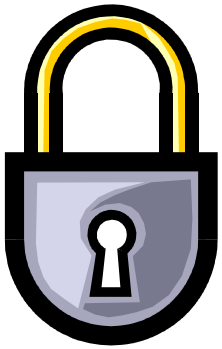


Sicurezza in Rete

Luigi Vetrano

TechnoLabs S.p.A.

http://www.hiperlab.org/univaq

L'Aquila, Gennaio 2011

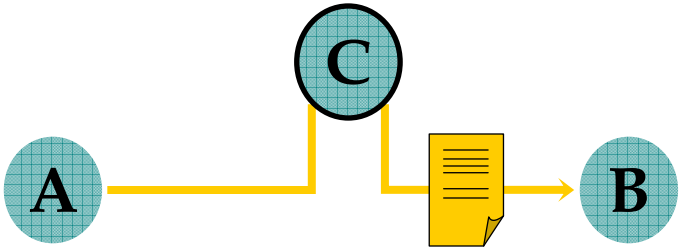
Definizione di Sicurezza Informatica

- Sicurezza:
  - ‘Assenza’ di rischio o pericolo
- Sicurezza Informatica
  - Prevenzione o protezione contro,
    - Accesso, distruzione o alterazione di risorse/informazioni da parte di utenti non autorizzati

Sicurezza Informatica

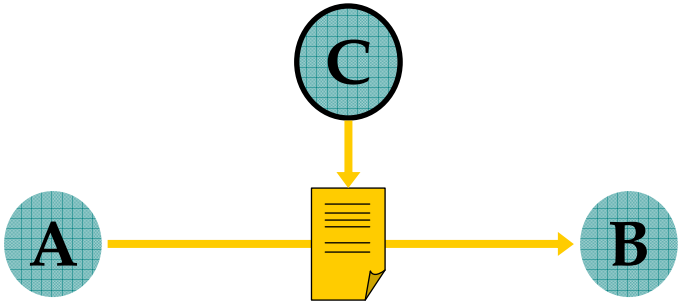
- Abilità di un sistema di proteggere informazioni, risorse ed il sistema stesso, rispetto alle nozioni di
  - Confidentialità (confidentiality)
  - Integrità (integrity)
  - Autenticazione (authentication)
  - Controllo degli Accessi (control access)
  - Non ripudio (non-repudiaton)
  - Disponibilità (availability)
  - Privatezza (privacy)

Le principali minacce nello scambio messaggi

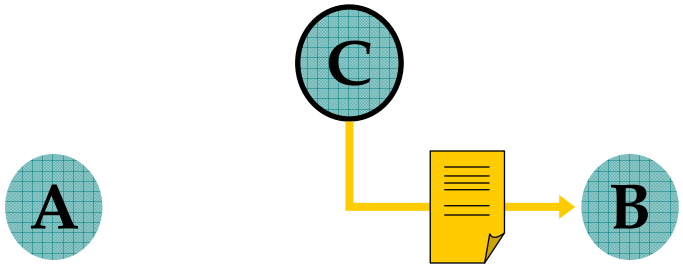


Intercettare un messaggio e leggere il suo contenuto

Negare di aver inviato un messaggio



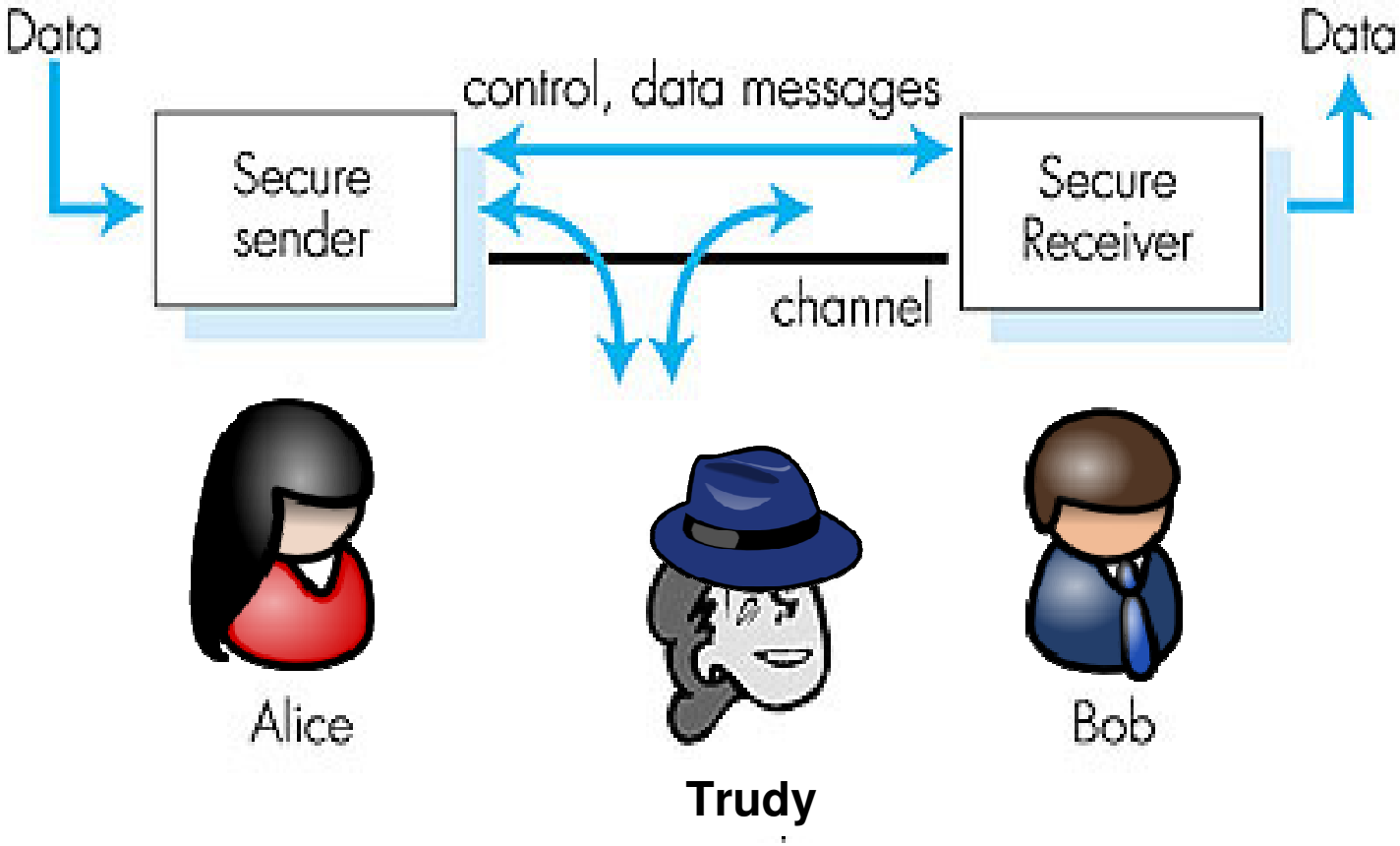
Modificare il contenuto di un messaggio



Inviare un messaggio sotto falso nome

TechnoLabs

Q: Perché c'è una esigenza di sicurezza?



Sender, receiver, intruder (Alice, Bob, Trudy)

A: Insecure Channel

Sicurezza dei protocolli di rete

- Il protocollo attualmente più diffuso è il TCP/IP.
- Il protocollo TCP/IP ha delle debolezze innate: fu creato nel 1974 pensando all'efficienza delle connessioni e non alla sicurezza.
- Queste debolezze permettono attacchi di diverso tipo.

Attacchi passivi o attivi

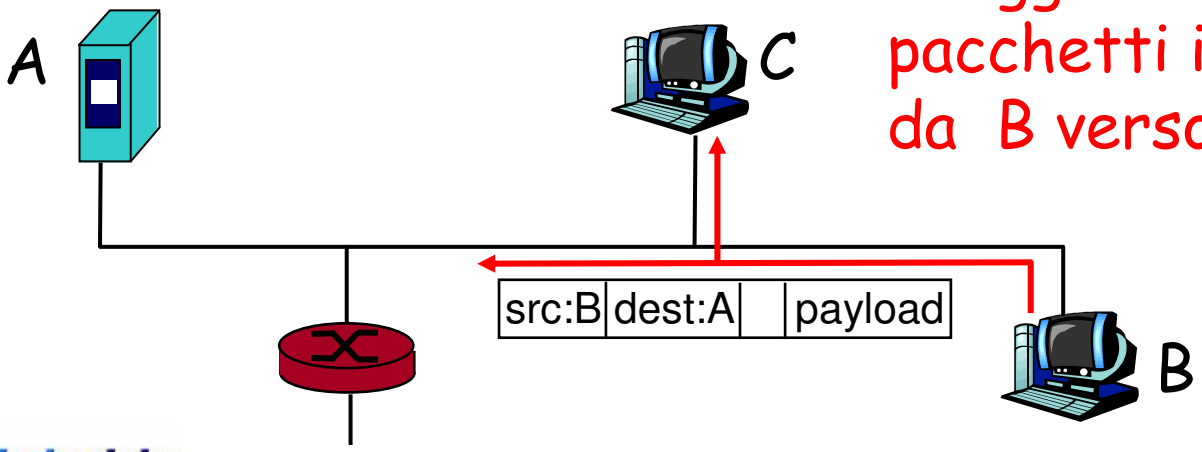
- **Attacco passivo**: sottrarre informazioni senza interferire sul sistema
- **Attacco attivo**: interferire sul sistema con vari scopi

Nota: Classificazione storica: oggi sono praticamente tutti attivi

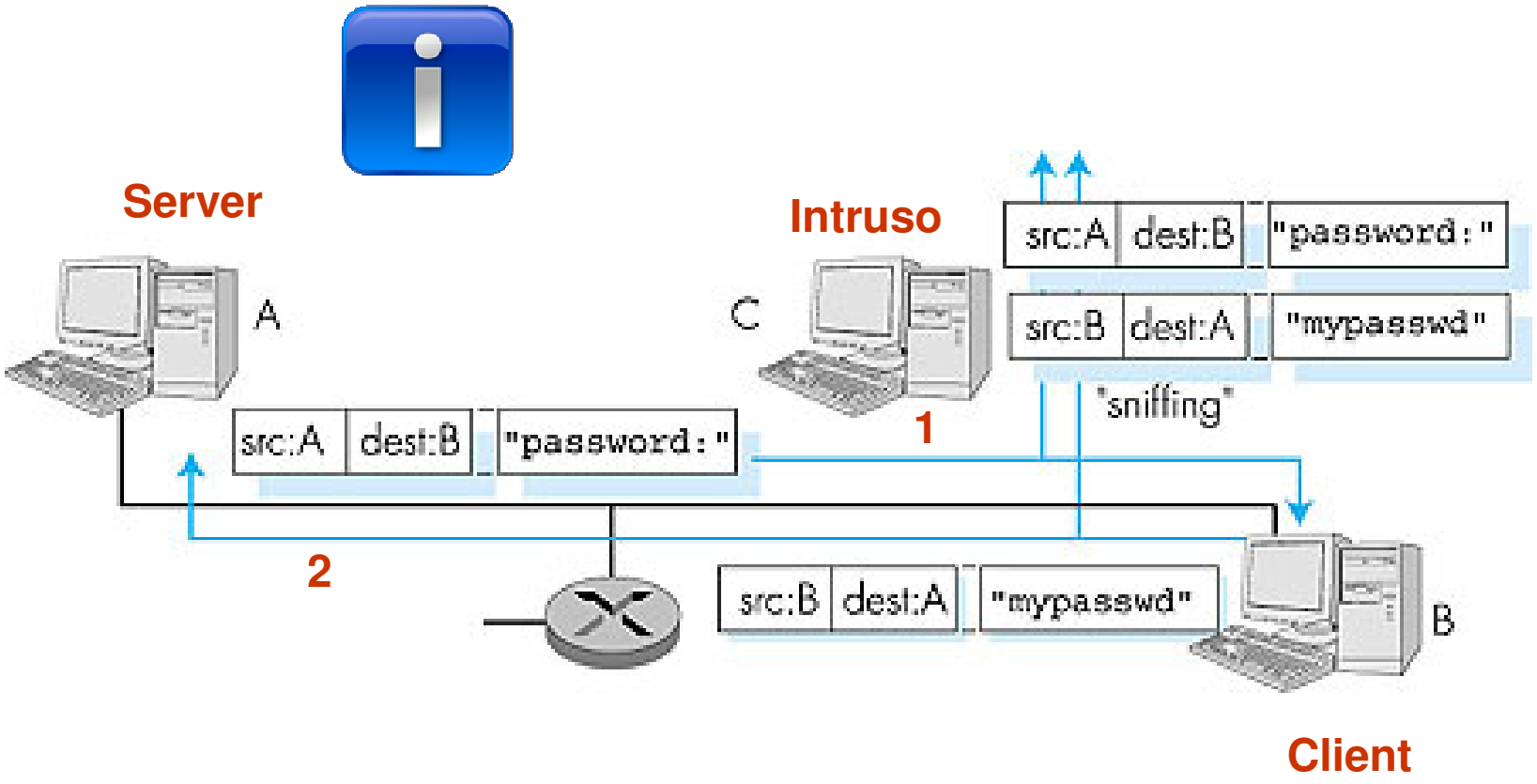
Minacce alla sicurezza in Internet

Packet sniffing (to sniff = “odorare”):

- Evidente in mezzi condivisi
- Un adattatore di rete (NIC) programmato ad hoc (promiscuous mode) legge tutti i pacchetti in transito
- Tutti i dati non cifrati (es.: password) possono essere letti



Sessione Telnet

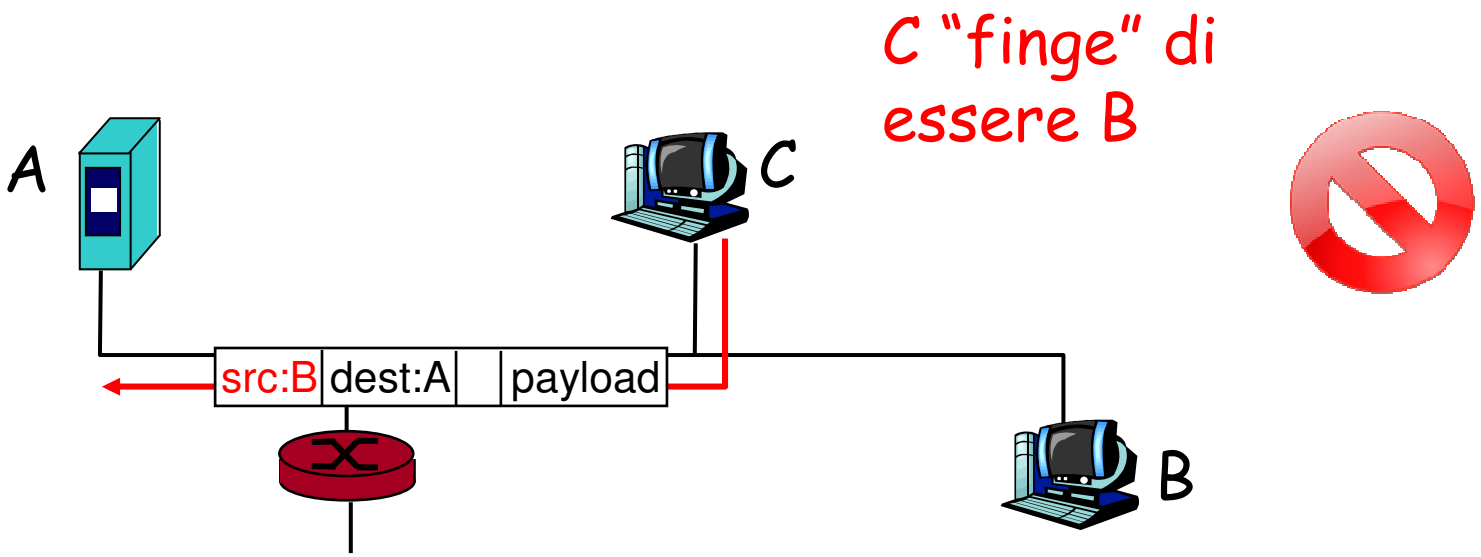


Packet sniffing

Minacce alla sicurezza (cont.)

IP Spoofing:

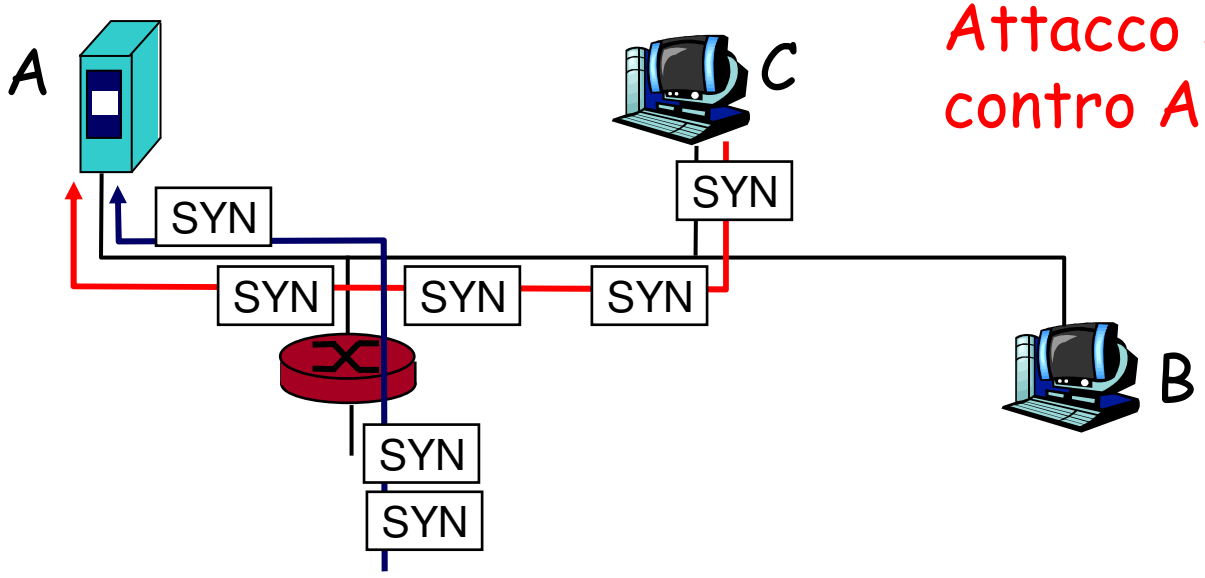
- Un host genera pacchetti IP con indirizzi di sorgente falsi
- Il ricevente non è in grado di stabilire se l'origine dei pacchetti sia quella autentica



Minacce alla sicurezza (cont.)

Denial of service (DoS):

- Flusso di pacchetti “maligni” che sommerge il ricevente
- Distributed DoS (DDoS): attacco coordinato multiplo

