



# **Navigare (pagare) sicuri in internet**

**Prof. Marco Mezzalama**

**Politecnico di Torino**





## *Wanted by the FBI*

[Home](#) • [Most Wanted](#) • [Cyber's Most Wanted](#)

## Cyber's Most Wanted

Select the images of suspects to display more information.



JOHN GORDON  
BADEN



EVGENIY  
MIKHAILOVICH  
BOGACHEV



SUN KAILIANG



HUANG ZHENYU



WEN XINYU



SHAILESHKUMARJABBERZEUS  
P. JAIN



SUBJECTS



BJORN DANIEL  
SUNDIN



ALEXANDR  
SERGEYEVICH  
BOBNEV



CARLOS  
ENRIQUE  
PEREZ-MELARA

# Un nuovo fenomeno

Il numero totale del mobile malware è valutato pari a 150.000, di cui 100.000 prodotti nel solo 2014, ed è quadruplicato rispetto al 2011.

I canali preferiti sono le apps seguite dagli sms/mms

L'obiettivo principale è sottrarre password, indirizzi, numeri telefonici ma ultimamente ha raggiunto limiti significativi il fenomeno dello **spyware**



# Social Engineering



Nel campo della sicurezza informatica, l'ingegneria sociale è lo studio del comportamento individuale di una persona al fine di carpire informazioni utili

# Phishing (la pesca dei creduloni)

Installa subito l'allegato monica.exe  
se vuoi chattare con Monica B.  
E' gratis!!!



# Nel 2014 password più usata '123456'

Analisi Splashdata su 3,3 mln parole chiave hackerate

Redazione ANSA

📍 ROMA

26 gennaio 2015

15:53

NEWS



Suggerisci



Facebook



Twitter



Google+



Altri





# **Autenticazione del sito (verifica URL)**

1. Attenti al nome (www.banca.it.ro)
2. Attenti al protocollo (https)
3. Diffidare (molti link presenti in mail, social media, icone pubblicitarie sono fraudolenti)
4. Diffidare degli allegati

# Canale sicuro





# Il crittanalista.....



.... il secondo mestiere più vecchio  
del mondo !

# La storia della crittografia



4500 a.C.



Cifrario di Cesare



Leon Battista Alberti  
(1404 - 1472)

# La storia della crittografia



Enigma (1932)



Alan Turing  
(1912 – 1954)



# Crittografia

## Il contesto applicativo:

- riservatezza
- autenticazione
- scambio chiavi segrete
- firma digitale



# Crittografia

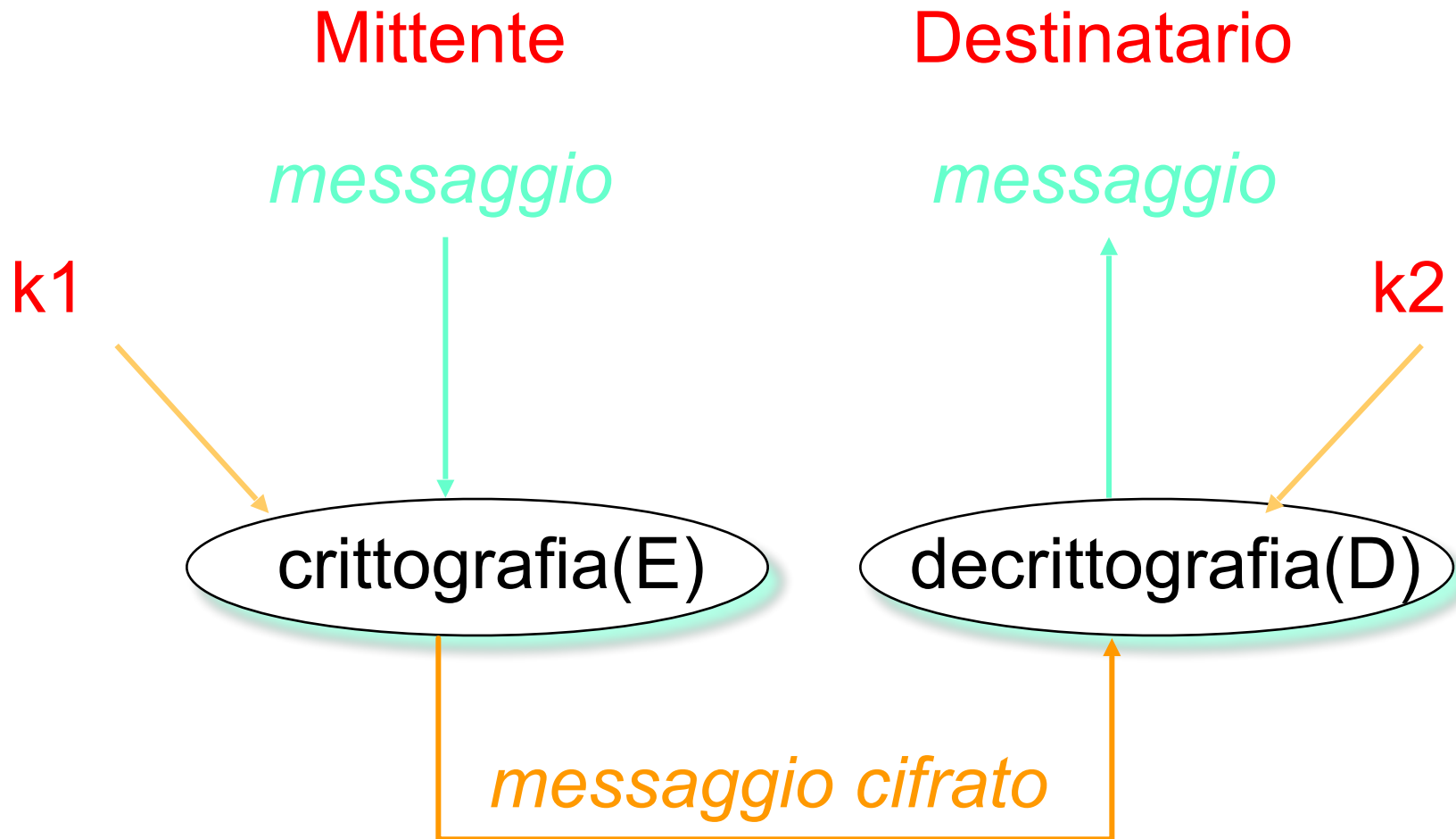
**Gli algoritmi crittografici possono essere classificati in tre categorie:**

