può essere **ripudiata** da chi l'ha generata: in quanto solo conoscendo $k_{U[priv]}$ (Alice!) è possibile generarla.

Il documento firmato non è indirizzato ad uno specifico destinatario. **Tutti possono fare la verifica.**

LABORATORIO: PGP



- Il sw più conosciuto è PGP = Pretty Good Privacy
- PGP è freeware (ver 8.0 su www.pgp.com)
- Ideato da Phil Zimmermann nel 1991
- Genera automaticamente le coppie di chiavi *pub* e *pri*
- Consente di:
 - Cifrare i messaggi
 - Decifrare i messaggi
 - Firmare digitalmente i messaggi di e-mail



BIBLIOGRAFIA

- A. Lorenzi – R. Giupponi
“Informatica: Sistemi operativi e reti per il sistema informativo aziendale” – Ed. ATLAS
- A. Lorenzi – T. Pizzigalli – M.A. Ratazzi
“I sistemi operativi, reti e internet, il sistema informativo aziendale” – Ed. ATLAS
- L. Margara: slides Master Alma
“Sicurezza dell’informazione” – Università di Bologna
(<http://www.cs.unibo.it/~margara/>)
- Sito dedicato a PGP dell’università di Torino: <http://www.pgp.unito.it/>