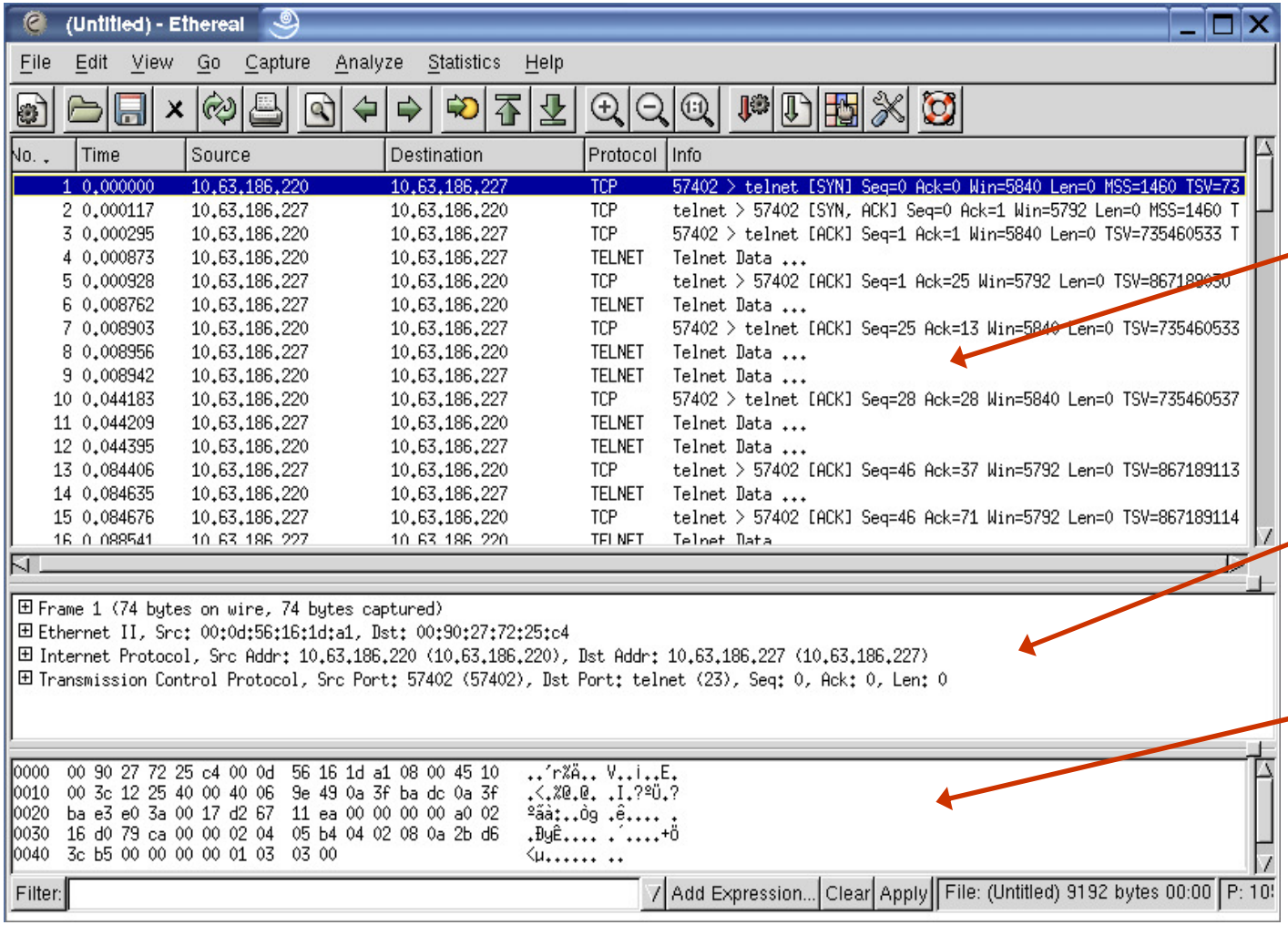


TechnoLabs

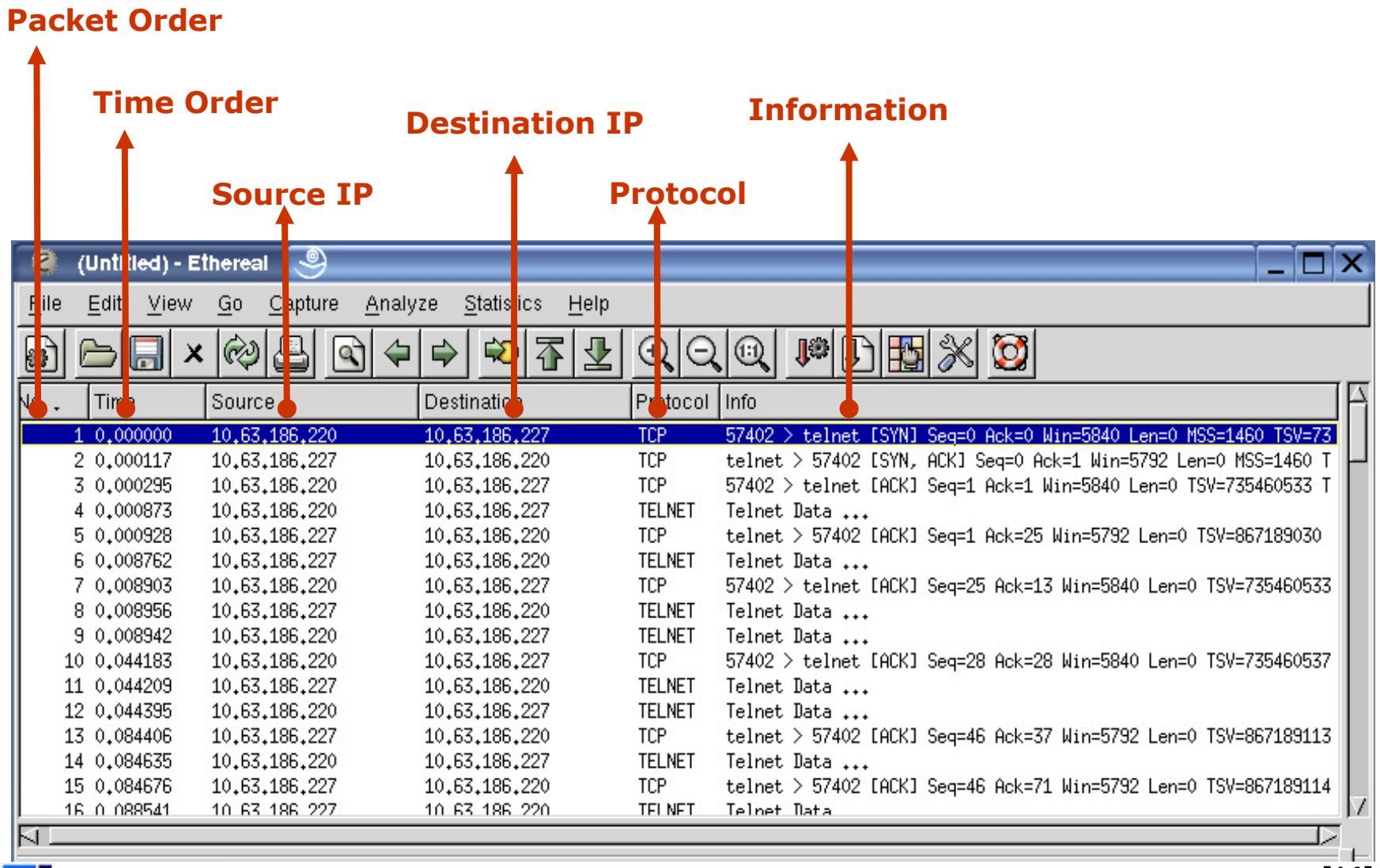
Strumenti Utilizzati

- Wireshark → Network Analyzer
  - Analizza traffico di rete
  - In grado di catturare pacchetti indirizzati ad altri host (Promiscous_Mode)
  - Qualsiasi protocollo anche proprietario (plug-in)
  - Packet Filtering

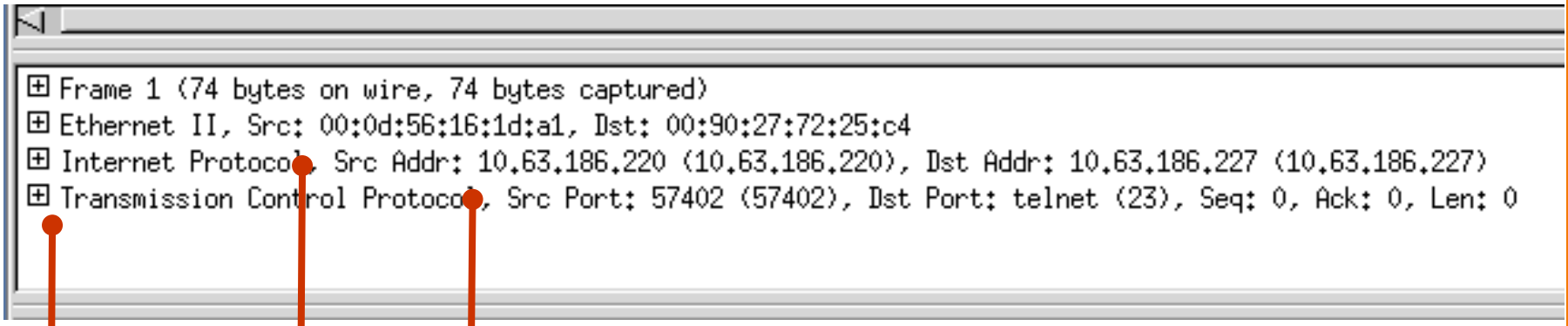
Screenshot di Ethereal



Packet List


Packet Order
Time Order
Source IP
Destination IP
Protocol
Information
(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
No. Time Source Destination Protocol Info
1 0.000000 10.63.186.220 10.63.186.227 TCP 57402 > telnet [SYN] Seq=0 Ack=0 Win=5840 Len=0 MSS=1460 TSV=73
2 0.000117 10.63.186.227 10.63.186.220 TCP telnet > 57402 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 T
3 0.000295 10.63.186.220 10.63.186.227 TCP 57402 > telnet [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSV=735460533 T
4 0.000873 10.63.186.220 10.63.186.227 TELNET Telnet Data ...
5 0.000928 10.63.186.227 10.63.186.220 TCP telnet > 57402 [ACK] Seq=1 Ack=25 Win=5792 Len=0 TSV=867189030
6 0.008762 10.63.186.227 10.63.186.220 TELNET Telnet Data ...
7 0.008903 10.63.186.220 10.63.186.227 TCP 57402 > telnet [ACK] Seq=25 Ack=13 Win=5840 Len=0 TSV=735460533
8 0.008956 10.63.186.227 10.63.186.220 TELNET Telnet Data ...
9 0.008942 10.63.186.220 10.63.186.227 TELNET Telnet Data ...
10 0.044183 10.63.186.220 10.63.186.227 TCP 57402 > telnet [ACK] Seq=28 Ack=28 Win=5840 Len=0 TSV=735460537
11 0.044209 10.63.186.227 10.63.186.220 TELNET Telnet Data ...
12 0.044395 10.63.186.227 10.63.186.220 TELNET Telnet Data ...
13 0.084406 10.63.186.227 10.63.186.220 TCP telnet > 57402 [ACK] Seq=46 Ack=37 Win=5792 Len=0 TSV=867189113
14 0.084635 10.63.186.220 10.63.186.227 TELNET Telnet Data ...
15 0.084676 10.63.186.227 10.63.186.220 TCP telnet > 57402 [ACK] Seq=46 Ack=71 Win=5792 Len=0 TSV=867189114

Packet Details

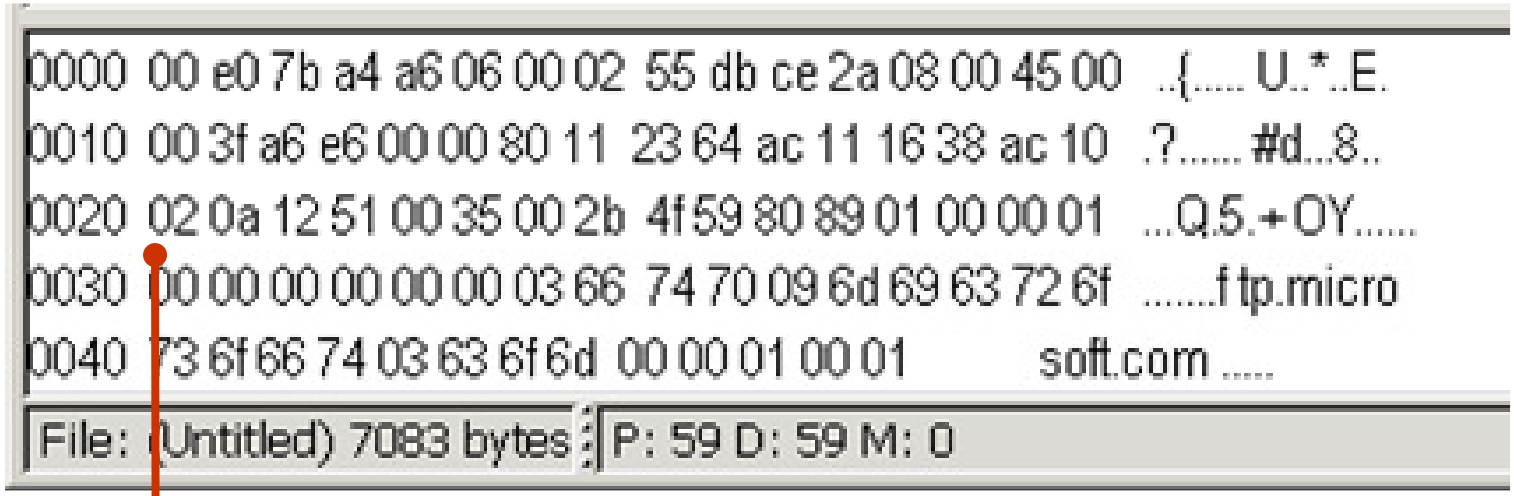


Source and Destination TCP Ports

Source and Destination IP

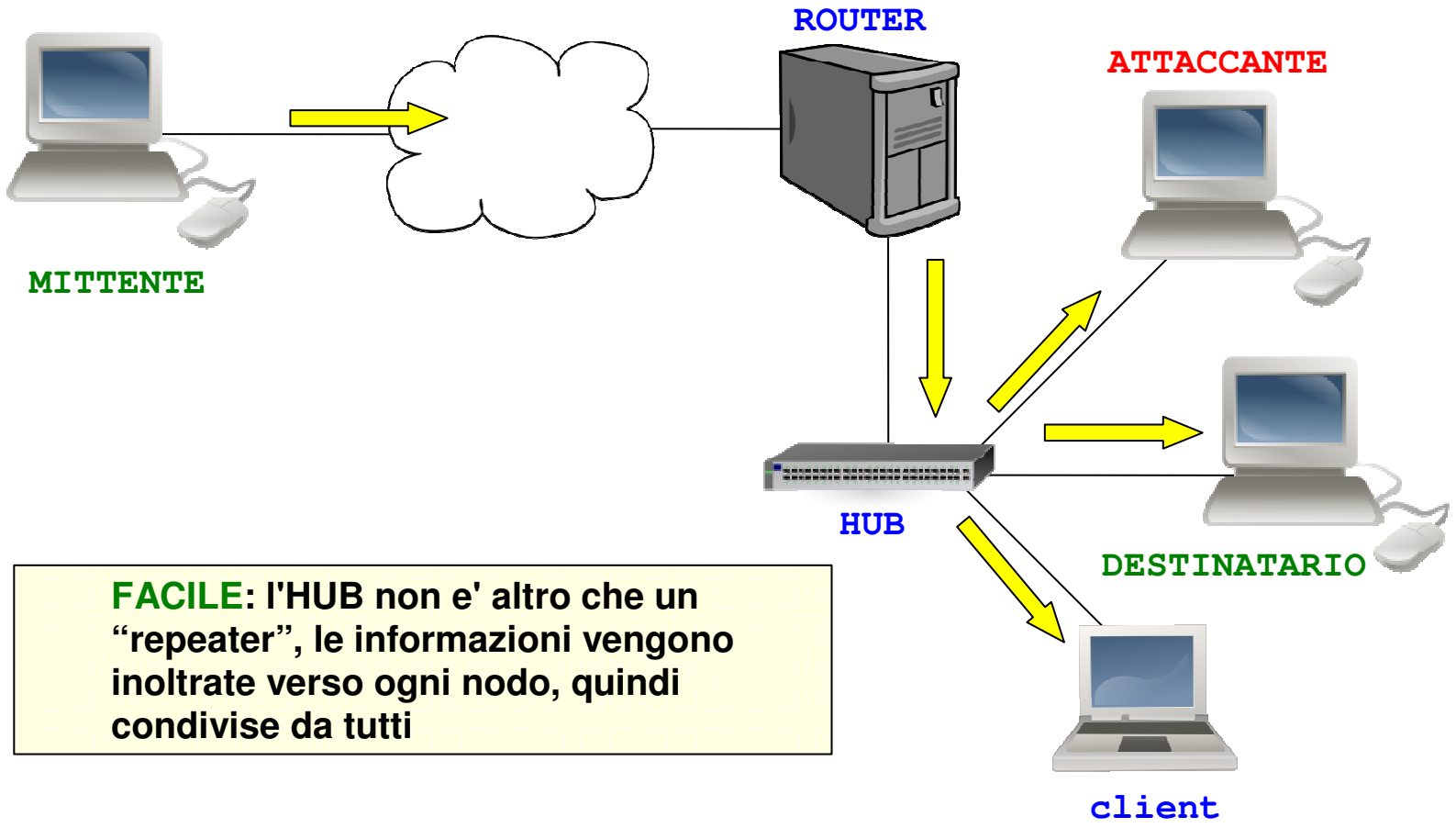
Breakdown of the Frame, the Packet, the TCP segment

Packet Bytes



Vista dei dati – Esadecimale e Raw

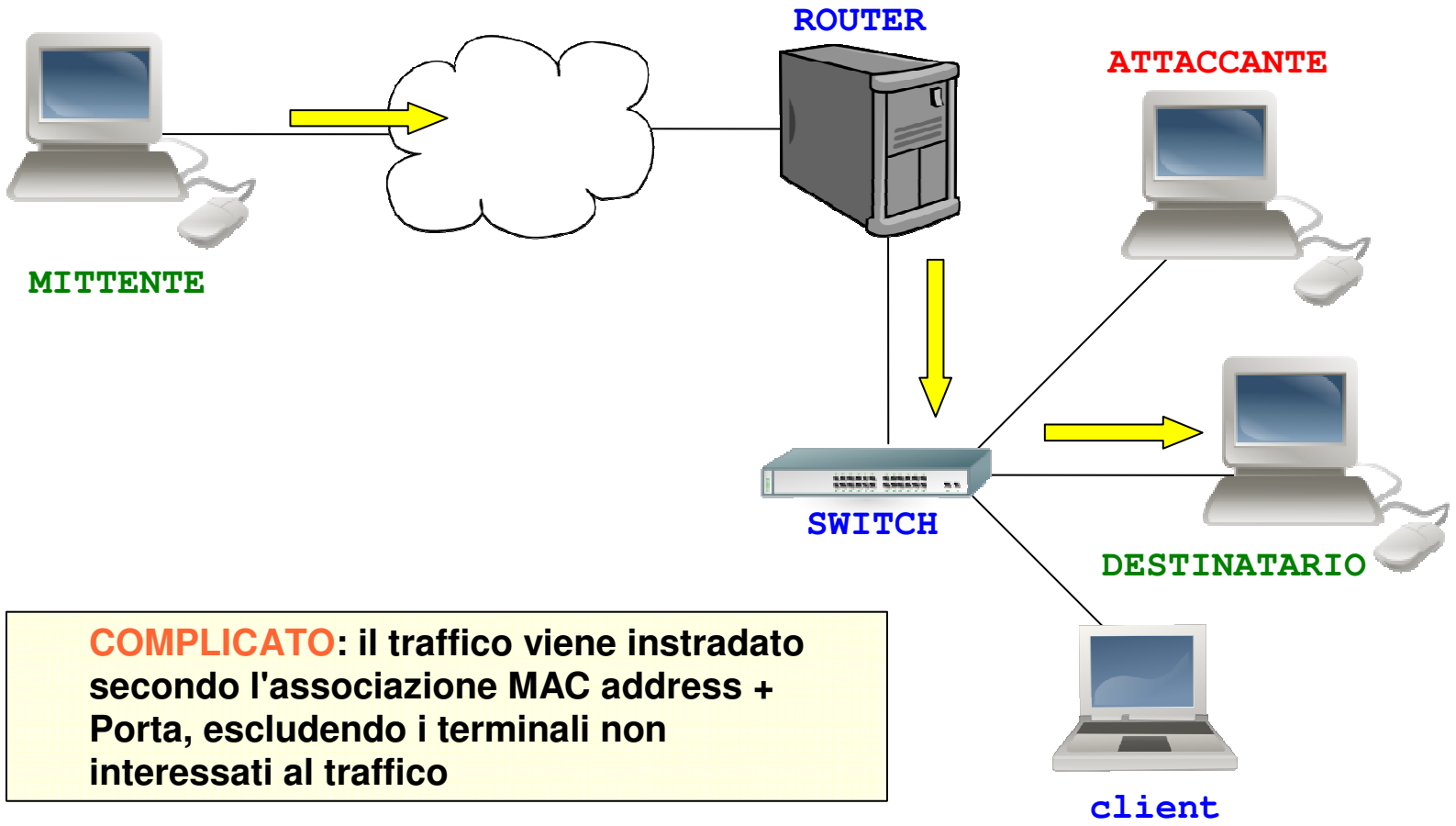
Sniffing su reti non-switchate



FACILE: l'HUB non e' altro che un "repeater", le informazioni vengono inoltrate verso ogni nodo, quindi condivise da tutti

TechnoLabs

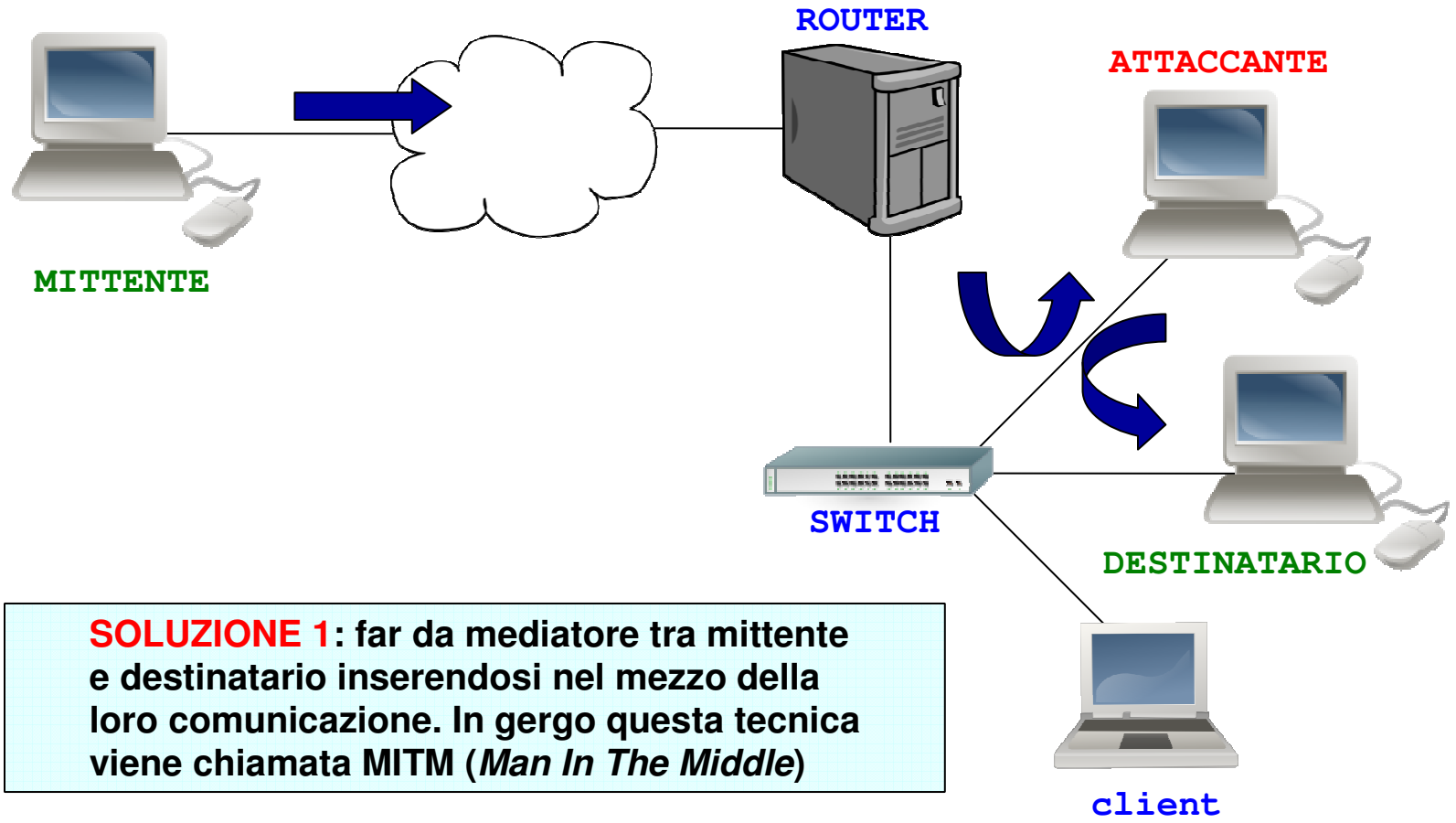
Sniffing su reti switchate



COMPLICATO: il traffico viene instradato secondo l'associazione MAC address + Porta, escludendo i terminali non interessati al traffico