- algoritmi a chiave segreta (alg. simmetrici)
- algoritmi a chiave pubblica (alg. asimmetrici)
- algoritmi di hash (digest, impronta, firma digitale)

# Crittografia

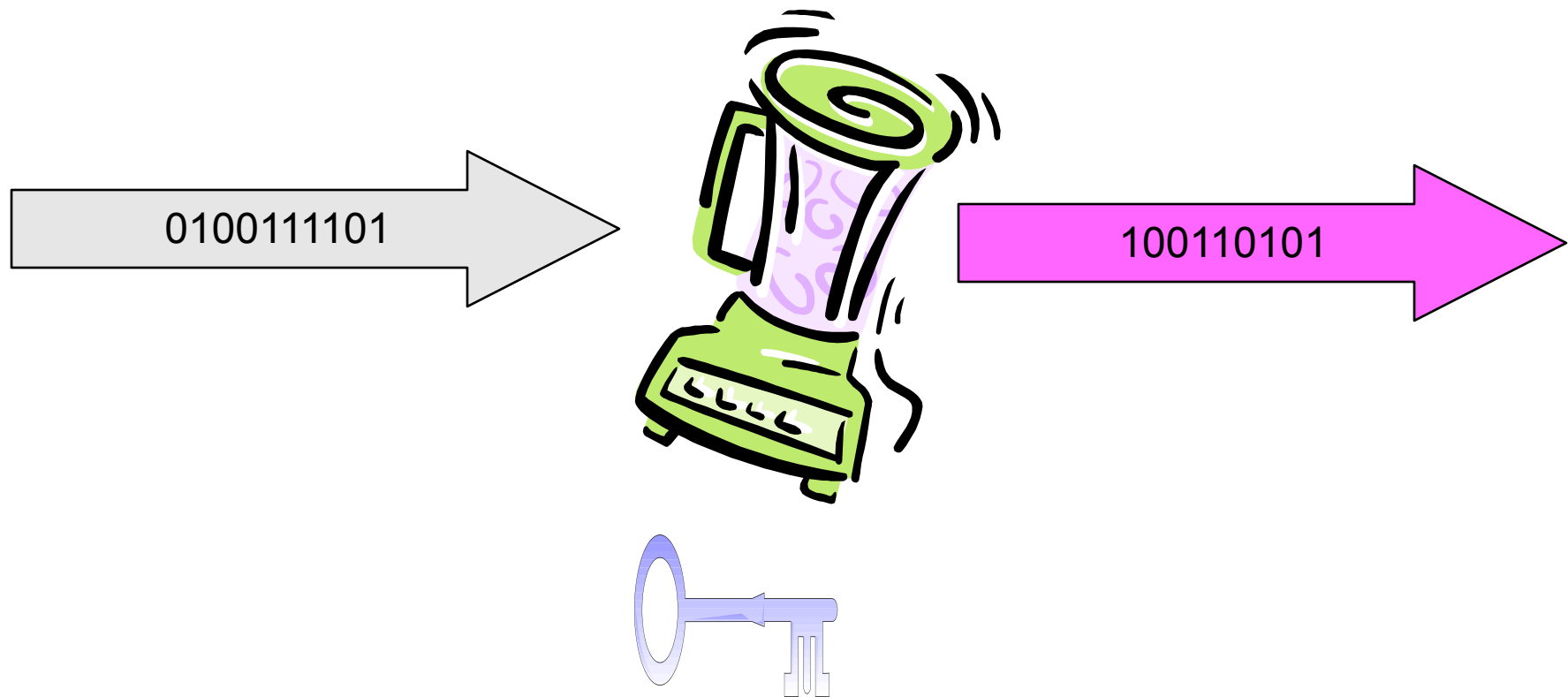
- Testo in chiaro (plaintext, T)
- testo cifrato (ciphertext, C)
- coppia di chiavi  $k_1$  e  $k_2$
- algoritmo di cifratura, E:  $C = E(T, K_1)$
- algoritmo di decifratura, D:  $T = D(C, K_2)$
- **Segretezza:**
  - algoritmi, E e/o D
  - chiavi  $k_1$  e/o  $k_2$