TechnoLabs

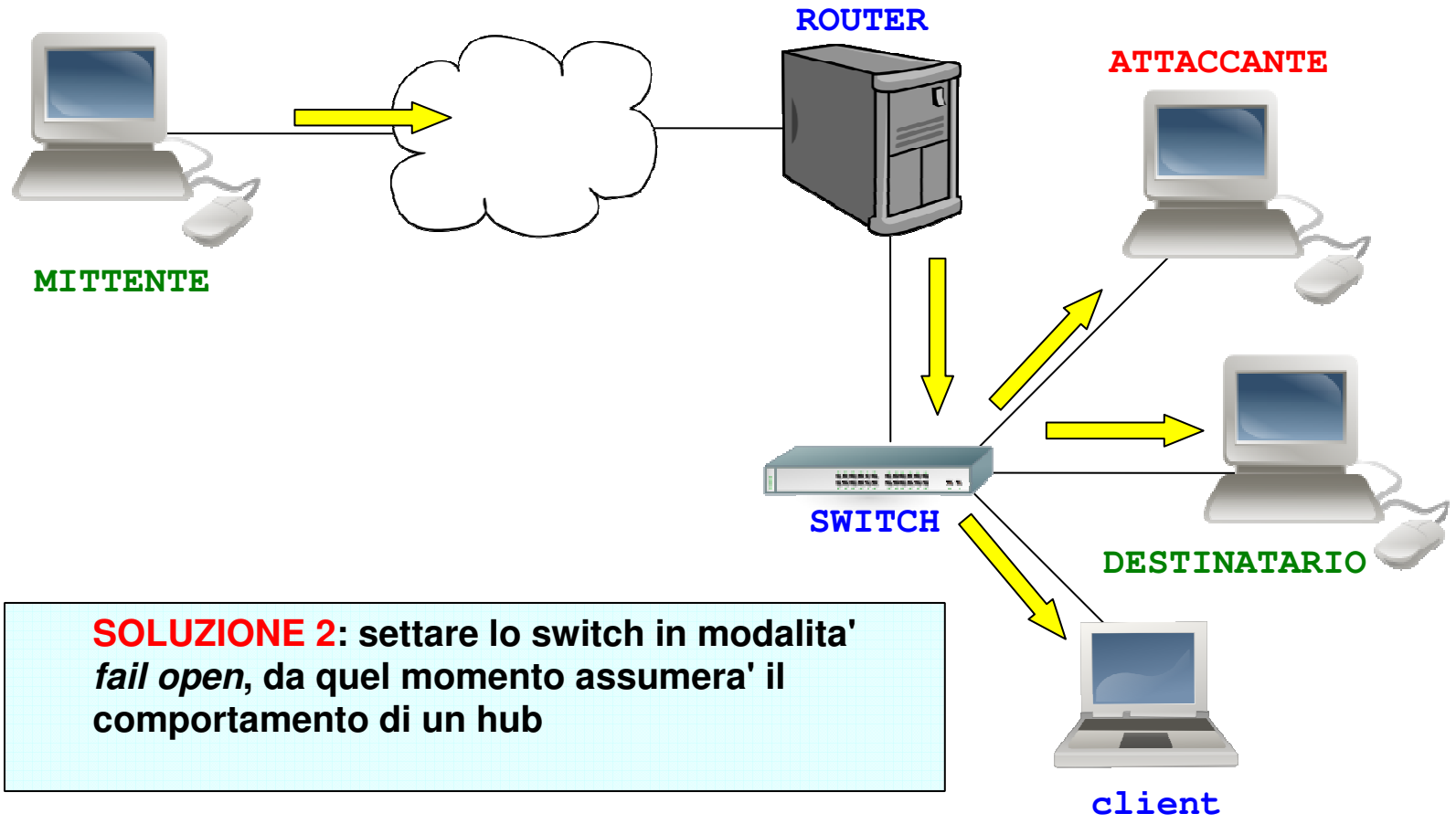
Sniffing su reti switchate



SOLUZIONE 1: far da mediatore tra mittente e destinatario inserendosi nel mezzo della loro comunicazione. In gergo questa tecnica viene chiamata MITM (*Man In The Middle*)

TechnoLabs

Sniffing su reti switchate

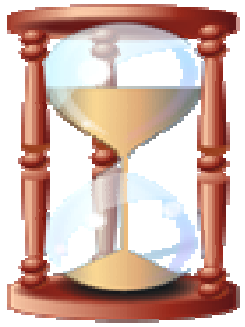


SOLUZIONE 2: settare lo switch in modalita' *fail open*, da quel momento assumera' il comportamento di un hub

TechnoLabs

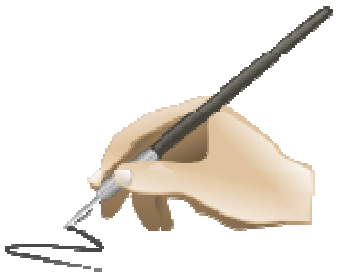
Next

- Avendo stabilito il framework, la terminologia, alcune delle definizioni più rilevanti, i tools e la necessità per “network security”, introduciamo ora I concetti fondamentali della crittografia, un argomento di centrale importanza per diversi aspetti di sicurezza.



La crittografia

Crittografia deriva dal greco *kryptós* (nascosto) e da *gráphein* (scrittura), quindi “scrittura nascosta”.



Rientra nell'universo della *confidenzialita'* ed e' un ottimo metodo per comunicare informazioni riservate.

Il suo utilizzo ha origini molto antiche, il primo (si dice) fu Cesare nell'antica Roma, e tutt'oggi e' alla base di tutte le comunicazioni segrete (soprattuto militari).

TechnoLabs

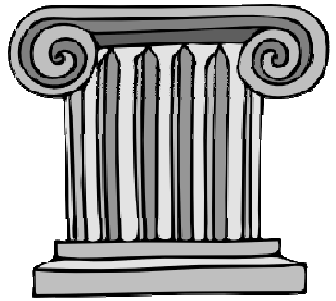
Storia della crittografia

La crittografia è un scienza molto antica:

- Mesopotamia: Assiri e Babilonesi (scritture cuneiformi): usavano sostituire parti terminali delle parole
- Bibbia: Atbash (alfabeto rovesciato), cifratura di Babilonia nel libro di Geremia
- India, Kama Sutra: tra le 64 arti la 45-esima Mlecchita-vikalpa, che le donne devono conoscere
- Plutarco, Vite parallele: gli spartani usavano la Scytala (cilindro su cui si arrotolava la pergamena)

Il cifrario di Cesare [cenni storici]

Il cifrario utilizzato da Cesare per comunicare in segretezza alle proprie truppe le strategie di guerra



TESTO IN CHIARO

A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z
D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z	A	B	C

CHIAVE (+3)

messaggio : **C I A**

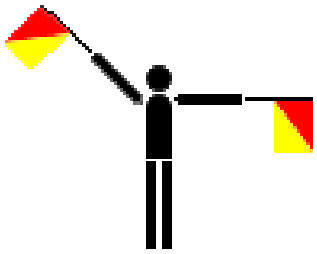
messaggio cifrato : **O**

F N D R

Cifrario detto anche “a scorrimento”.
Della stessa serie e' anche ROT13 che usa un *offset* di +13

TechnoLabs

Il quadrato di Polibio [cenni storici]



CHIAVE

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

TESTO IN CHIARO

messaggio : C I A O

coordinate: (1,3) (2,4) (1,1) (3,4)

lettura in riga:

riaccoppiamento 1 2 1 3 3 4 1 4

messaggio cifrato : (1,2) (1,3) (3,4) (1,4)

B C O D

E' un primo approccio al concetto di diffusione, sul quale si basano molti degli algoritmi di cifratura moderni.

TechnoLabs

Storia della crittografia

Sostituzione di cifra

Permutazione del testo:

- Scrivi il messaggio in blocchi di lunghezza fissa
- Riordina le lettere usando la chiave

Esempio: **Nel mezzo del cammin di nostra vita..**

Chiave: **domani**

264153	123456
nelmez	mnzlee
zodelc	ezcdlo
ammind	iadmnm

Cifrario di Porta

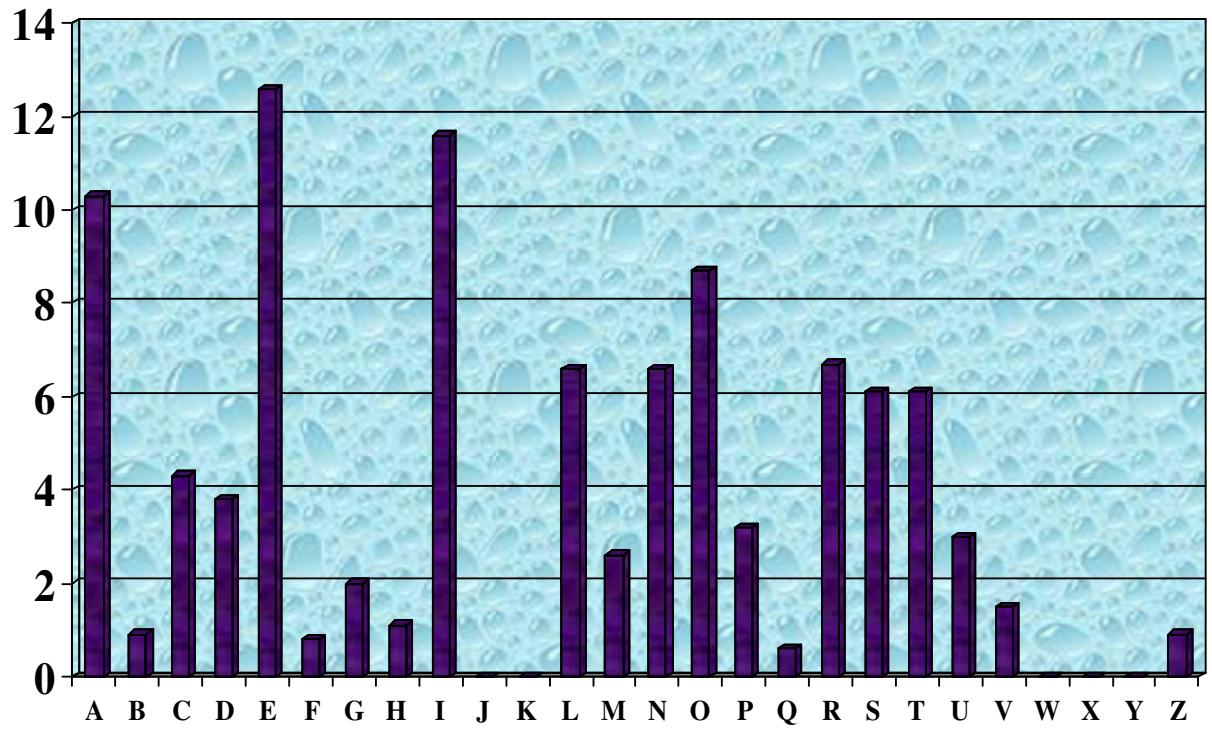
Giovanni Battista Porta, primo cifrario per digrammi [1563]

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
B	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51
C	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77
D	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100	101	102	103
E	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127	128	129
F	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155
G	156	157	158	159	160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181
H	182	183	184	185	186	187	188	189	190	191	192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207
I	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223	224	225	226	227	228	229	230	231	232	233
J	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255	256	257	258	259
K	260	261	262	263	264	265	266	267	268	269	270	271	272	273	274	275	276	277	278	279	280	281	282	283	284	285
L	286	287	288	289	290	291	292	293	294	295	296	297	298	299	300	301	302	303	304	305	306	307	308	309	310	311
M	312	313	314	315	316	317	318	319	320	321	322	323	324	325	326	327	328	329	330	331	332	333	334	335	336	337
N	338	339	340	341	342	343	344	345	346	347	348	349	350	351	352	353	354	355	356	357	358	359	360	361	362	363
O	364	365	366	367	368	369	370	371	372	373	374	375	376	377	378	379	380	381	382	383	384	385	386	387	388	389
P	390	391	392	393	394	395	396	397	398	399	400	401	402	403	404	405	406	407	408	409	410	411	412	413	414	415
Q	416	417	418	419	420	421	422	423	424	425	426	427	428	429	430	431	432	433	434	435	436	437	438	439	440	441
R	442	443	444	445	446	447	448	449	450	451	452	453	454	455	456	457	458	459	460	461	462	463	464	465	466	467
S	468	469	470	471	472	473	474	475	476	477	478	479	480	481	482	483	484	485	486	487	488	489	490	491	492	493
T	494	495	496	497	498	499	500	501	502	503	504	505	506	507	508	509	510	511	512	513	514	515	516	517	518	519
U	520	521	522	523	524	525	526	527	528	529	530	531	532	533	534	535	536	537	538	539	540	541	542	543	544	545
V	546	547	548	549	550	551	552	553	554	555	556	557	558	559	560	561	562	563	564	565	566	567	568	569	570	571
W	572	573	574	575	576	577	578	579	580	581	582	583	584	585	586	587	588	589	590	591	592	593	594	595	596	597
X	598	599	600	601	602	603	604	605	606	607	608	609	610	611	612	613	614	615	616	617	618	619	620	621	622	623
Y	624	625	626	627	628	629	630	631	632	633	634	635	636	637	638	639	640	641	642	643	644	645	646	647	648	649
Z	650	651	652	653	654	655	656	657	658	659	660	661	662	663	664	665	666	667	668	669	670	671	672	673	674	675

Cifrario di Porta

testo in chiaro:	**DO**	**MA**	**NI**
testo cifrato:	**92**	**312**	**346**

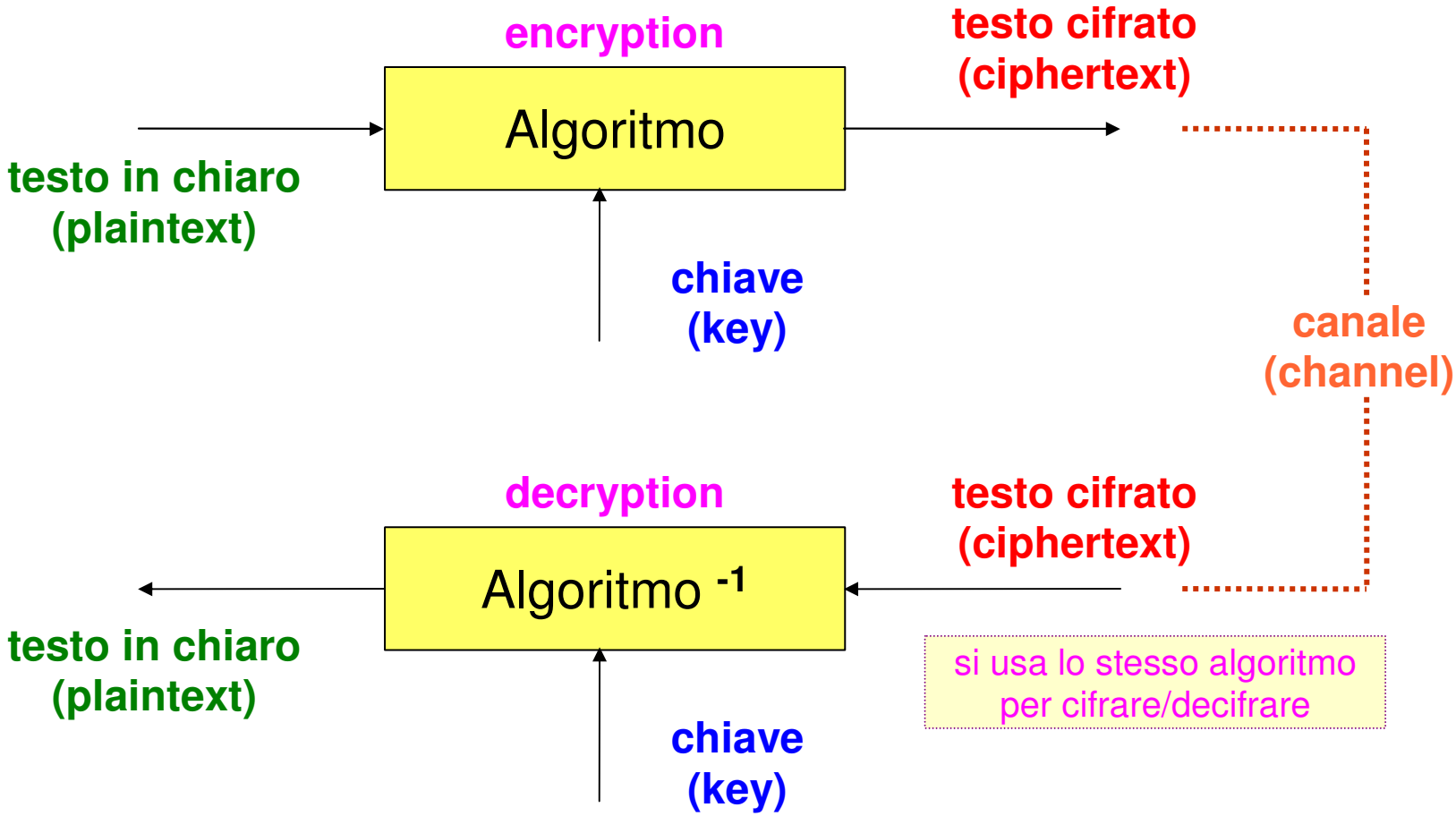
Frequenze di occorrenze lettere



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
italiano	10,3	0,9	4,3	3,8	12,6	0,8	2,0	1,1	11,6	0,0	0,0	6,6	2,6	6,6	8,7	3,2	0,6	6,7	6,1	6,1	3,0	1,5	0,0	0,0	0,0	0,9
inglese	7,3	1,3	3,5	4,3	12,8	3,0	2,0	3,5	7,8	0,3	0,5	3,7	2,8	7,8	7,5	2,8	0,5	8,5	6,0	9,3	3,0	1,5	1,5	0,5	2,3	0,3
francese	8,3	1,3	3,3	3,8	17,8	1,3	1,3	1,3	7,3	0,8	0,0	5,8	3,2	7,2	5,7	3,7	1,2	7,3	8,3	7,2	6,3	1,8	0,0	0,0	0,8	0,0

Crittografia: nomenclatura

Schema a blocchi:



TechnoLabs

Sicurezza di un algoritmo

La sicurezza in crittografia è valutata in base alle risorse di tempo e di calcolo necessarie per dedurre informazioni

- *ogni protocollo crittografico puo' essere "rotto" con sufficienti risorse di tempo e calcolo*
- *se un algoritmo puo' essere "rotto" usando per 30 anni un sistema di calcolo del valore di 10 miliardi di Euro allora puo' essere ritenuto sicuro*.

La sicurezza di un algoritmo dipende dal campo di applicazione.

Sicurezza di un algoritmo

- La sicurezza di un protocollo dipende anche dal numero di possibili chiavi:
  - se ci sono molte possibili chiavi allora ci vuole molto tempo (o molta fortuna) per trovare la chiave segreta:
    - 20 bit (circa 1 milione di diverse chiavi) allora non e' affatto sicuro
    - 56 bit (circa 66 milioni di miliardi diverse chiavi) andava bene dieci anni fa ma oggi e' "poco" sicuro
    - 512 bit (piu' di 40000000….0000000000 - 4 seguito da 153 zeri - diverse chiavi) oggi e' sicuro; domani?

Grandi Numeri

- Colonne Enalotto $622.614.630 = 1.15 \times 2^{29}$
- Secondi dalla creazione del sistema solare 1.38×2^{57}
- Cicli in un secolo di una macchina a 2 GHz 2.7×2^{61}
- Cicli in un secolo di 1M di macchine a 2 GHz 2.7×2^{81}
- Numeri primi di 249 bit 1.8×2^{244}
- Elettroni nell'universo 1.8×2^{258}

Sicurezza di un algoritmo

La Crittoanalisi studia le modalità di attacco dei protocolli crittografici

Diversi tipi di attacco basati su

- ***Conoscenza*** *di testo cifrato*
- ***Conoscenza*** *testo in chiaro e corrispondente testo cifrato*
- ***Scelta*** *di testo in chiaro e conoscenza del corrispondente testo cifrato*
- ***Scelta*** *di testo crittato e conoscenza del corrispondente testo in chiaro*

Principio di Kerckhoffs':

"La sicurezza di un sistema crittografico deve dipendere solo dalla segretezza della chiave e non dalla segretezza del metodo" Jean Guillaume Hubert Victor Francois Alexandre Auguste Kerckhoffs von Nieuwenhof (1835-1903), "*La Cryptographie militaire*", 1883.

Quanto è complesso "rompere" un codice?:

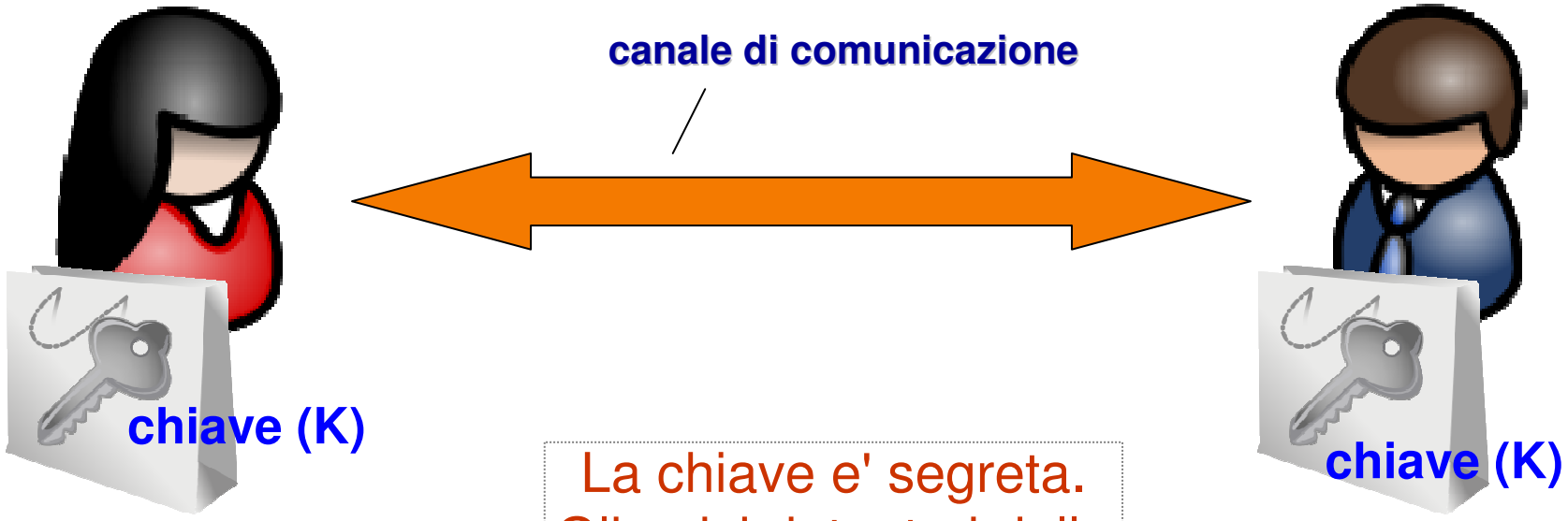
- forza bruta: se il numero di chiavi e' piccolo: il codice si "rompe" facilmente con un computer
- altri sistemi? (attacchi basati sulla conoscenza dell'algoritmo di cifratura)

Algoritmi di crittografia

- Gli algoritmi di crittografia possono essere classificati come
  - **simmetrici**, anche detti ***a chiave segreta*** *(o* ***privata***): usano la stessa chiave per codificare e decodificare
  - **asimmetrici**, anche detti ***a chiave pubblica:*** usano due chiavi distinte: una per codificare e una per decodificare***.***
- Tutti codificano il testo a blocchi (es. 64, 128 byte)

La cifratura a chiave simmetrica

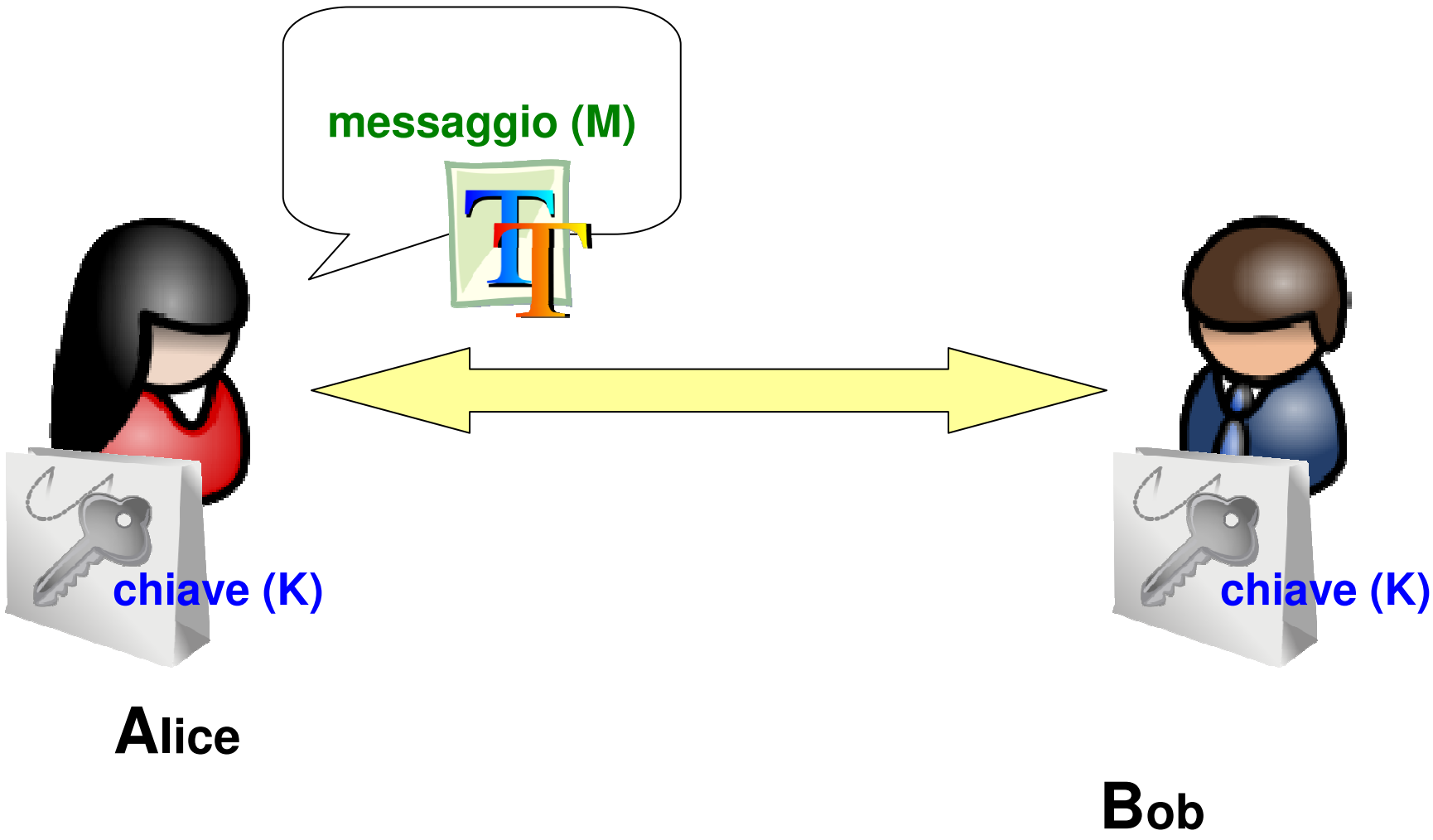
Soluzione basata su chiave segreta



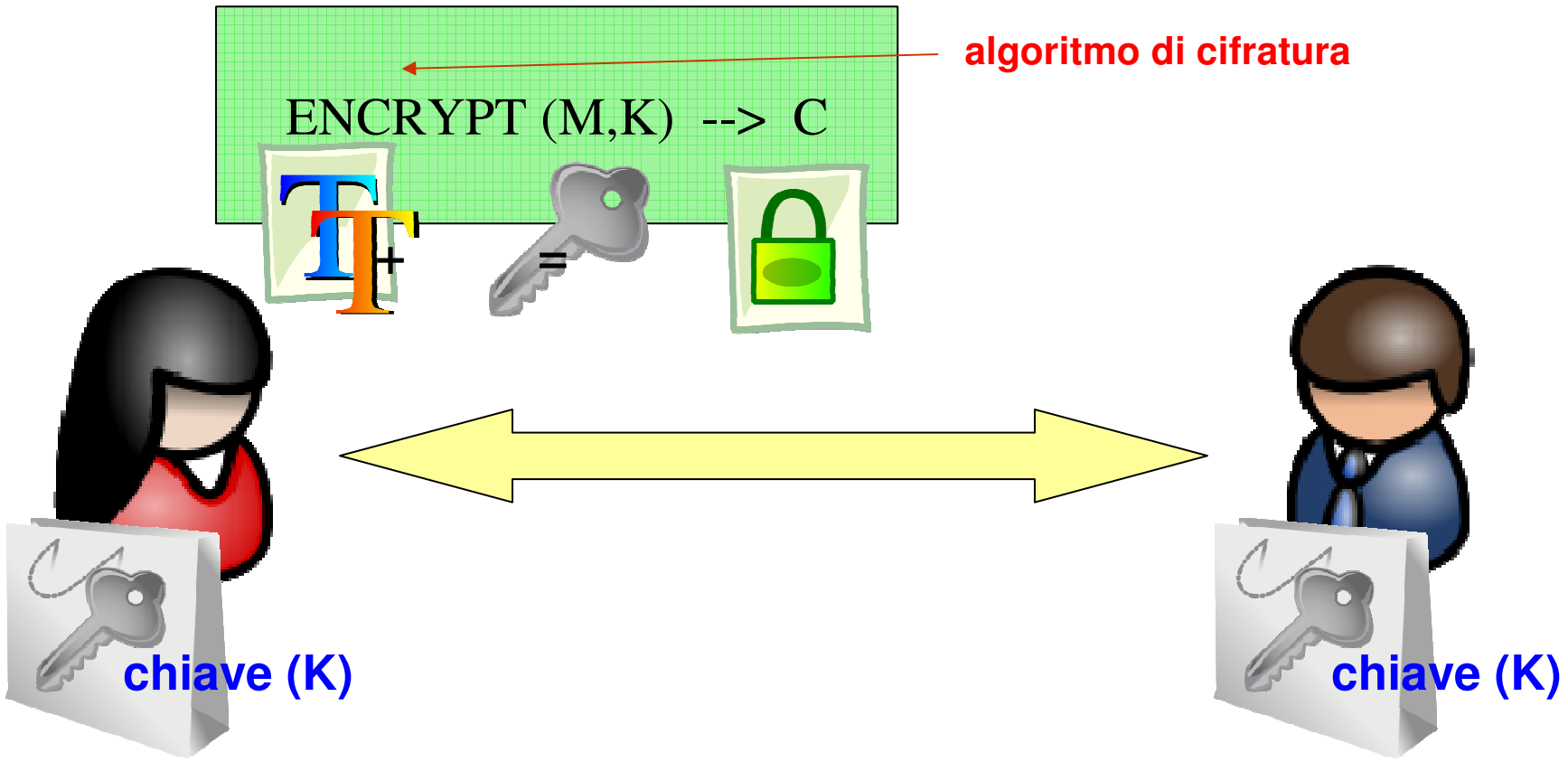
La chiave e' segreta. Gli unici detentori della chiave sono Alice e Bob

TechnoLabs

La cifratura a chiave simmetrica

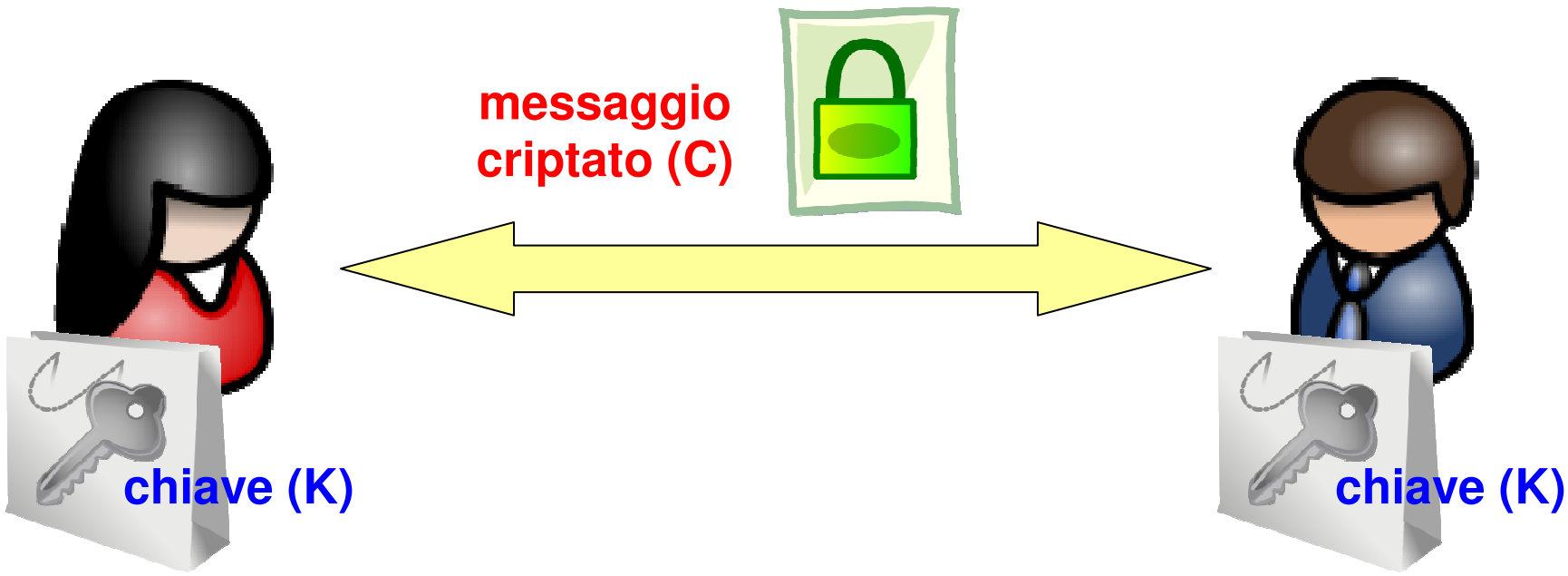


La cifratura a chiave simmetrica



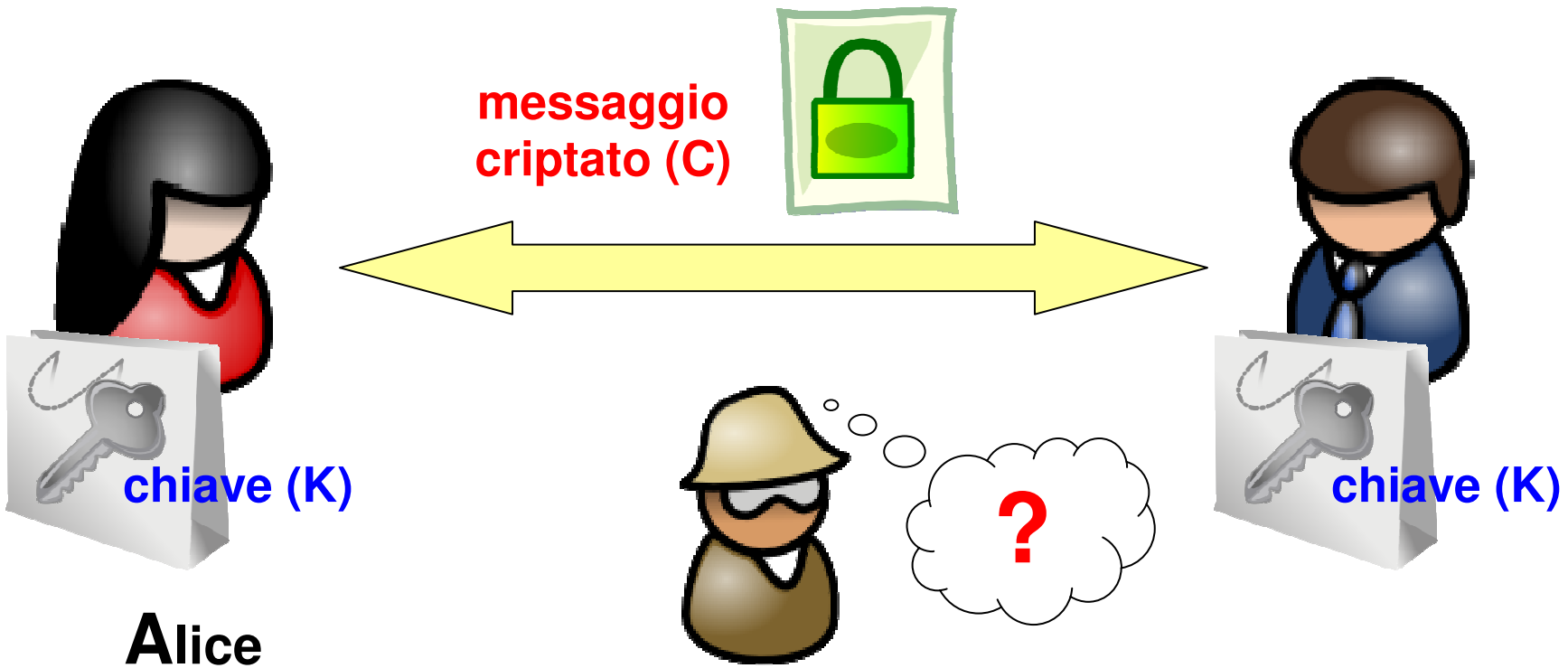
TechnoLabs

La cifratura a chiave simmetrica

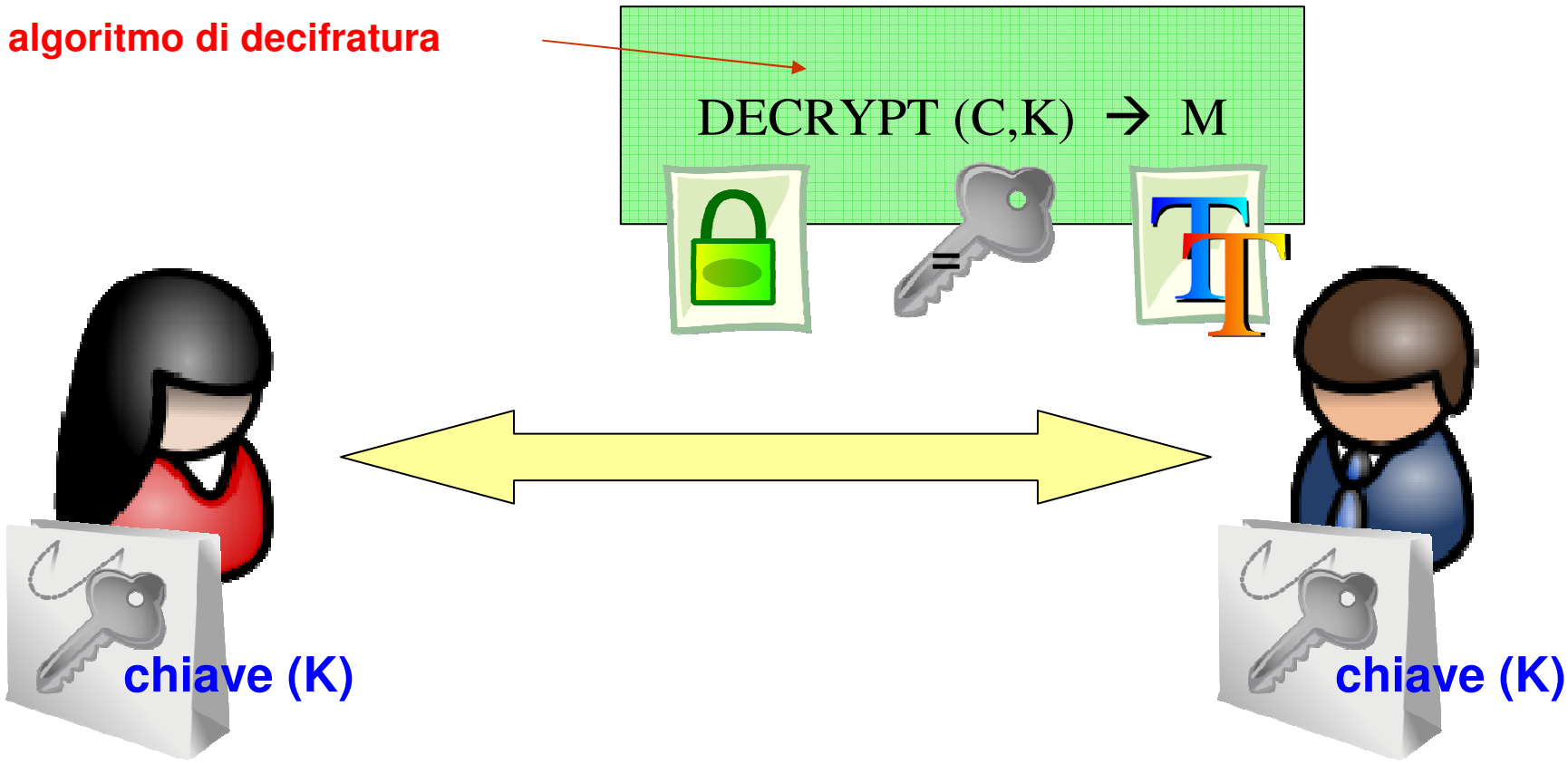


TechnoLabs

La cifratura a chiave simmetrica



La cifratura a chiave simmetrica



TechnoLabs

Data Encryption Standard: DES

DES codifica blocchi di 64 bit e usa chiavi di 56 bit; versioni successive (DES triplo) usano 2 o 3 chiavi da 56 bit (112,168 bit).

Codifica e decodifica con DES sono veloci; esistono implementazioni hardware

Storia

- Maggio 1973: richiesta pubblica per standard
- 1976: Modifica di Lucifer (IBM)
- 1977: viene pubblicato lo standard
- 2001: Advanced Encryption Standard (AES)

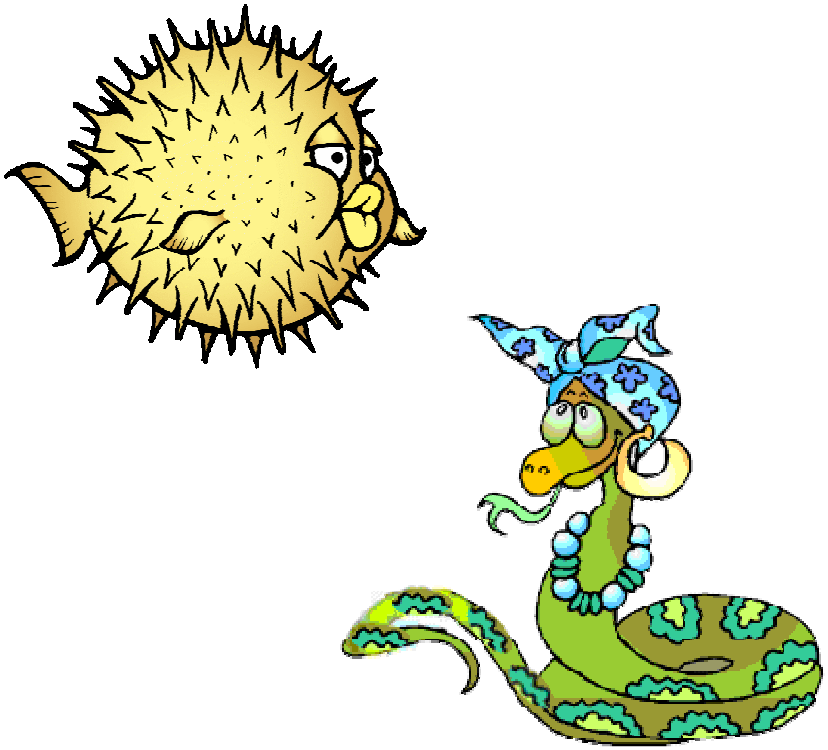
Altri algoritmi a chiave segreta

Esistono molte altre proposte e di solito:

- La codifica si basa su permutazione e sostituzione di parti del testo
- Le operazioni di permutazione sono ripetute diverse volte con modalità diverse e dipendono dalla chiave
- La lunghezza della chiave è variabile
- L'algoritmo deve essere semplice e non destare sospetti sulla sua correttezza (esistenza funzioni trapdoor); es. se si usano funzioni algebriche si devono usare funzioni ben note

La cifratura a chiave simmetrica

- Alcuni tipi:
  - DES, 3DES
  - CAST5
  - RC2, RC4, RC6
  - BLOWFISH
  - IDEA
  - RIJNDAEL (AES)
  - SERPENT
  - ...



Advanced Encryption Standard (AES)

1997 : NIST (National Institute of Standard and Technology, USA)

Concorso pubblico per AES : nuovo standard a blocchi per uso commerciale.

Perché nuovo standard?