# Crittografia



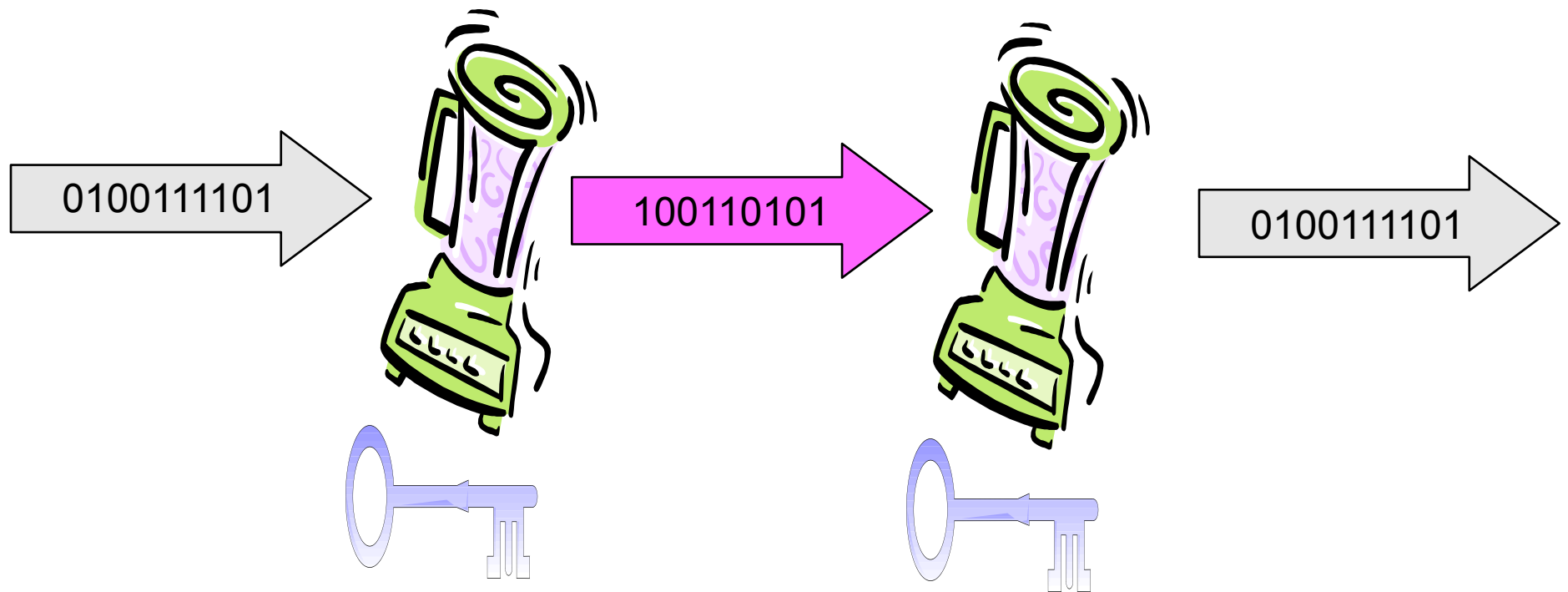


# Il frullino crittografico ....



La chiave di selezione del programma

# Il frullino crittografico .... simmetrico

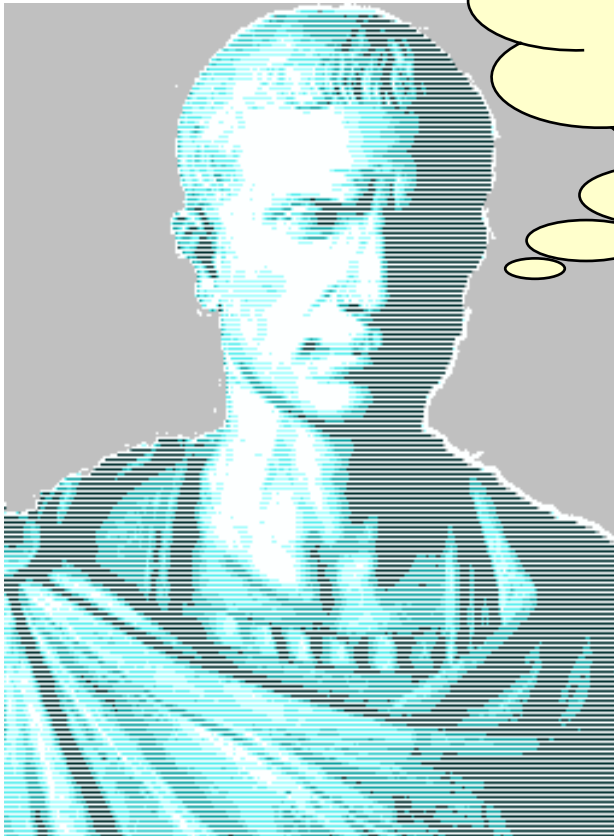


# Crittografia (cifrario di Atbash)

Il libro di Geremia nella Bibbia usa un semplicissimo cifrario monoalfabetico per cifrare la parola Babele; la prima lettera dell'alfabeto ebraico (Aleph) viene cifrata con l'ultima (Taw), la seconda (Beth) viene cifrata con la penultima (Shin) e così via; da queste quattro lettere è derivato il nome di Atbash (A con T, B con SH) per questo codice.

CHIARO	a	b	c	d	e	f	g	h	i	j	k	l	m
CIFRATO	Z	Y	X	W	V	U	T	S	R	Q	P	O	N
CHIARO	n	o	p	q	r	s	t	u	v	w	x	y	z
CIFRATO	M	L	K	J	I	H	G	F	E	D	C	B	A