Chiave DES corta, problemi di sicurezza

Esistenza di funzioni trapdoor? (qualcuno pensa che nel progetto di DES esista una modalità che permette al NIST di decodificare anche senza conoscere la chiave)

Advanced Encryption Standard

Requisiti: Cifrario a blocchi con chiavi fra 128 e 256 bit

- Resistente ai tipi di attacco noti
- Semplice, veloce e con codice compatto (implementabile su smart card)
- Senza royalties

La selezione utilizza un pubblico esame ed è basata su sicurezza, efficienza della implementazione (velocità e memoria richiesta)

Advanced Encryption Standard

SELEZIONE

- Giugno 1998: 15 candidati: descrizione algoritmo con analisi efficienza e robustezza rispetto ad attacchi piu' comuni
- Agosto 1999: dopo pubblico scrutinio scelta 5 finalisti: Mars(IBM), RC6 (RSA Lab.), Rijndael (Daemen e Rjinen), Serpent (Anderson et al.), Twofish (Schneider et al.)
- Ottobre 2000: RIJNDAEL è stato scelto: pubblico esame e eventuale revisione
- 2001 : RIJNDAEL è proposto come standard AES

Advanced Encryption Standard

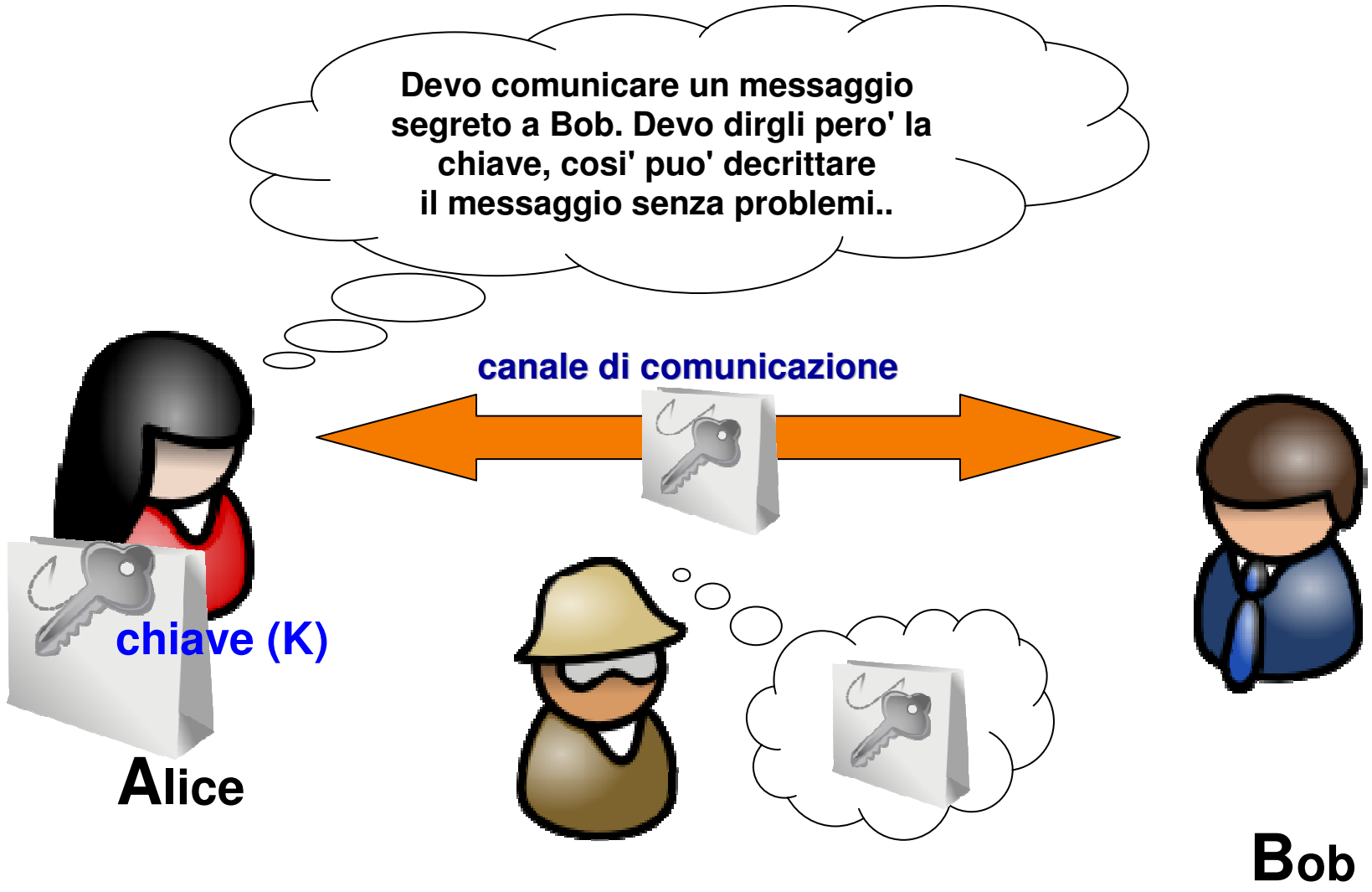
AES usa chiavi di 128, 192 o 256 bit

128 bit: 10 (round) iterazioni

- La chiave è espansa in 10 chiavi da 128 bit ciascuna
- Ogni round cambia lo stato e poi si esegue EXOR con la chiave
- Stato: 128 bit organizzati in una matrice 4 x 4 di byte

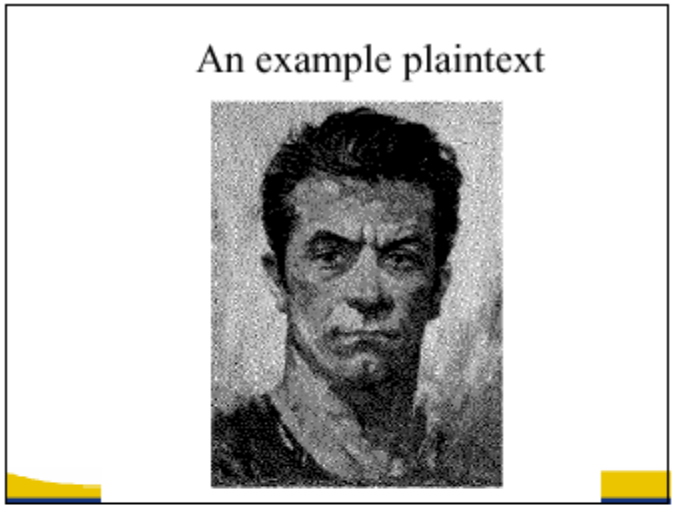
E' facile rompere AES con 1 o 2 round; ma non si sa come fare con 5 round; con 10 round è considerato impossibile!

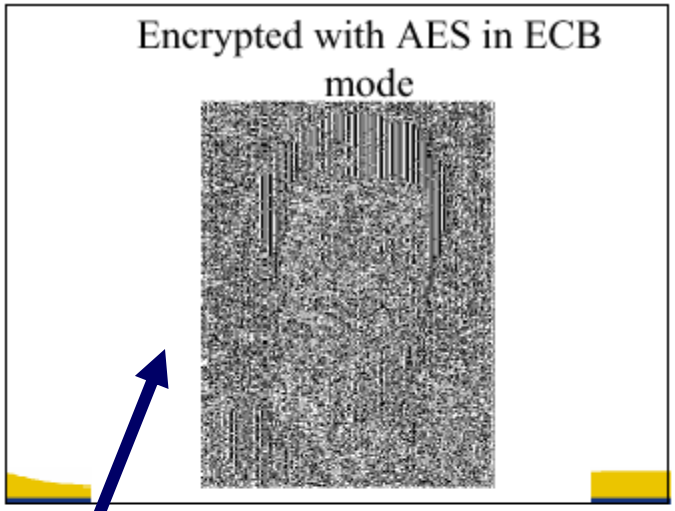
Sniffing della chiave



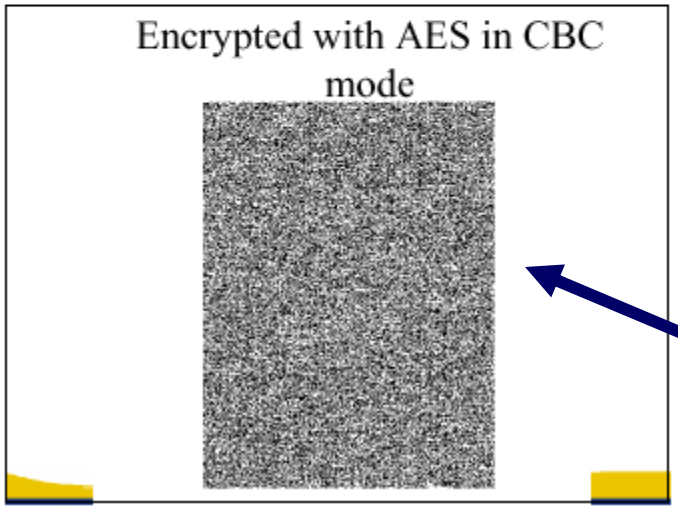
TechnoLabs

Comparison for AES





Similar plaintext blocks produce similar ciphertext (see outline of head)



No apparent pattern

Algoritmi asimmetrici

Problemi con crittografia a chiave simmetrica

- Richiede che mittente e ricevente abbiano la stessa chiave segreta
  - D.: come ci si accorda sulla chiave (specialmente tra computer)? Ci si incontra?
- Nella comunicazione fra n soggetti, si usano complessivamente $O(n^2)$ chiavi
  - Bisogna fare attenzione a non usare la chiave sbagliata

Algoritmi asimmetrici

Gli algoritmi **asimmetrici** utilizzano due chiavi distinte **generate insieme**:

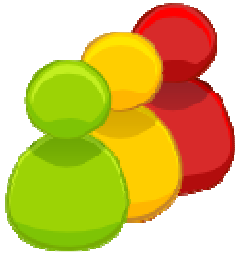
- La ***chiave pubblica*** usata per codificare e puo' essere distribuita
- La ***chiave privata*** usata per decodificare (deve essere segreta)

- La stessa chiave pubblica è usata da tutti gli utenti
- Nella comunicazione fra n soggetti, un algoritmo asimmetrico usa 2n chiavi.

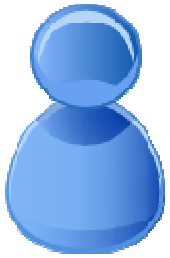
La cifratura a chiave asimmetrica

- Ogni utente ha due chiavi


- Una delle chiavi è resa pubblica

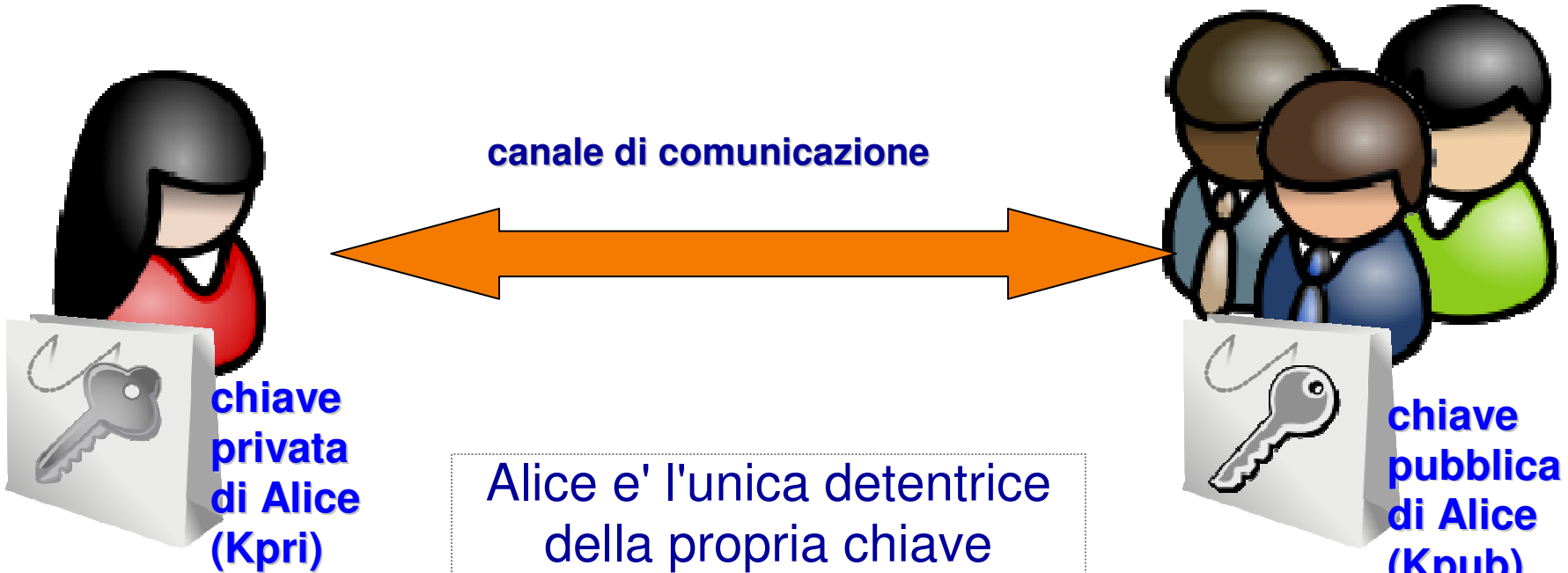
- La chiave segreta (privata) è nota soltanto al suo proprietario

TechnoLabs

La cifratura a chiave asimmetrica

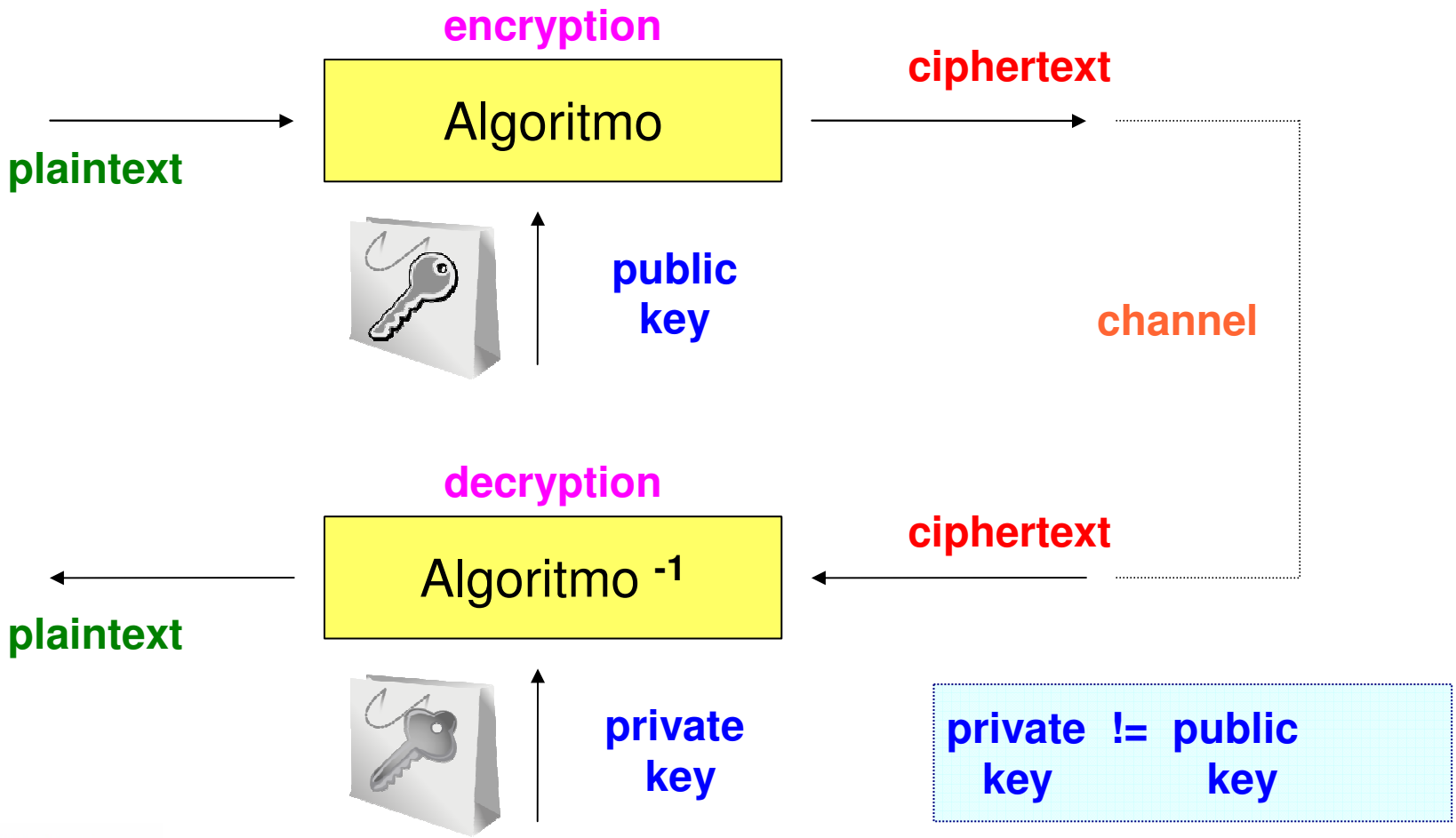
Soluzione basata su chiavi pubbliche



TechnoLabs

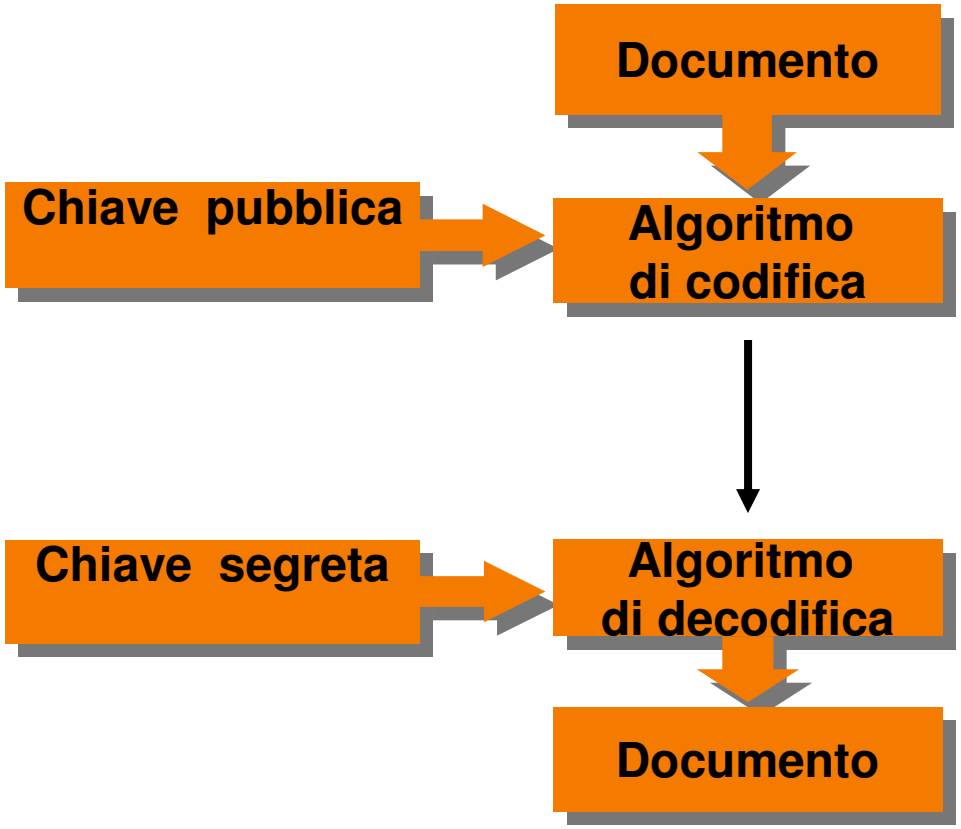
La cifratura a chiave asimmetrica

Schema a blocchi:



TechnoLabs

Algoritmi asimmetrici: codifica e decodifica



Conoscere la chiave pubblica non deve permettere di conoscere la chiave segreta

La cifratura a chiave asimmetrica

- E' possibile mantenere un *portafoglio* di chiavi pubbliche per ogni soggetto che si vuole contattare
- Bob
- Cris
- Dilan

- Oppure esistono dei circuiti chiamati *keyserver* dove e' possibile reperire le chiavi dei soggetti cercati
- (vedi http://pgp.mit.edu)

Algoritmi asimmetrici: storia

Idea originaria crittografia chiave pubblica circa 1950 (non pubblicata)

Diffie- Hellman proposero un metodo (non sicuro)

1978: Rivest Shamir e Adleman proposero il metodo **RSA**, che è ancora oggi il più usato in pratica.

RSA: scelta delle chiavi

1. Scegli due numeri primi grandi *p*, *q*.
   (es., 1024 bit ciascuno)

2. Calcola *n* = *pq*, *z* = *(p-1)(q-1)*

3. Scegli *e* (con *e<n)* privo di fattori comuni con z.
   (es. *e=99* e *z=100* non sono primi ma non hanno fattori comuni)

4. scegli *d* tale che *ed-1* sia esattamente divisibile per *z*.
   (cioè: *ed* mod *z* = *1*).

5. La chiave *Pubblica* è *(n,e)*, quella *Privata* è *(n,d)*.

RSA: cifratura, decifrazione

0. Dati (n,e) e (n,d) calcolati come al punto precedente

1. Per cifrare la stringa di bit corrispondente a m, calcola

   $c = m^e \bmod n$ (resto di m^e diviso n)

2. Per decifrare c, calcola

   $m = c^d \bmod n$ (resto di c^d diviso n)

Questa è vera ! $m = (m^e \bmod n)^d \bmod n$

RSA: Esempio

Bob sceglie *p=5, q=7*. Allora *n=35, z=24*.

e=5
d=29 (*ed-1* esattamente divisibile per z)

	lettera	m	m^e	$c = m^e \bmod n$
Cifra:	l	12	1524832	17

	c	c^d	$m = c^d \bmod n$	letter
Decifra:	17		12	l

481968572106750915091411825223072000

TechnoLabs

RSA: Implementazione

Come trovare le chiavi

1. Genera due primi p,q
2. Calcola n= pq
3. Scegli a caso e
4. Se MCD (e, (p-1)(q-1)) =1 (MCD= Massimo Comun Divisore)
   - Allora $d= e^{-1} \bmod (p-1)(q-1)$
   - Altrimenti vai a 3

RSA: Implementazione (cont.)

Come trovare un numero primo

1. Scegli un numero dispari a caso
2. Verifica se è primo (Esistono algoritmi veloci → polinomiali)

I numeri primi sono frequenti: $\pi(x)$ = n. primi tra 2 e x, $\pi(x)$ appross. $x/\ln x$

Es.: in $[2^{511}, 2^{512}]$ la probabilità che un numero dispari sia primo è >1/178

RSA: Implementazione (cont.)

Come calcolare MCD(x,y): algoritmo di Euclide

Come calcolare la potenza: il metodo di elevazione a potenza modulare esegue un numero logaritmico di moltiplicazioni

ESEMPIO

$40 = 0 \cdot 2^0 + 0 \cdot 2^1 + 0 \cdot 2^2 + 1 \cdot 2^3 + 0 \cdot 2^4 + 1 \cdot 2^5$

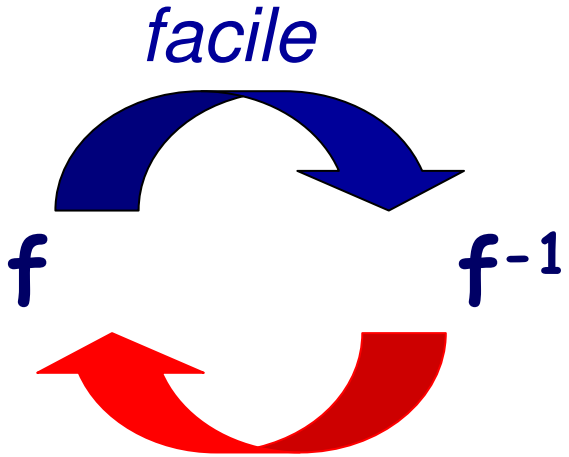
$x^{40} = (x^1)^0 * (x^2)^0 * (x^4)^0 * (x^8)^1 * (x^{16})^0 * (x^{32})^1$

Spesso e=3 oppure 65537 (solo due 1 in binario!)

RSA: Sicurezza

Funzione one way:

- facile da calcolare
- difficile da invertire



Facile: Esiste Algoritmo veloce (tempo polin.)

Difficile: Non esiste (o si crede che non esista) algoritmo polinomiale

RSA: Sicurezza (cont.)

- Se l'avversario sa fattorizzare $N = pq$ allora può conoscere la chiave segreta:

  Calcola $(p-1)(q-1)$ e poi $d = e^{-1} \bmod (p-1)(q-1)$

- Inoltre la definizione di RSA implica che se si conosce la chiave segreta allora è facile conoscere come si fattorizza N

Fattorizzare N e decodificare sono problemi computazionalmente equivalenti

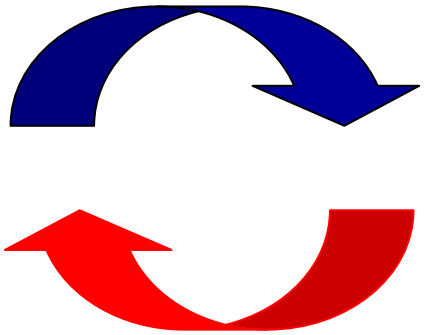
Non sono noti attacchi migliori che fattorizzare N:

Es. Conoscere (p-1)(q-1) equivale a conoscere la fattorizzazione di N

RSA: Sicurezza (cont.)