# Crittografia (cifrario di Cesare)



**Attenzione!  
Asterix ci ascolta!**



# Tecniche di sostituzione

A	D
B	E
C	F
.....	
W	Z
X	A
Y	B
Z	C

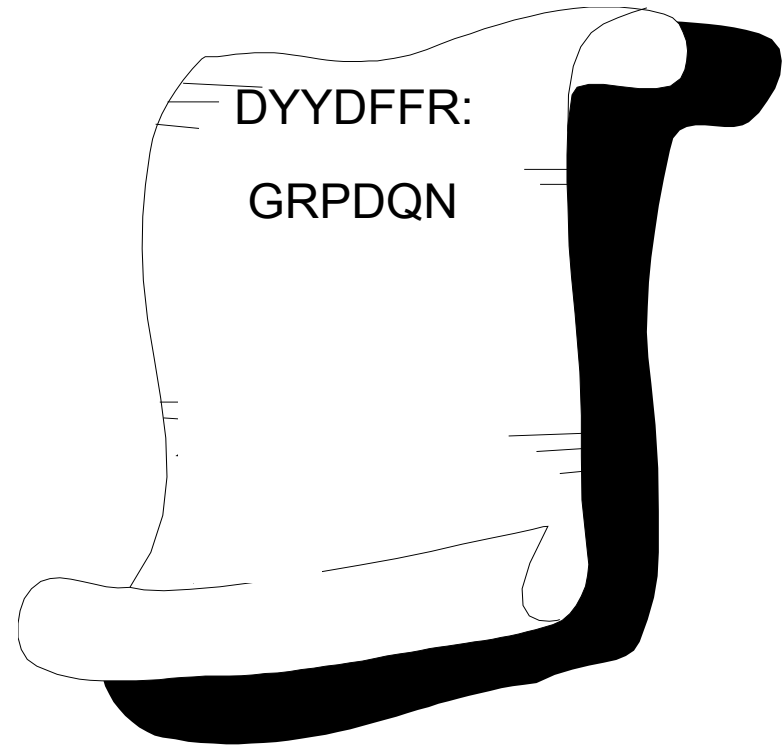
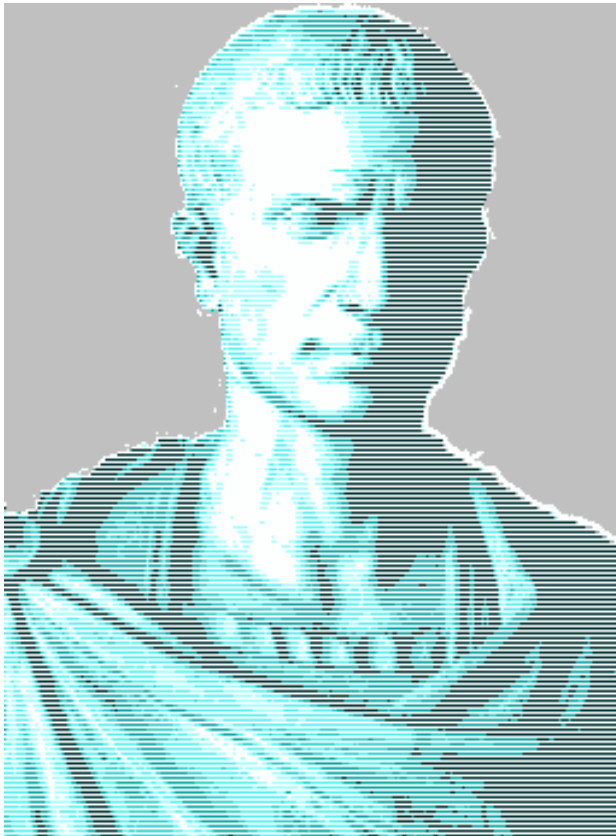
Ad ogni lettera si sostituisce quella che la segue spostata di un numero fisso di posizioni

$$C = (\text{lettera} + 3) \bmod 26$$



Chiave segreta





$K = 3$



# Tecniche di trasposizione

Testo = MARCO MEZZALAMA.

Algoritmo = prendo due simboli e li inverte con i successivi (chiave = 2,2)

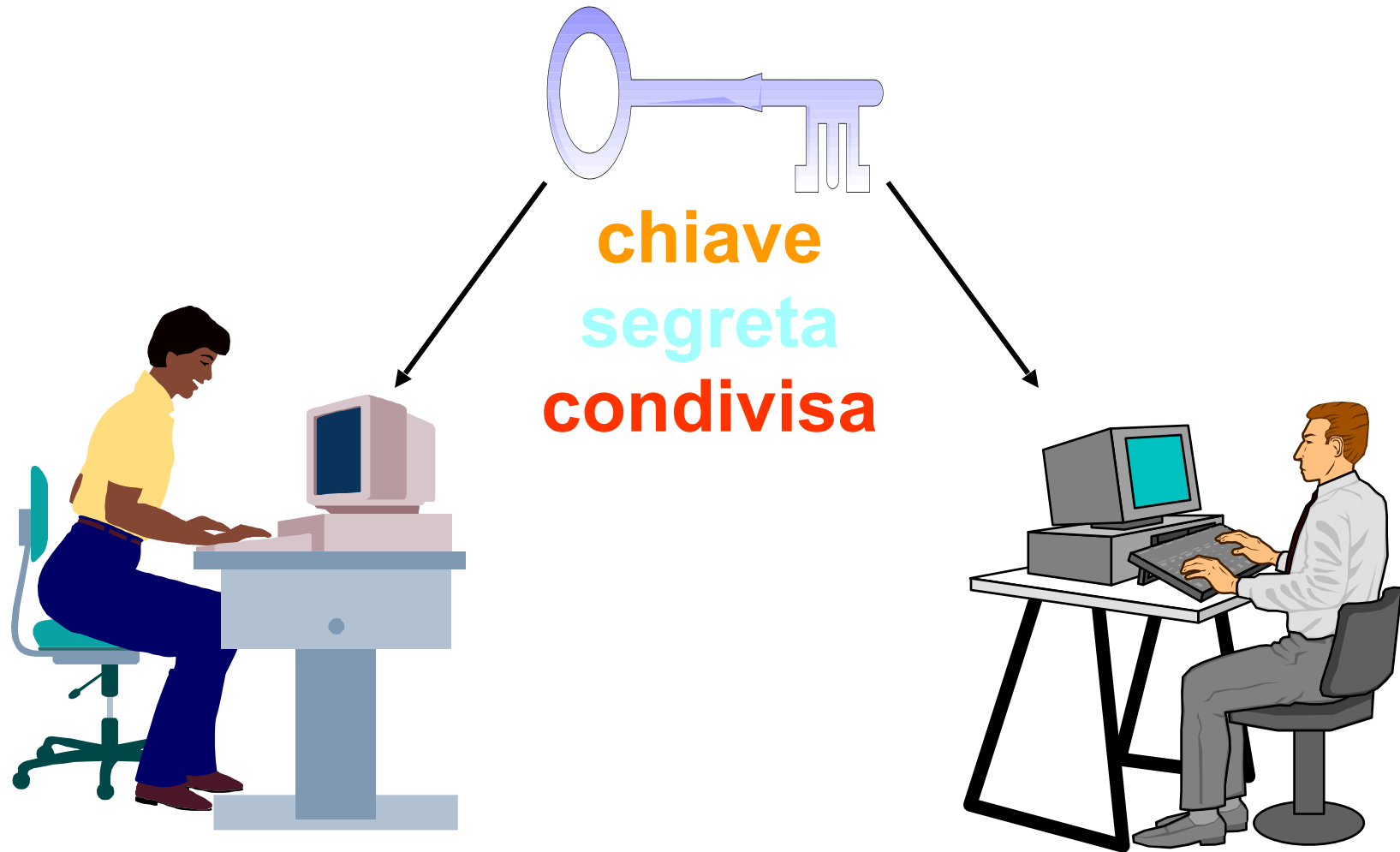
Testo = MA RC O ME ZZ AL AM A.

Testo cifrato = RCMAMEO ALZZA.AM

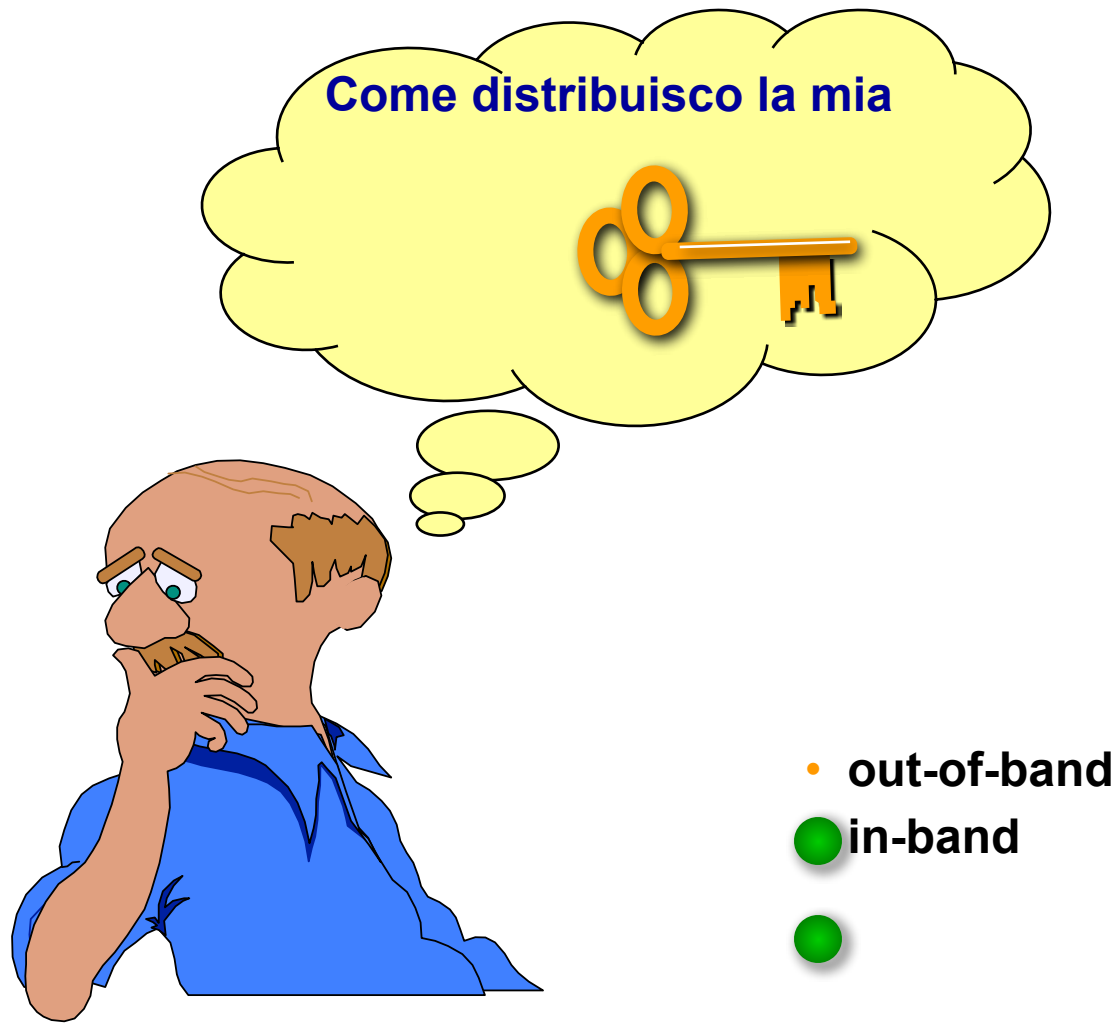
# Principali algoritmi di crittografia simmetrica

Algoritmo	Chiave	Blocco Base	Applicazione tipica
DES	56 bit	64 bit	Bancaria, networking, Internet (SSL, S/MIME)
Triplo DES	112o168 bit	64 bit	
IDEA	128 bit	64 bit	E-mail (PGP)
RC2	8-1024 bit	64 bit	Internet (SSL, S/MIME)
RC4	Ignota	Stream	Internet (SSL, S/MIME)
RC5	1-2048 bit	1-256 bit	WAP
AES	128-256 bit	128 bit	applicazioni bancarie