Moltiplicare e fattorizzare:

facile



p,q N=pq

difficile

Funzione one way:

Facile da calcolare

Difficile da invertire

Moltiplicazione facile ⟹ codifica veloce

Fattorizzazione difficile ⟹ decodifica molto lunga (se non si conosce la chiave)

RSA: Sicurezza (cont.)

Test primalità : facile

Fattorizzazione: difficile (algoritmo semplice $O(N^{1/2})$; algoritmi migliori sono noti ma non sono polinomiali)

Nota bene: algoritmo polinomiale nella lunghezza dell'input. La rappresentazione di N richiede (log N) bit.

Es.: N da 1024 bit (155 cifre decim.)

$O(N^{1/2}) = O(2^{512})$

RSA: Sicurezza (cont.)

Esempio: Ago. 1999 RSA-155 è stato fattorizzato usando 300 elaboratori (tipo Pentium 2, WS Sun-400 MHz) in 7.4 mesi

- I numeri più difficili da fattorizzare sono quelli n= pq, dove p e q hanno la stessa lunghezza
- Per essere tranquilli
  - 768 bit (230 digit) uso personale
  - 1024 bit per aziende
  - 2048 per chiavi importanti

RSA: utilizzo in pratica

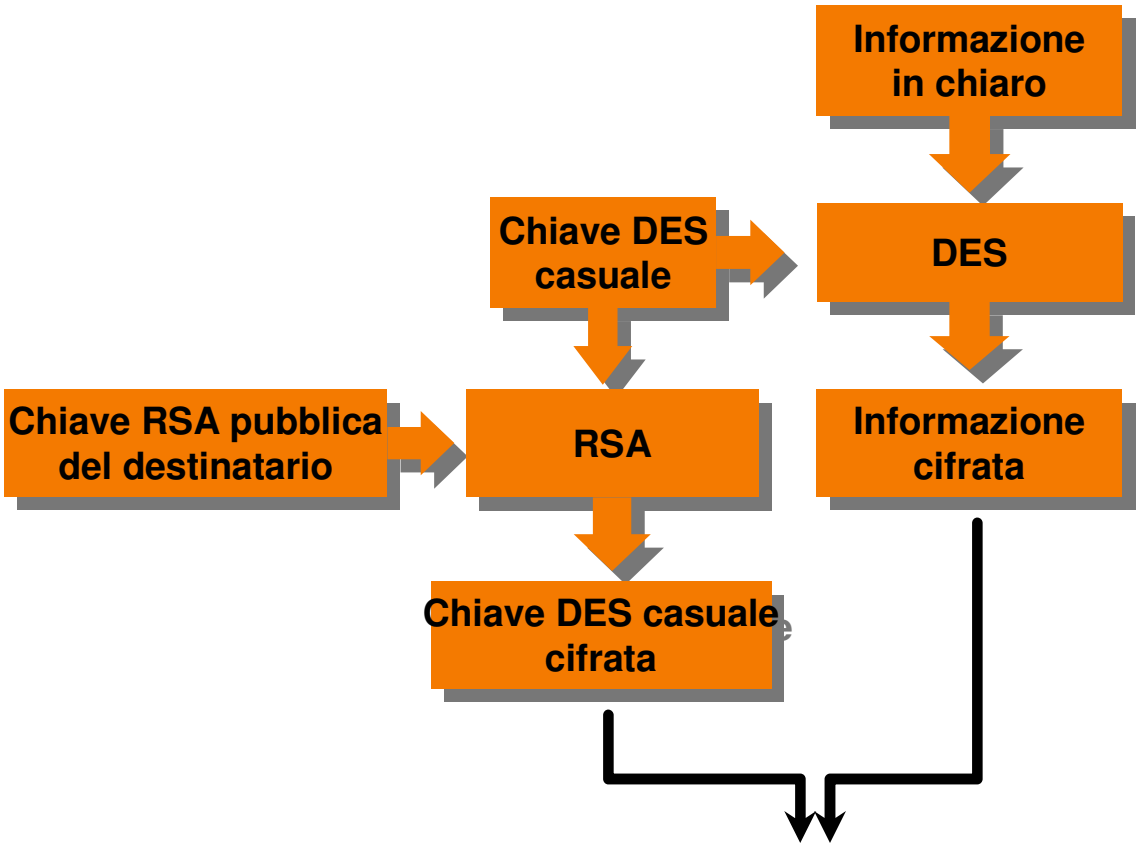
Per molte applicazioni RSA e' lento:

si può usare RSA con DES (o con altro metodo a chiave segreta)

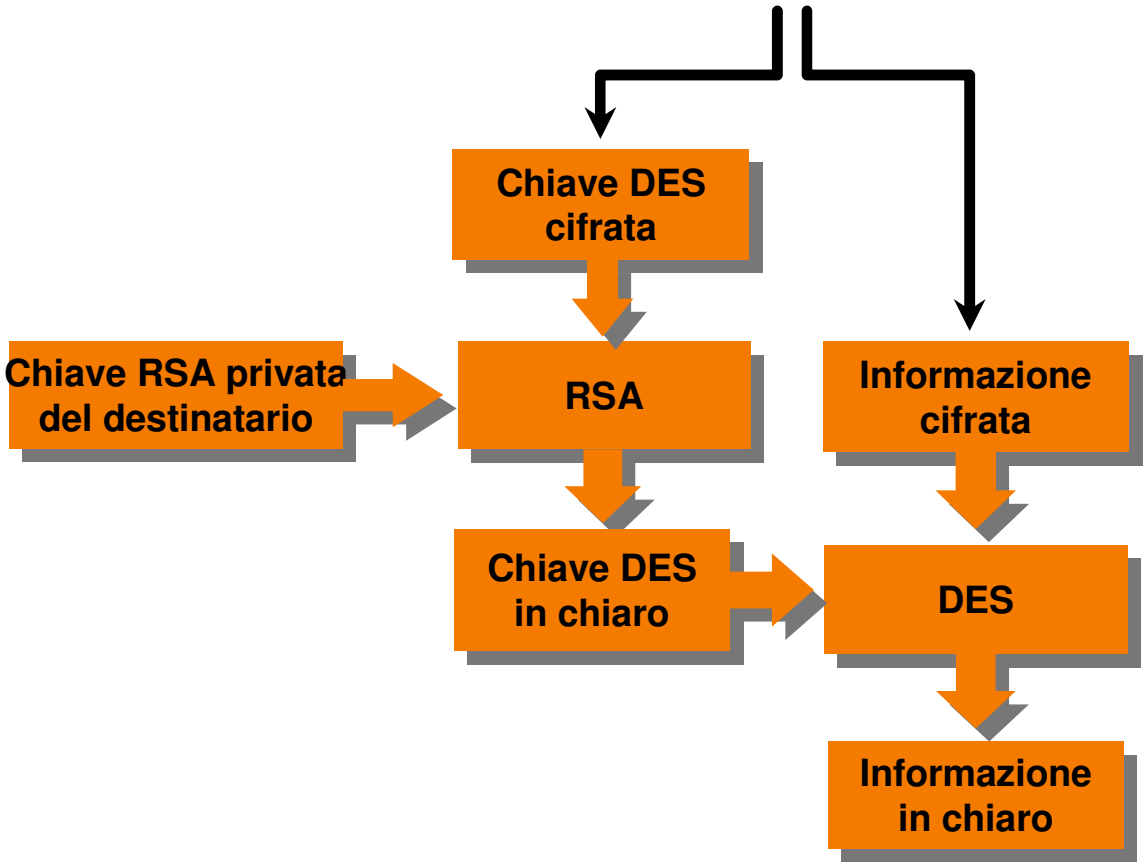
Esempio: A invia un messaggio M a B

- A genera una chiave C, cifra C con RSA e M con DES (con chiave C)
- A invia il documento cifrato con DES e la chiave cifrata con RSA a B
- B usa la sua chiave privata RSA per conoscere la chiave C e poi usa DES per ottenere il messaggio.

RSA: utilizzo in pratica (cont.)



RSA: utilizzo in pratica (cont.)



Brevetti su algoritmi di cifratura (USA)

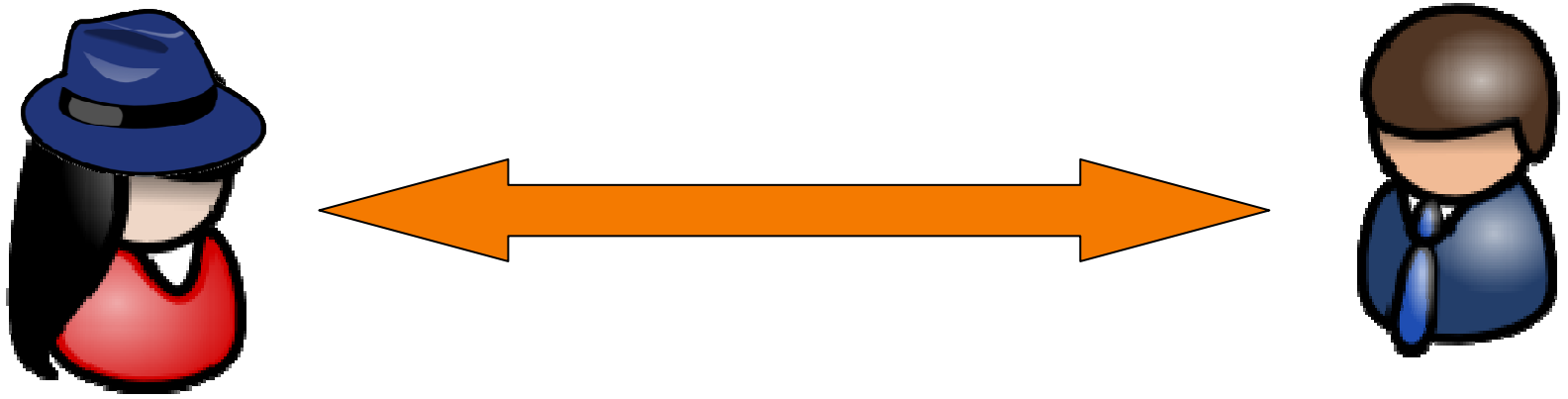
numero	oggetto	inventore	scadenza
3.962.539	DES	Ehrsam ed al.	1993
4.200.770	Diffie-Hellman	Hellman, Diffie, Merkle	1997
4.218.582	Critt. chiave pubblica	Helman, Merkle	1997
4.424.414	Pohling-Hellman	Hellman, Pohling	3 gen 2001
4.405.829	RSA	Rivest, Shamir, Adleman	20 sett 2000
4.748.668	Shamir-Fiat	Shamir, Fiat	2005
4.850.017	Vettori di controllo	Matyas, Meyer, Bracht	2006
5.140.634	Guillou-Quisquater	Guillou-Quisquater	2009
5.231.668	DSA	Kravitz	2010
5.214.703	IDEA	Massey-Lai	2010
5.276.737	Fair Cryptosystems	Micali	2011

La cifratura a chiave asimmetrica

PROBLEMA

Bob si chiede: “chi mi assicura che il messaggio che ho ottenuto sia veramente quello scritto da Alice e non sia stato alterato da un Ficcanaso?”

SOLUZIONE → **autenticazione con firma digitale**



TechnoLabs

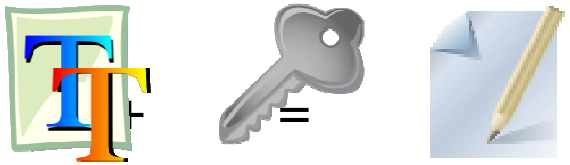
La firma digitale

Se cifro un messaggio con la mia chiave privata ottengo un *messaggio firmato*. Il destinatario utilizzando la mia chiave pubblica riuscirà ad attestarne l'autenticità.

Cifratura:

plaintext **Kpub** **ciphertext**

Firma:



plaintext **Kpriv** **digital signature**

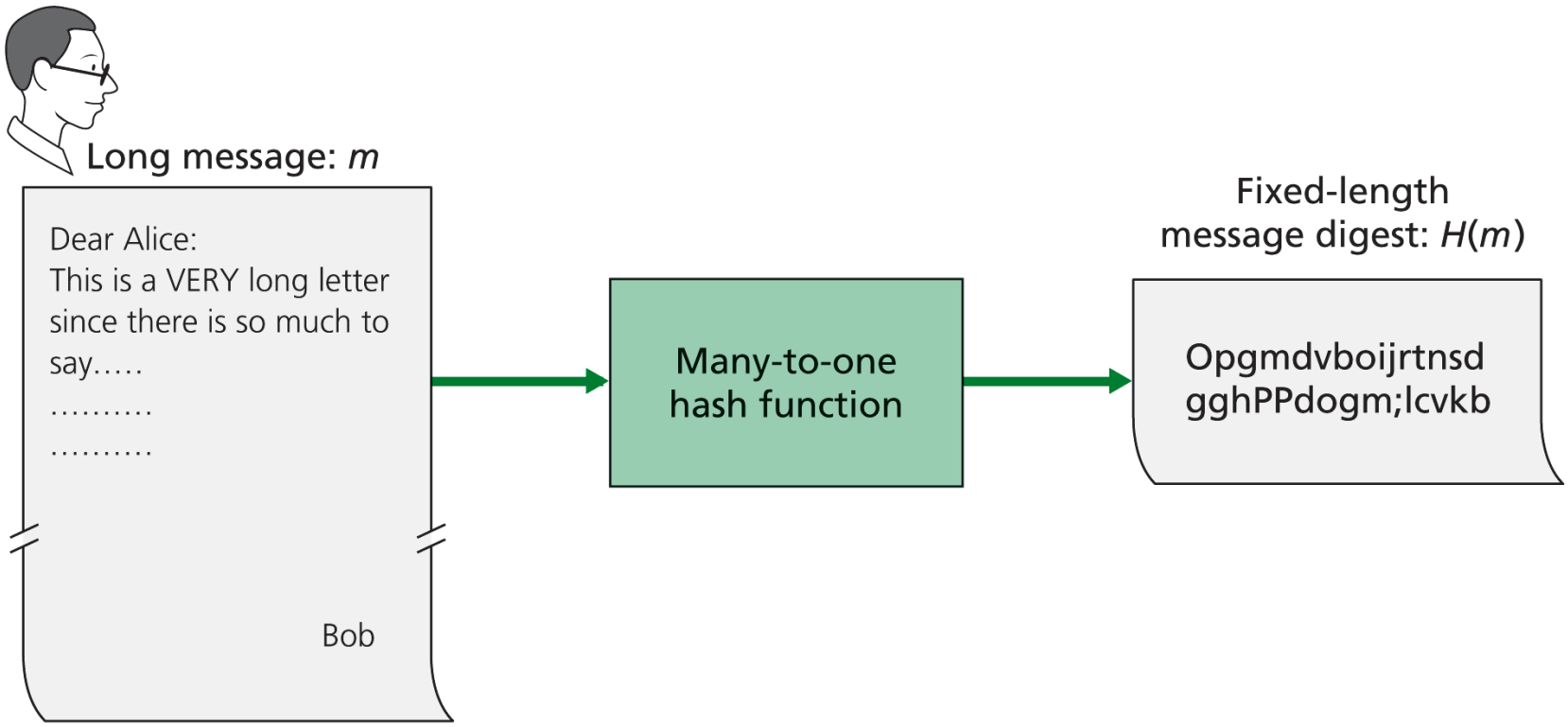
La <u>combinazione</u> di queste tecniche garantisce **privatezza** ed **autenticità**.

TechnoLabs

Integrità: one-way hash

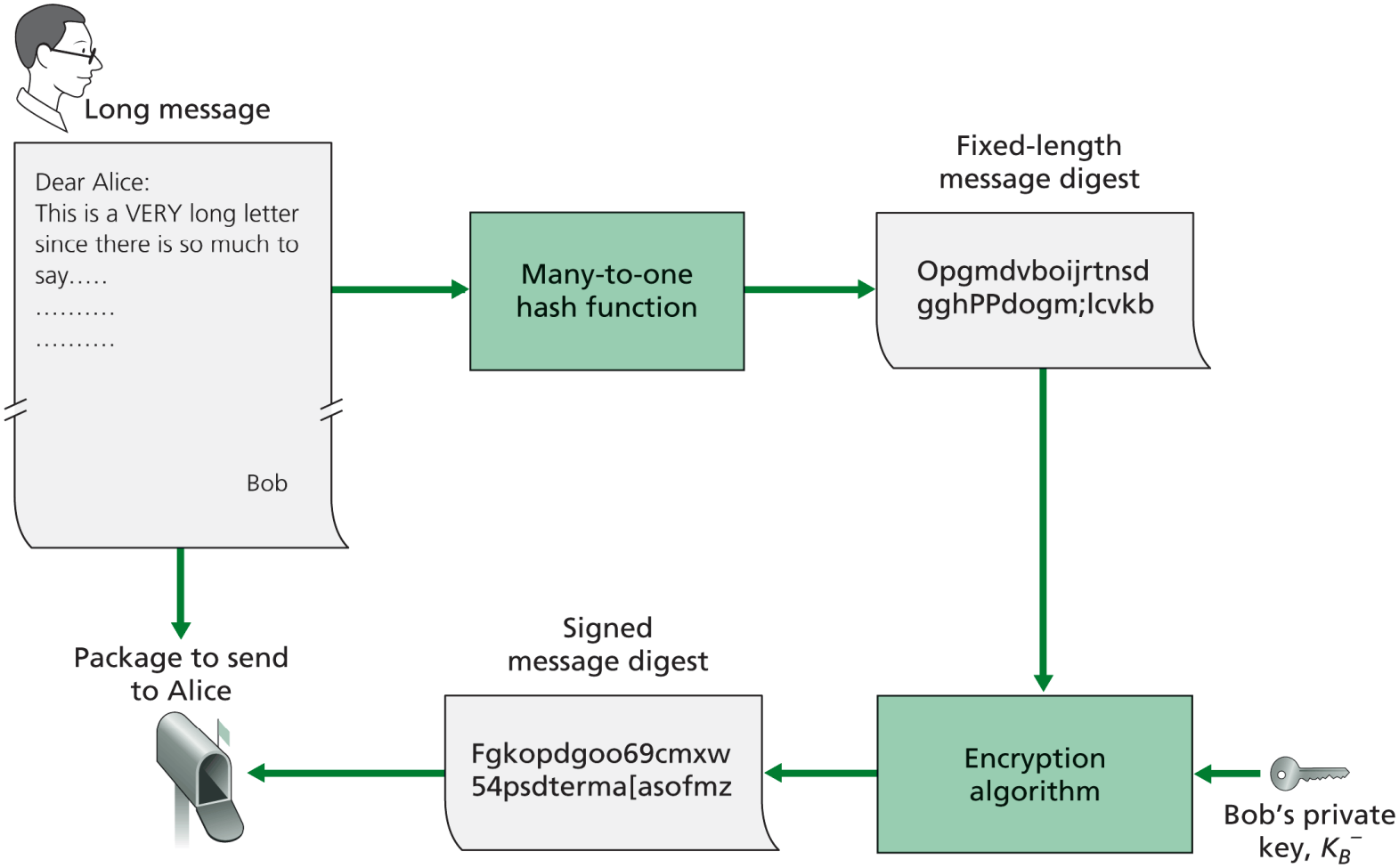
- Funzioni che hanno in ingresso un messaggio di lunghezza variabile e producono una stringa di lunghezza fissa (*hash*).
- È praticamente impossibile trovare un messaggio che produca un hash specificato.
- Modificando anche un solo bit del messaggio si ottiene un hash completamente diverso.

Hashing



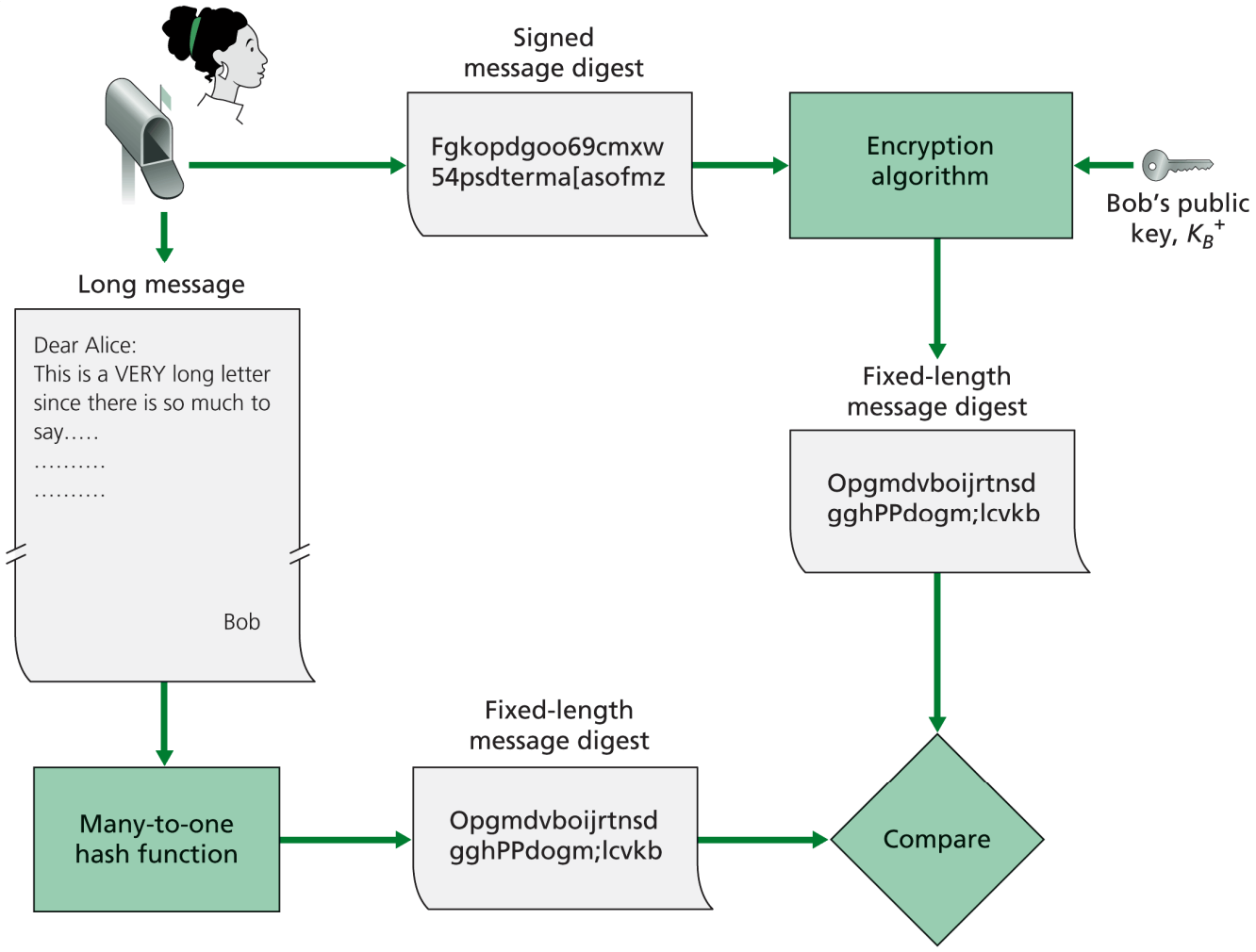
- Hash functions are used to create message digests.