# Distribuzione delle chiavi



# Distribuzione delle chiavi



# **Crittografia a chiavi asimmetriche**

## **Chiave pubblica/chiave privata**

### **Certificato**



**Bailey Whitfield 'Whit' Diffie**



**Martin Edward Hellman**

# Crittografia a chiavi asimmetriche

## RSA

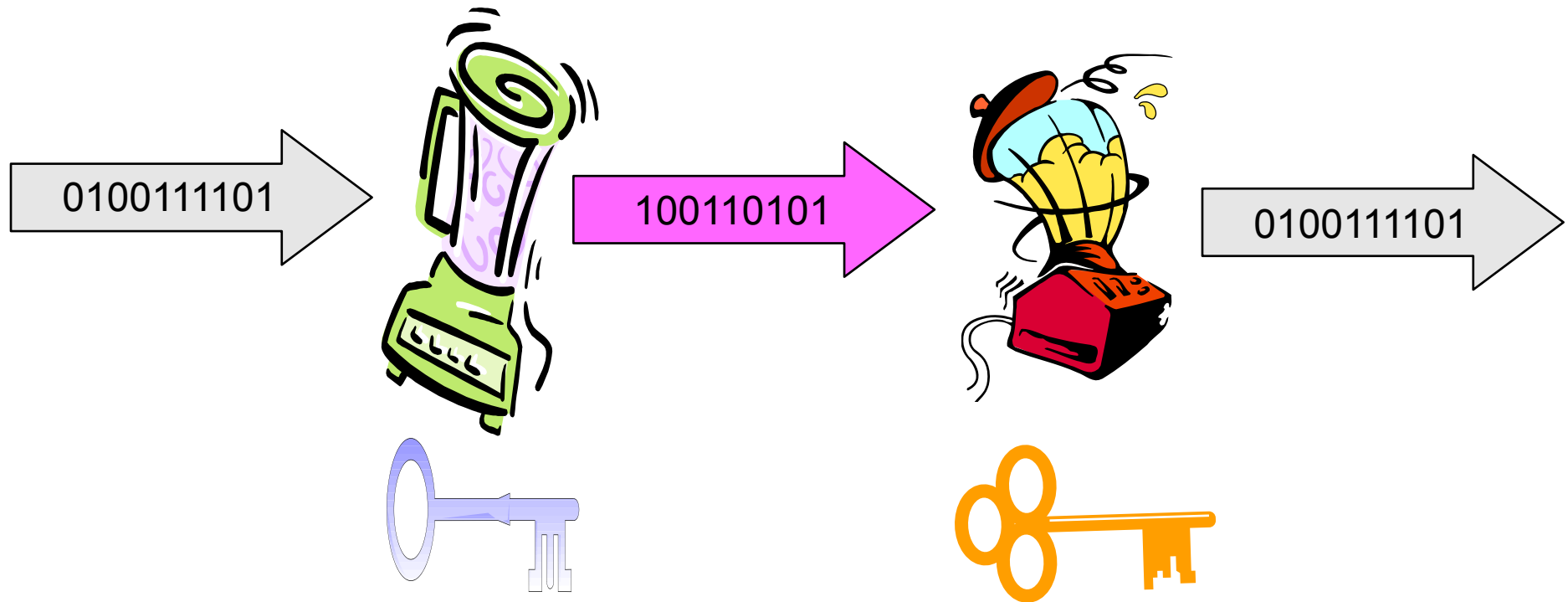
### (1977)



River, Shamir, Adelman (MIT)



# Il frullino crittografico .... asimmetrico





# Crittografia a chiave pubblica

- $k_1 \neq k_2$ 
  - $K_1 = K_{pub} = \text{chiave pubblica}$
  - $K_2 = K_{pri} = \text{chiave privata}$
- algoritmi asimmetrici
- coppie di chiavi (*pubblica e privata*)
- ruolo delle chiavi interscambiabile
- alto carico computazionale

# Crittografia a chiave pubblica

- **si basa sulle funzioni unidirezionali:**

- $y = f(x)$       complessità bassa (P)
- $x = f^{-1}(y)$       complessità molto alta (NP)

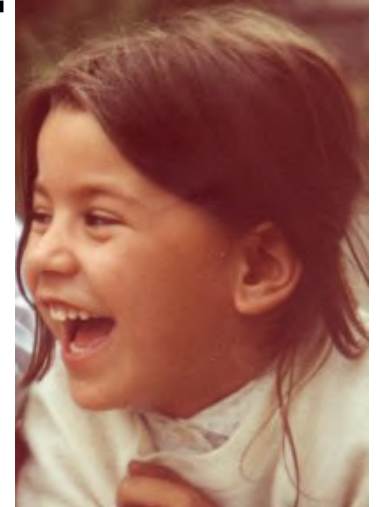
- **Esempi:**

- elevazione potenza:  $3^4 = 3 \times 3 \times 3 \times 3 = 81$
- ma, logaritmo:  $\log_3 81 = ?$
- Fattorizzazione (scomposizione in fattori primi) di numeri grandi con fattori grandi (dato un numero intero positivo esiste una sola sequenza di numeri primi uguale al numero dato)
- Il tutto complicato nell'operare in algebra mod  $n$

# Crittografia a chiave pubblica

- **usato per distribuire chiavi segrete e per la firma elettronica**
- **RSA (Rivest - Shamir - Adleman)**
  - brevettato da RSA
- **DSA (Digital Signature Algorithm)**
  - standard
- **Diffie-Hellman**
  - scambio chiavi

# Ognuno ha la sua coppia di chiavi asimmetriche..



***Chiave  
privata  
di marco***



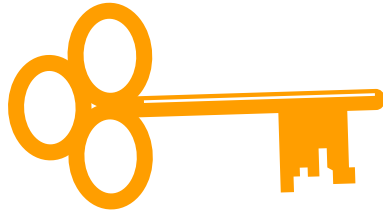
***Chiave  
privata  
di giulia***

***Chiave  
pubbliche  
di marco***

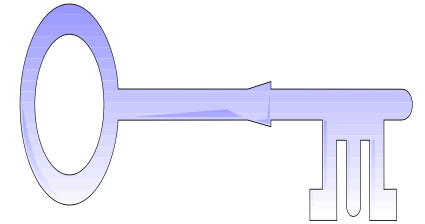


***Chiave  
pubblica  
di giulia***

# Crittografia a chiavi asimmetriche



**chiave pubblica**



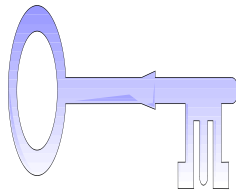
**chiave  
privata**



# La serratura ... asimmetrica



**Se chiudo con la chiave**



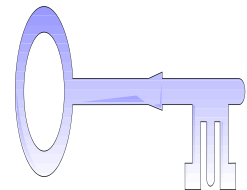
**apro solo**



**Se chiudo con la chiave**



**apro solo**



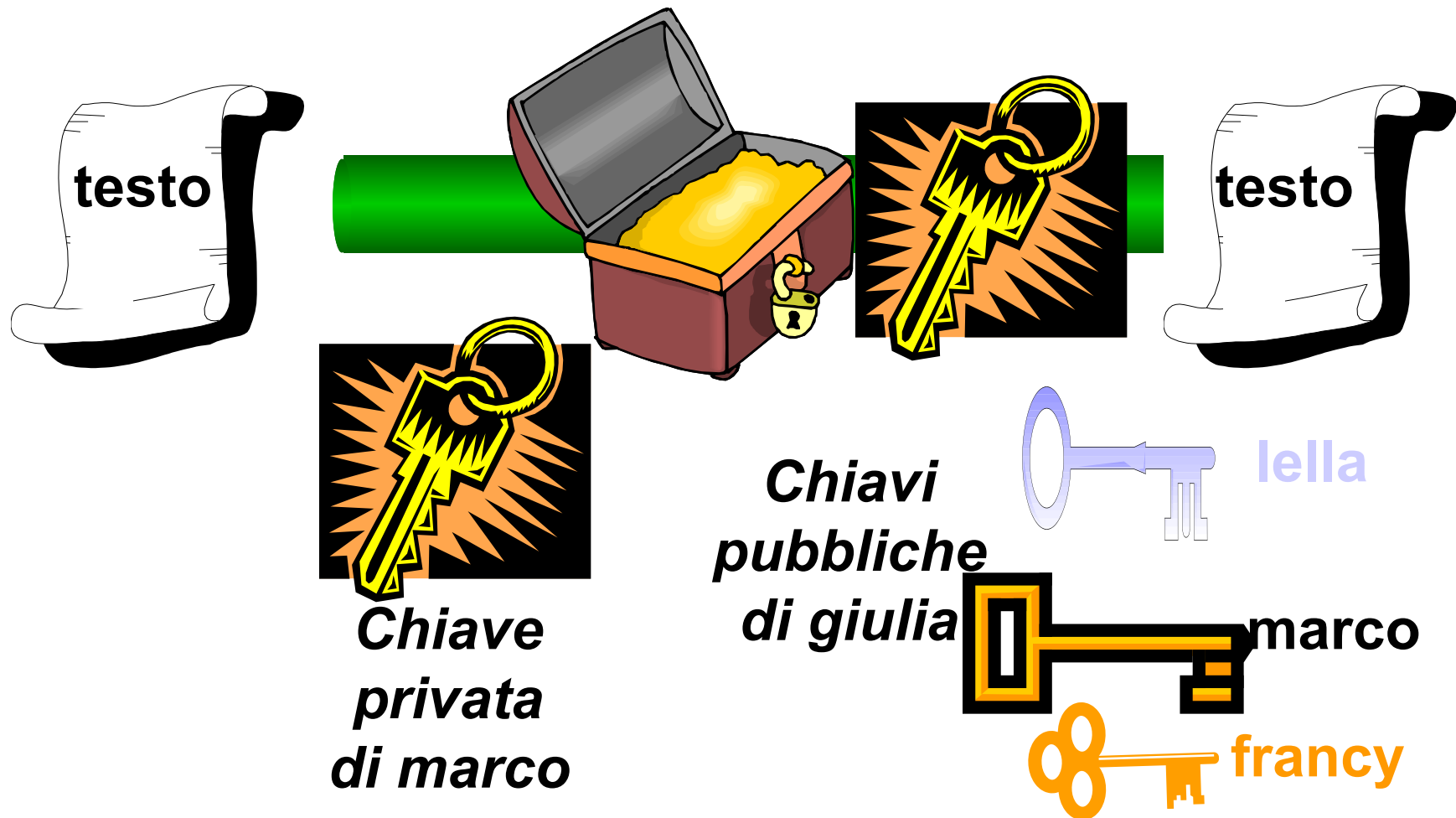
# Segretezza (la trasmissione della carta di credito) (*messaggio da marco a giulia*)