Signature



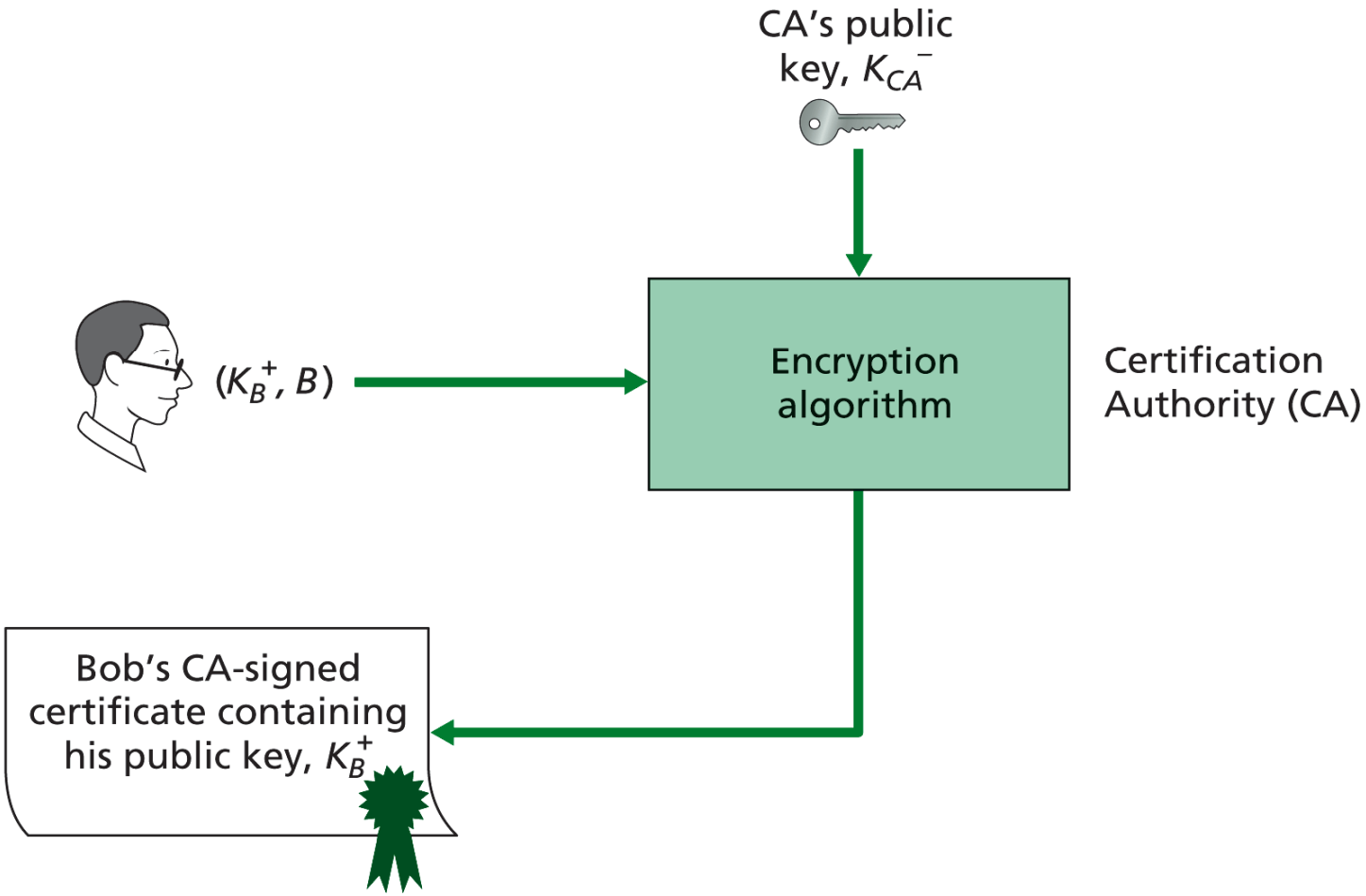
- Sending a digitally signed message

Verifica



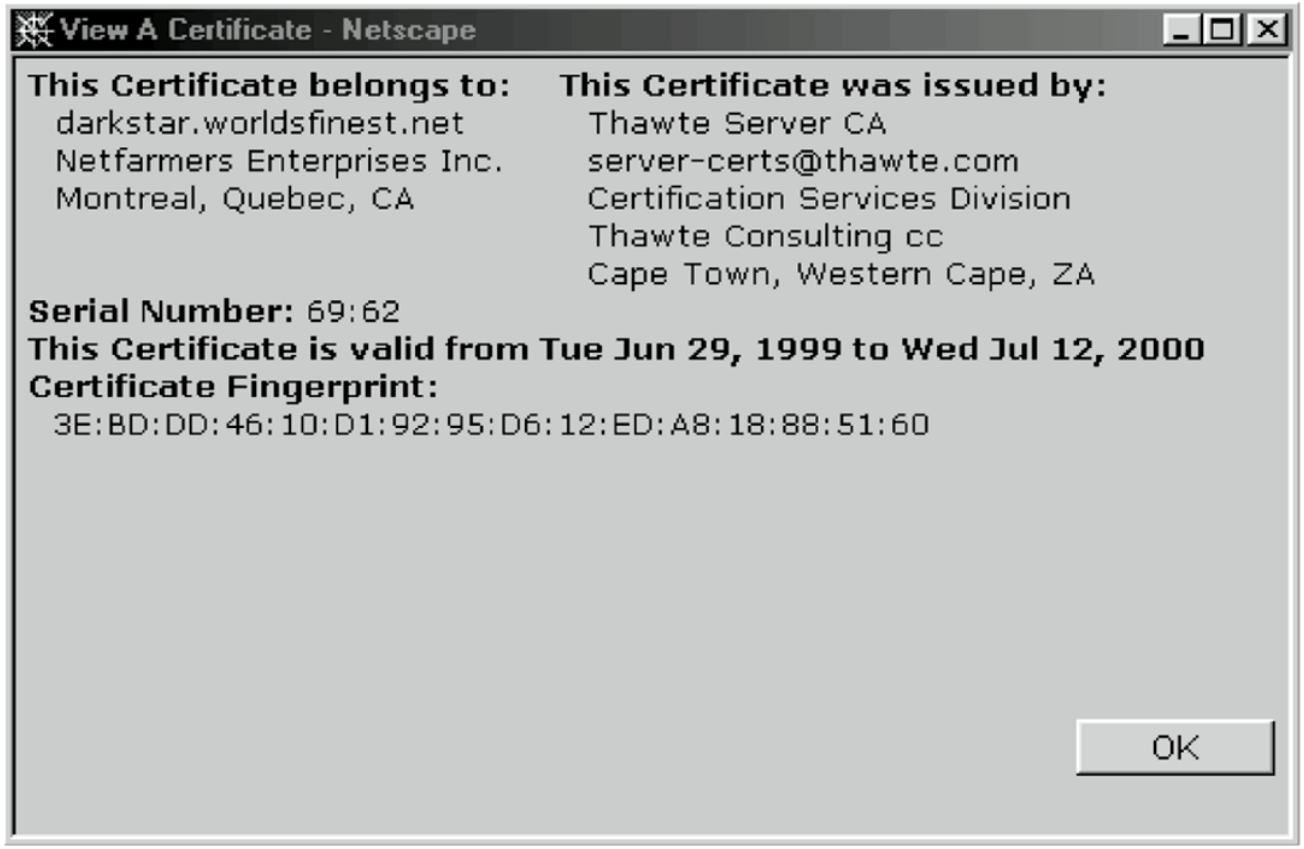
♦ Verifing the integrity of a signed message

Certification Authority



- Bob obtains a certificate from the CA.

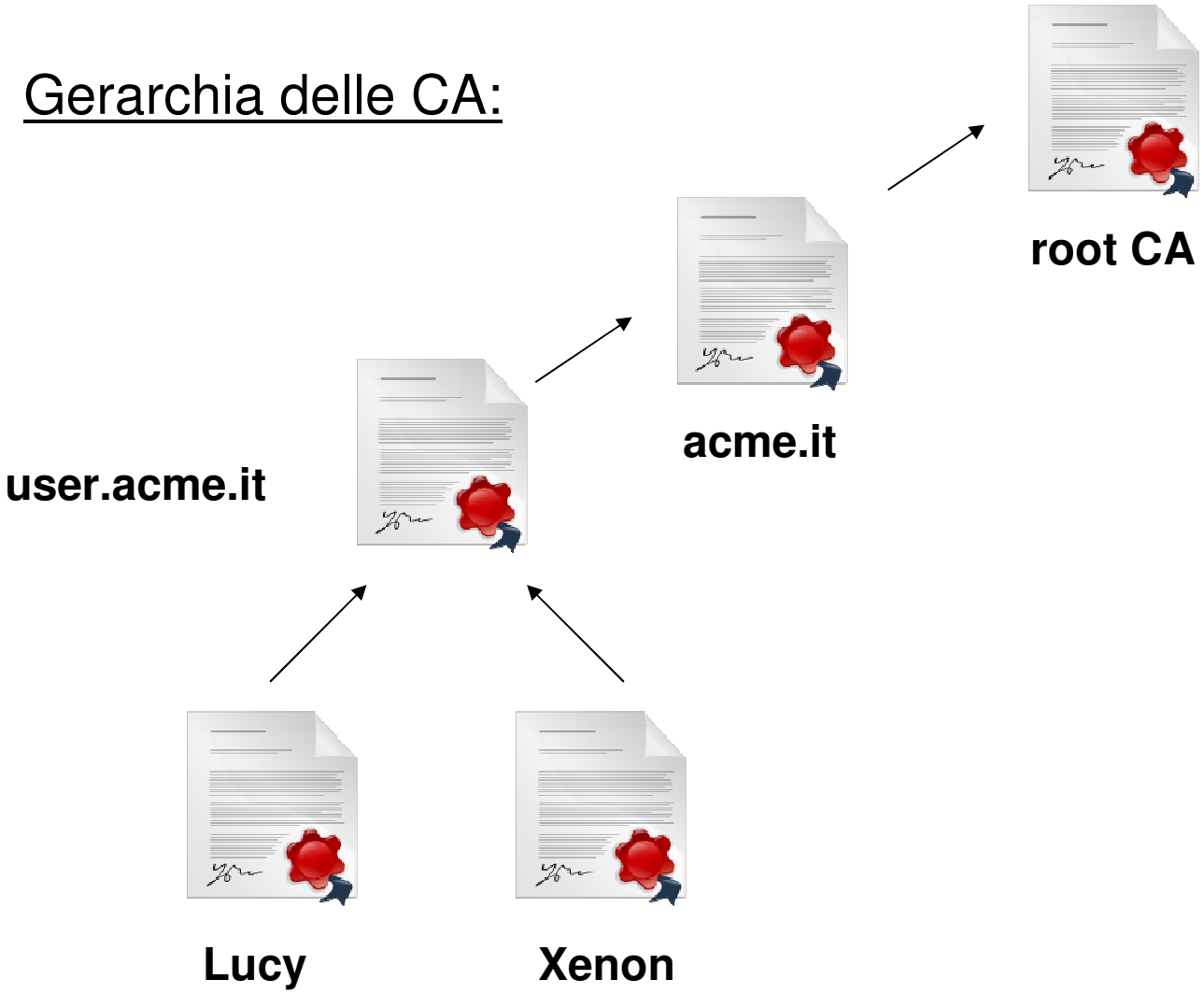
Certificato



- A certificate issued by Thawte Consulting to Netfarmers Enterprises, Inc.

Il certificato a chiave pubblica

Gerarchia delle CA:



TechnoLabs

La firma digitale

mittente

Schema a blocchi

destinatario

messaggio da spedire

messaggio ricevuto

MESSAGE DIGEST

MESSAGE DIGEST

MD

MDrx = MDtx ?

Kpriv

Kpub

ALGORITMO ASIMMETRICO

ALGORITMO ASIMMETRICO

digital signature

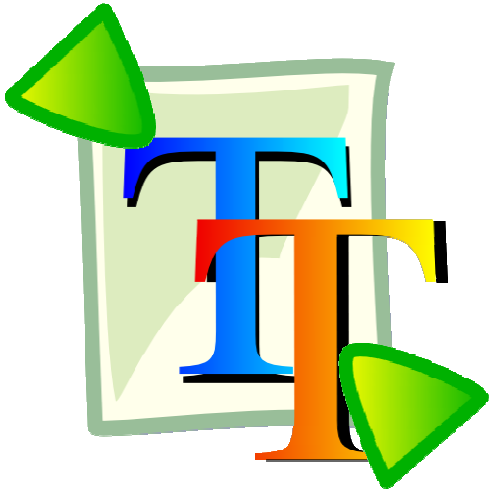
TechnoLabs

Cos'e' il MESSAGE DIGEST?

E' una *funzione di hash* che riassume un messaggio in una sua rappresentazione non falsificabile

Alcuni algoritmi utilizzati per il message digest sono:

- MD5 (digest a 128 bit)
- SHA (digest a 160 bit)



A che cosa servono le due chiavi ?

- L'utente X, con la sua chiave segreta:
  - FIRMA il messaggio
  - DECIFRA il messaggio indirizzatogli
- Gli altri utenti, con la chiave pubblica dell'utente X
  - VERIFICANO che il messaggio sia stato realmente inviato da X
  - CIFRANO il messaggio per X

Come usare le chiavi

- Chiave PRIVATA
  - Riservata
  - Protetta da una password lunga detta “PASS PHRASE”
    - ➔ FIRMA messaggi
    - ➔ DECIFRA messaggi
- Chiave PUBBLICA
  - Distribuibile a chiunque, attraverso:
    - key servers
    - distribuzione diretta
    - pubblicata su WEB

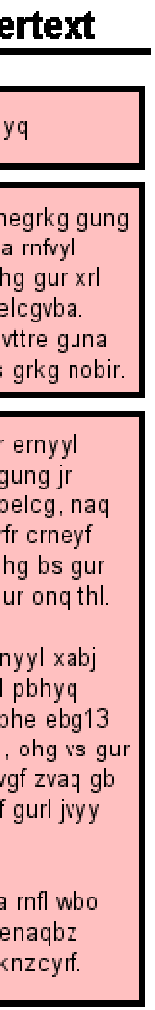
Le chiavi vengono mantenute in due
files indirizzati attraverso la variabile d’ambiente PGPPATH:

+ pubring.pgp
+ secring.pgp

Autenticazione: certificati

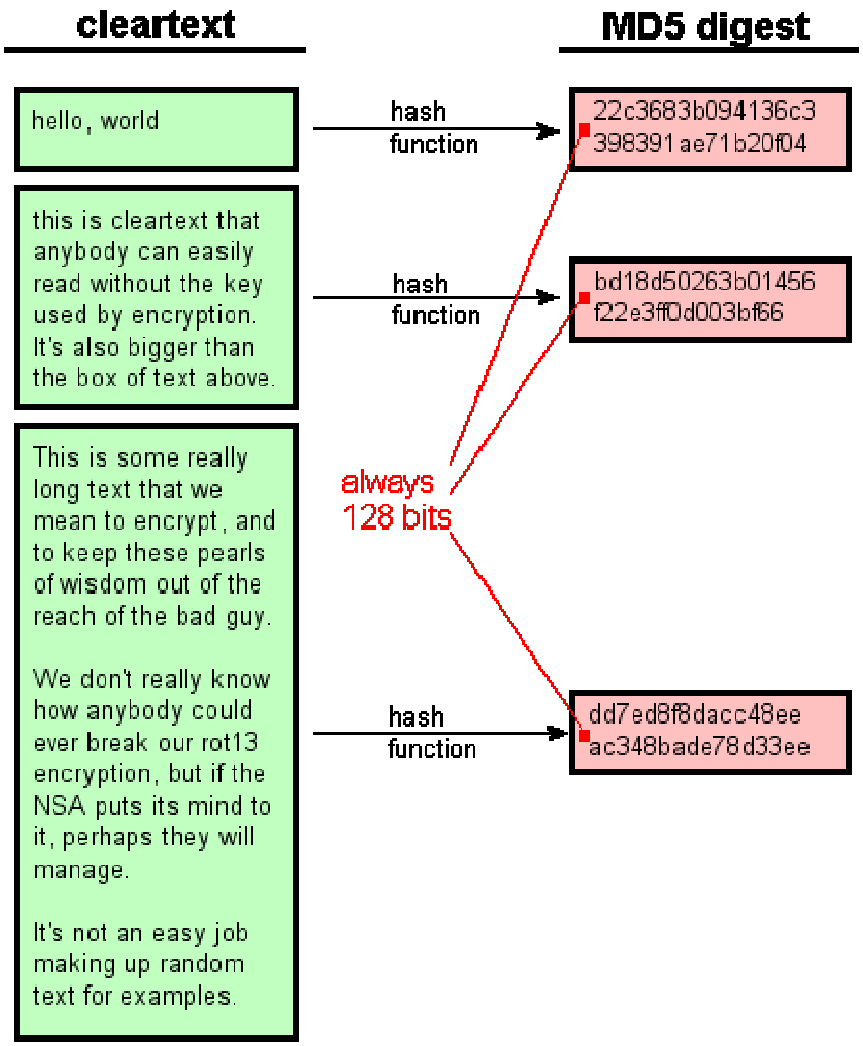
- La firma digitale rende sicuro un messaggio se:
  - la chiave privata di **A** non è stata compromessa;
  - **B** è in possesso della *vera* chiave pubblica di **A**.
- La convalida delle chiavi pubbliche viene fatta tramite i **certificati**: un'autorità esterna (*Certification Authority*) garantisce dell'autenticità delle chiavi pubbliche.
- Due modelli esistenti:
  - X.509: organizzazione gerarchica;
  - PGP: "web of trust"

Encryption - a two-way operation



TechnoLabs

Hashing - a one-way operation



TechnoLabs

Verifying file integrity

- ProFTPD

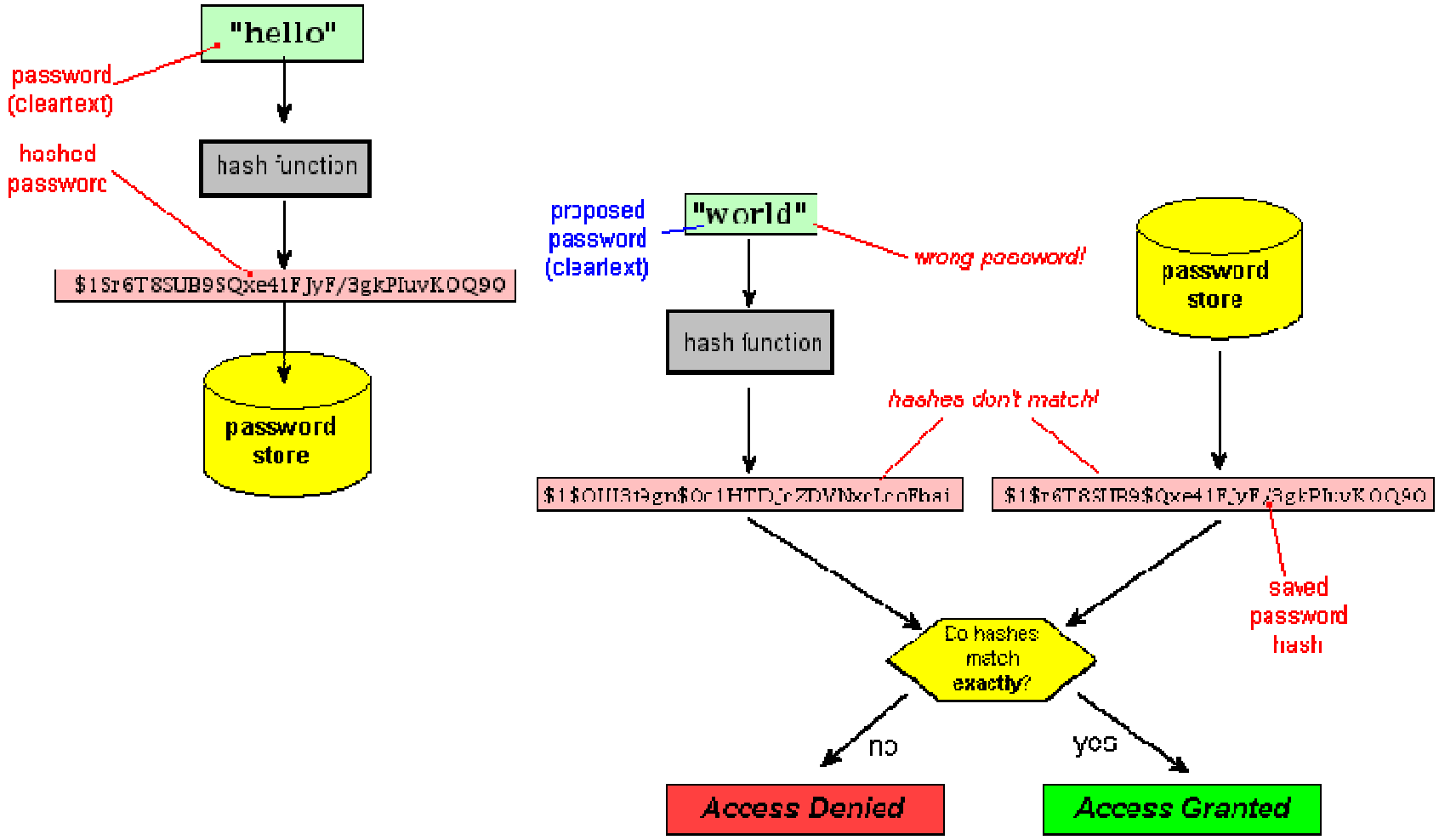
Highly configurable GPL-licensed FTP server software