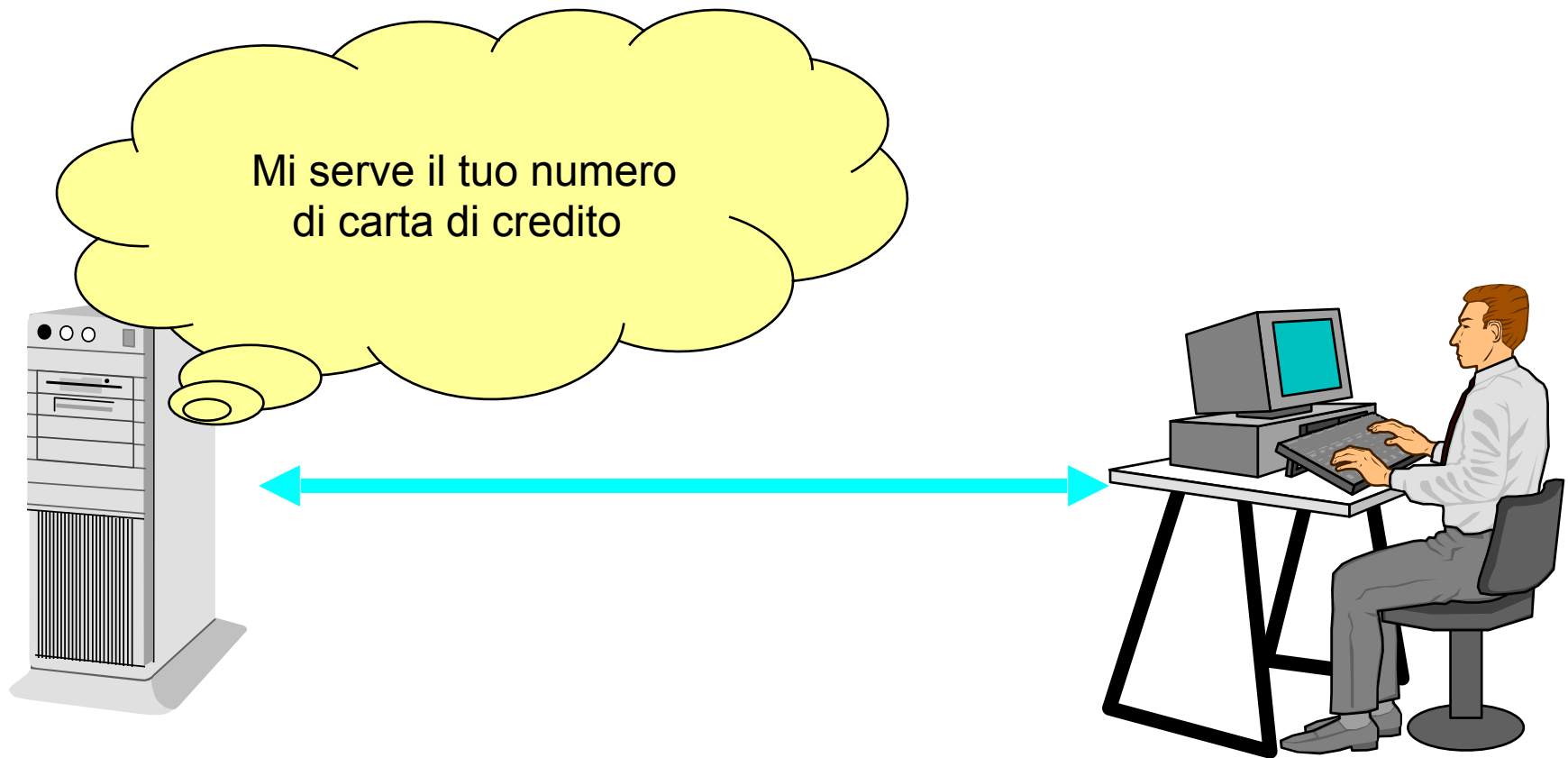


# Autenticazione (la firma digitale)

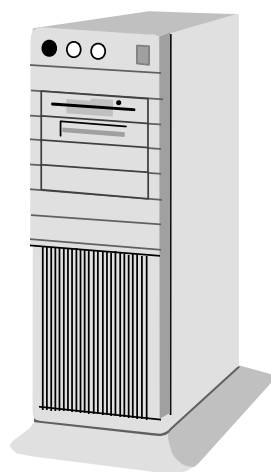
*(di un messaggio da marco a giulia)*



# Canale sicuro



# Canale sicuro



**Kpub**  
**Kpri**

1. Kpub



2.

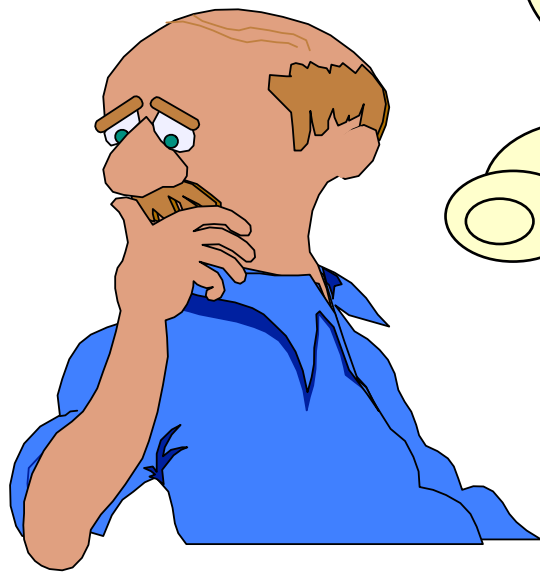


# Firma digitale

Documenti digitali  
Contratti digitali  
Posta elettronica certificata (pec)  
Autenticazione siti web (https)  
Certificazione software (app)



## Il dilemma



**1. Dove trovo la Kpub ?**

**2. Chi mi garantisce  
che sia proprio lui?**

# Certificato a chiave pubblica

- La sola firma con una coppia di chiavi non mi garantisce la *corrispondenza con un soggetto fisico*



Chi è Marco?  
Sarà proprio  
la firma di Marco ?



# Certificato a chiave pubblica

- È necessario un *certificato d'autenticità* che garantisca in modo esplicito l'identità del soggetto **SIGILLO**



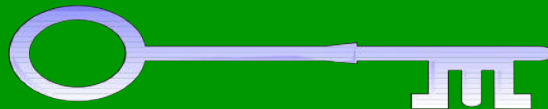
**Riconosco  
il timbro?**



*In God we trust ....*

*... All Other must submit an X.509  
certificate*

Certifico che la seguente è  
la chiave pubblica di  
Mezzalama:



**Firmato: il presidente  
MATTARELLA**



# Autorità di certificazione

Una autorità accreditata da un insieme di utenti per creare ed assegnare certificati a chiave pubblica





**GRAZIE!**