MD5 sums and PGP signatures of release files

MD5 Digest Hashes

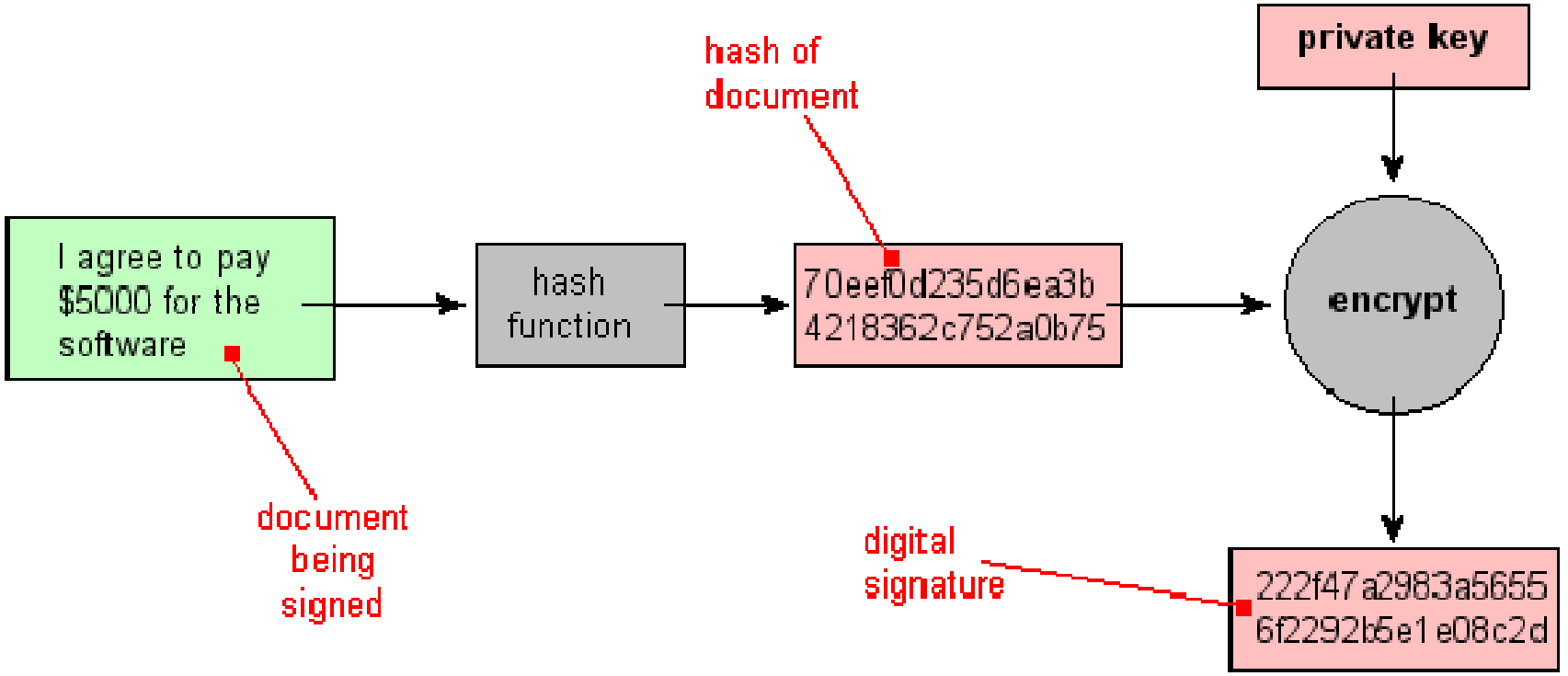
```
417e41092610816bd203c3766e96f23b proftpd-1.2.8p.tar.bz2
abf8409bbd9150494bc1847ace06857a proftpd-1.2.8p.tar.gz
7c85503b160a36a96594ef75f3180a07 proftpd-1.2.9.tar.bz2
445fbf24e2ec300800a184eb81296bda proftpd-1.2.9.tar.gz
d834bb822816a2ce483cc2ef1a9533e7 proftpd-1.2.10rc3.tar.bz2
1e306d2f54ea92895ecff6659498b911 proftpd-1.2.10rc3.tar.gz
```

Hashing Passwords



TechnoLabs

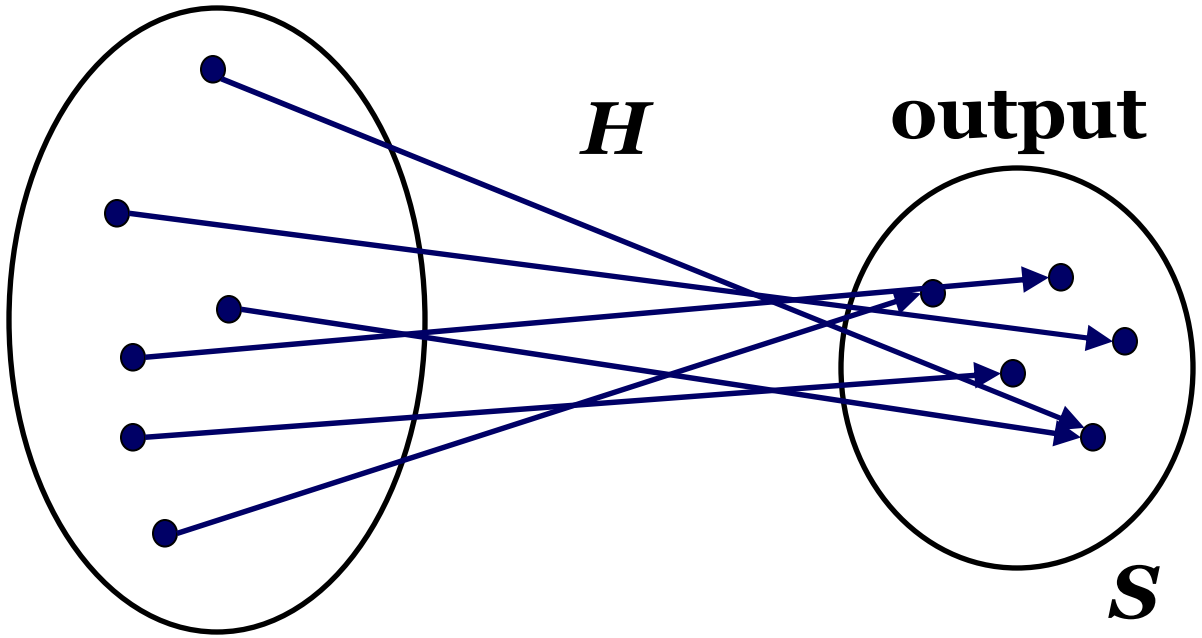
Digitally Signed Documents



TechnoLabs

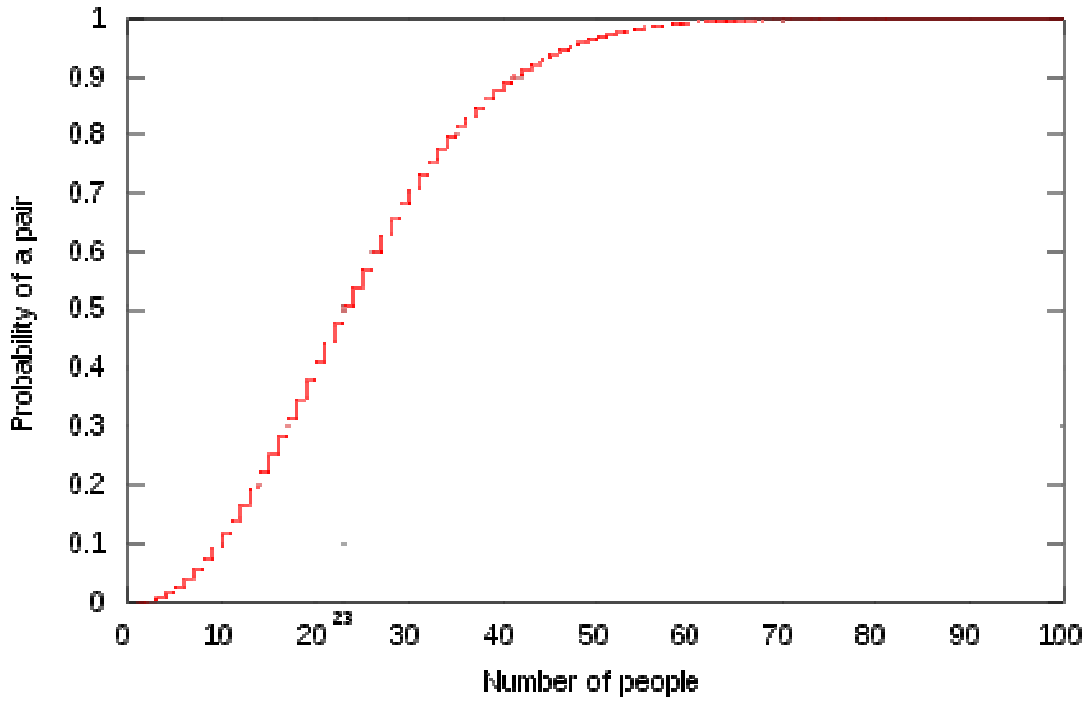
Birthday paradox

- Finding collision: $\sim\sqrt{|S|} = 2^{n/2}$



TechnoLabs

Paradosso del compleanno



TechnoLabs

Security level

		hash output
• Insecure:	2^{64} operations	128 bits
• Medium-term:	2^{80}	160 bits
• Long-term* :	2^{128}	256 bits
• Paranoid:	2^{256}	512 bits

* (~20 years)

TechnoLabs

Collision in MD5

```
0x80000000 98163156 d685de69 e985b795 b4320c10 cd350030 c014ca29 850b7d6d
  0934ad59 4871afd0 aa480edf e4fc0320 7bb68ed1 3b505ddf 5e5d5df6 b539a48d

  fcb488ff adf40003 88d9fda4 d72a8fdc a887f4ca eec4f800 b75f8b20 7f1e9b51
  9ab427cc 45c236f1 73f20086 e000005a 3b6550cc b6cc1c59 0fe9f71a a0403064
```

collides with

```
0x80000000 98163156 d685de69 e985b795 34320c10 cd350030 c014ca29 850b7d6d
  0934ad59 4871afd0 aa480edf e4fc0320 7bb68ed1 3b505ddf de5d5df6 b539a48d

  fcb488ff adf40003 88d9fda4 d72a8fdc a887f4ca eec4f800 b75f8b20 7f1e9b51
  9ab427cc 45c236f1 73f20086 dfff805a 3b6550cc b6cc1c59 0fe9f71a a0403064
```

TechnoLabs

Internet Cryptographic Protocols

Protocol	Purpose
CyberCash (5)	Electronic funds transactions
DNSSEC (5)	Domain Name System
IPSec (layer 3)	Packet-level encryption
PCT	TCP/IP level encryption
PGP **(layer 5)**	E-mail
S-HTTP **(layer 5)**	Web browsing
Secure RPC	Remote procedure calls
SET (layer 4)	Electronic funds transactions
SSL (layer 4)	TCP/IP level encryption

TechnoLabs

Limiti della crittografia

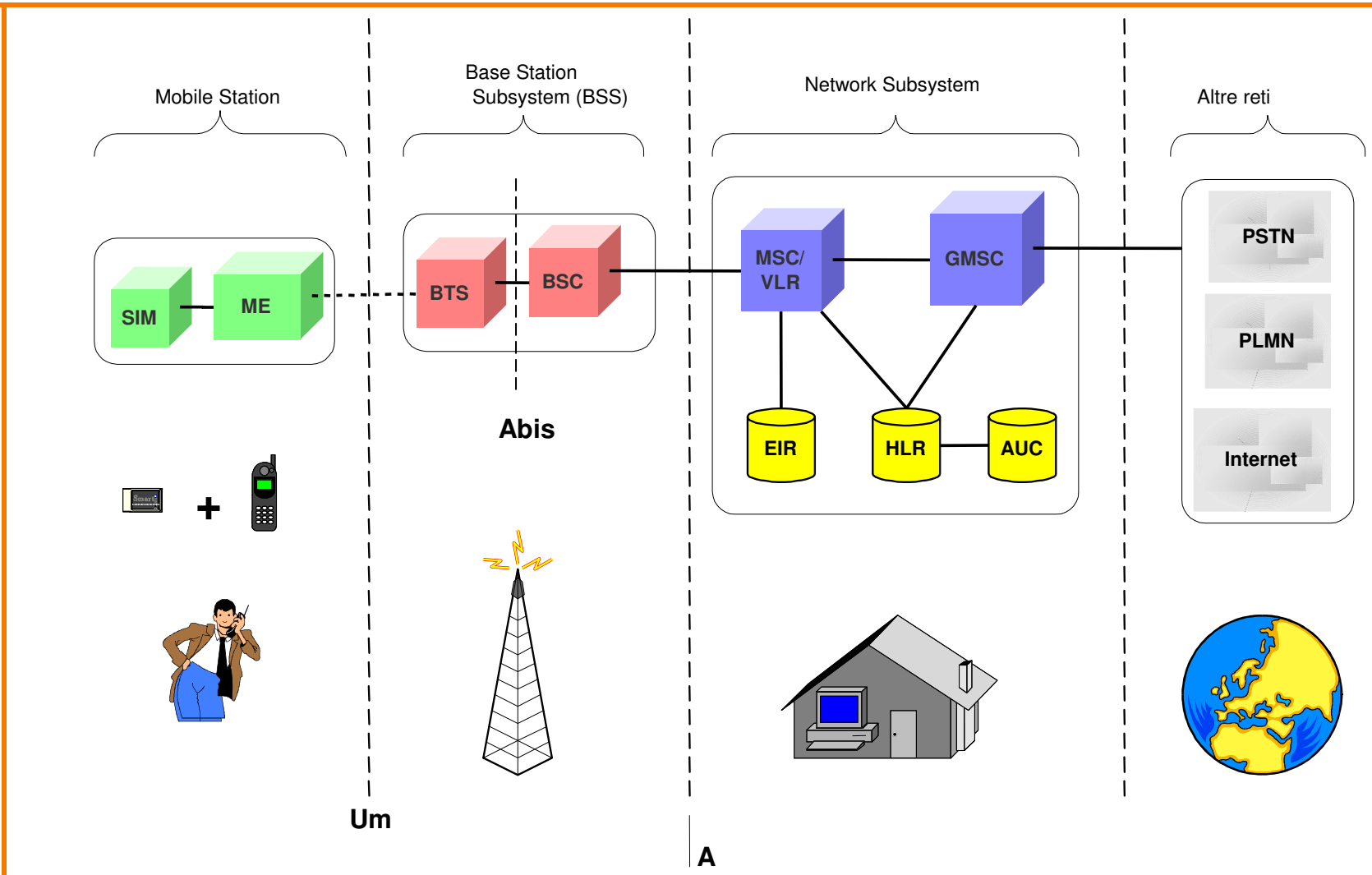
- La maggior parte dei problemi di sicurezza non sono approcciabili con la crittografia
- La cosa buona
  - La crittografia funziona !!!
- La cosa cattiva
  - La gente fa altri errori;
  - La crittografia non è in grado di risolverli

Crittografia

Case Study

TechnoLabs

Architettura di una rete GSM



TechnoLabs

Procedure di sicurezza

- Autenticazione:
  - ha il compito di verificare l'identità dell'utente e proteggere da utilizzi fraudolenti degli identificativi
- Cifratura:
  - ha il compito di rendere non facilmente decodificabile il flusso dati da e verso la MS da parte di intrusi
- In GSM le procedure di autenticazione e cifratura sono strettamente collegate nella prima fase di gestione delle chiavi segrete

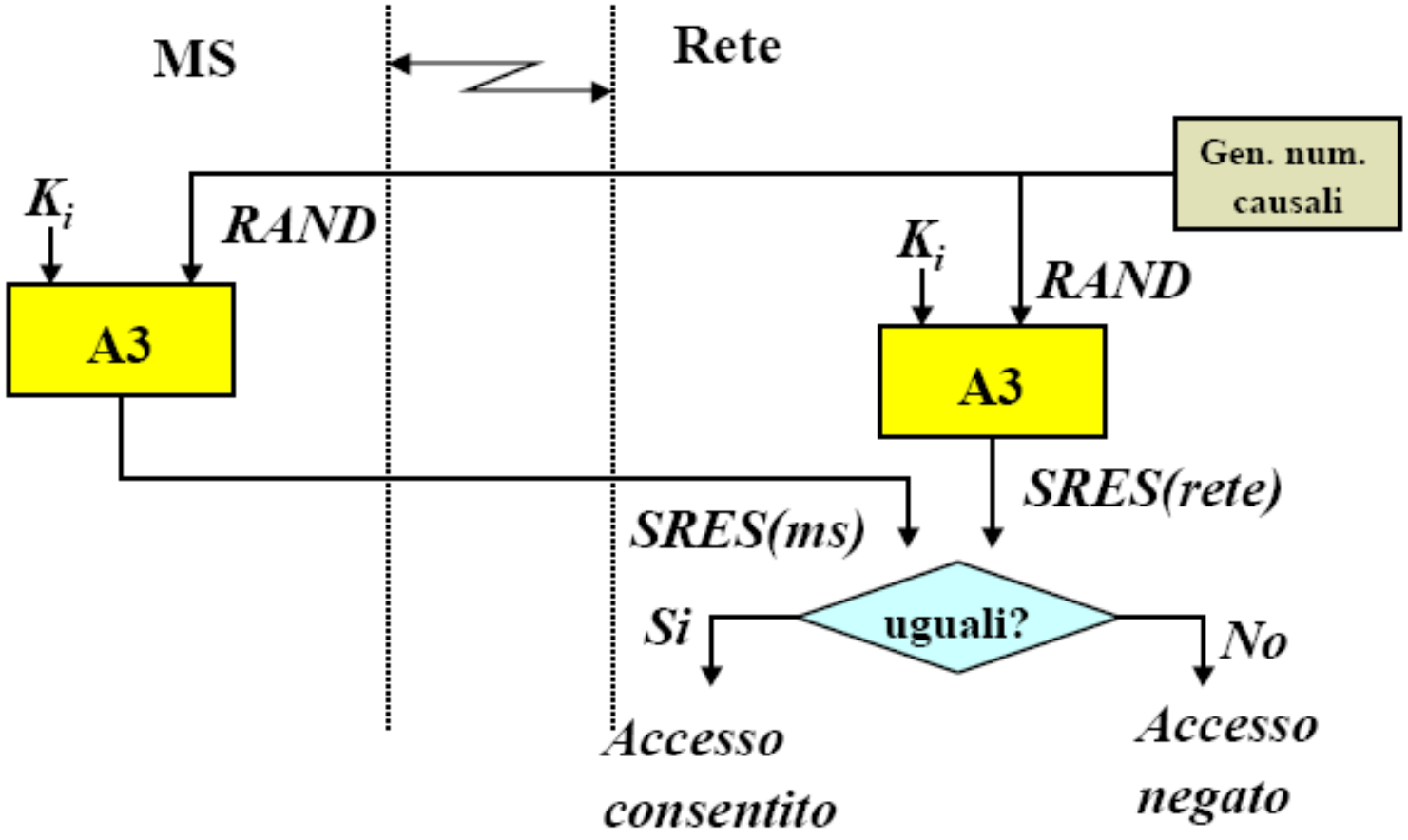
Procedure di sicurezza

- Elementi delle procedure:
  - K_i
    - chiave di autenticazione dell'utente di 128 bit memorizzata nell'AuC e nella SIM
  - *RAND*
    - numero casuale di 128 bit generato dall'AuC e poi inviato all'MSC
  - *A3*
    - algoritmo di autenticazione memorizzato nell'AuC e nella SIM
  - *A8*
    - algoritmo che determina la chiave di cifratura K_c, memorizzato nell'AuC e nella SIM
- Risultati delle procedure:
  - K_c
    - chiave di cifratura
  - *SRES*
    - risultato dell'algoritmo di autenticazione

Triplette
(*RAND*, *SRES*, K_c)
sono generate in sequenza per ogni IMSI e memorizzate nell'HLR

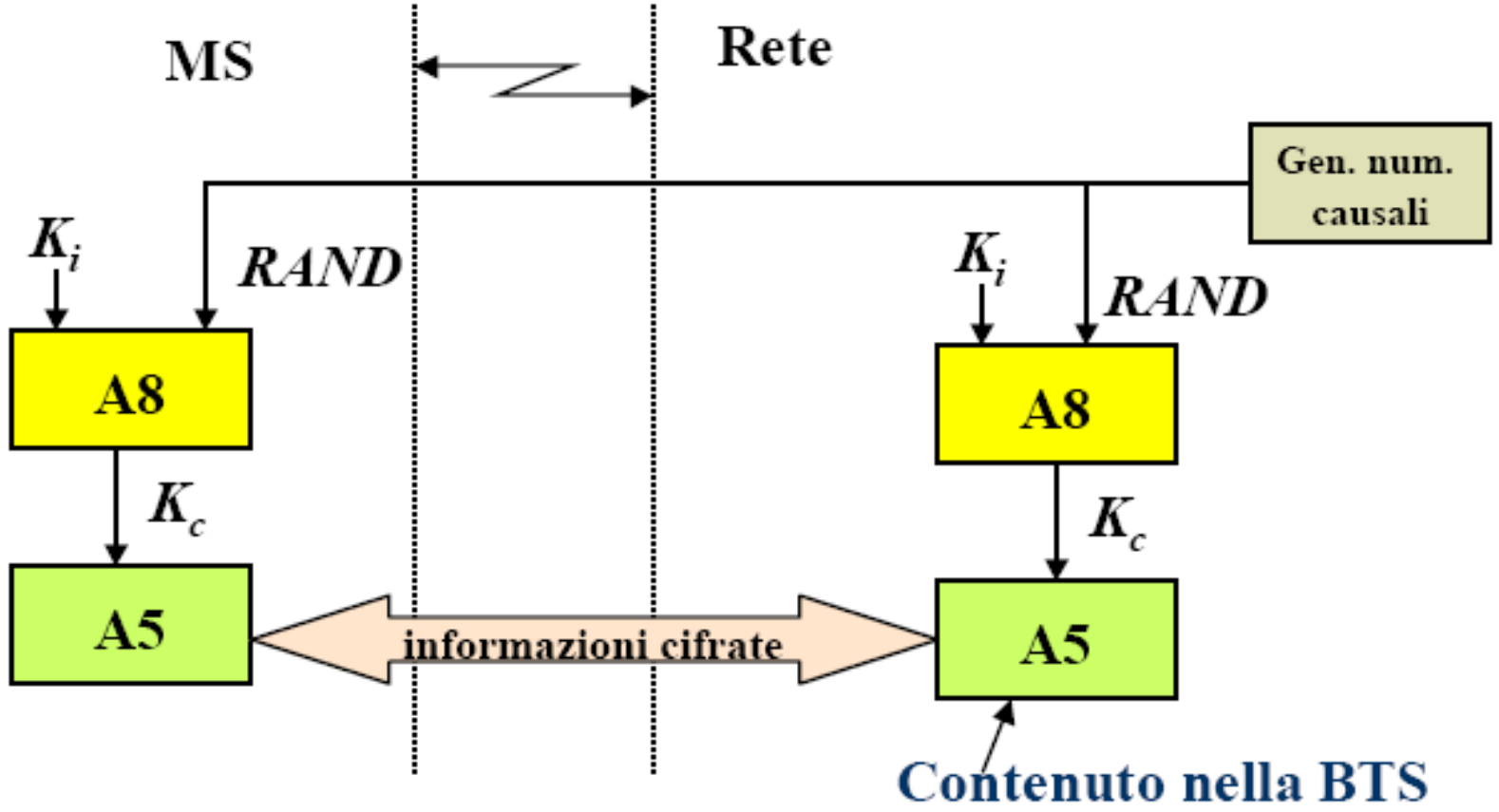
Procedure di sicurezza

- **Autenticazione:**



Procedure di sicurezza

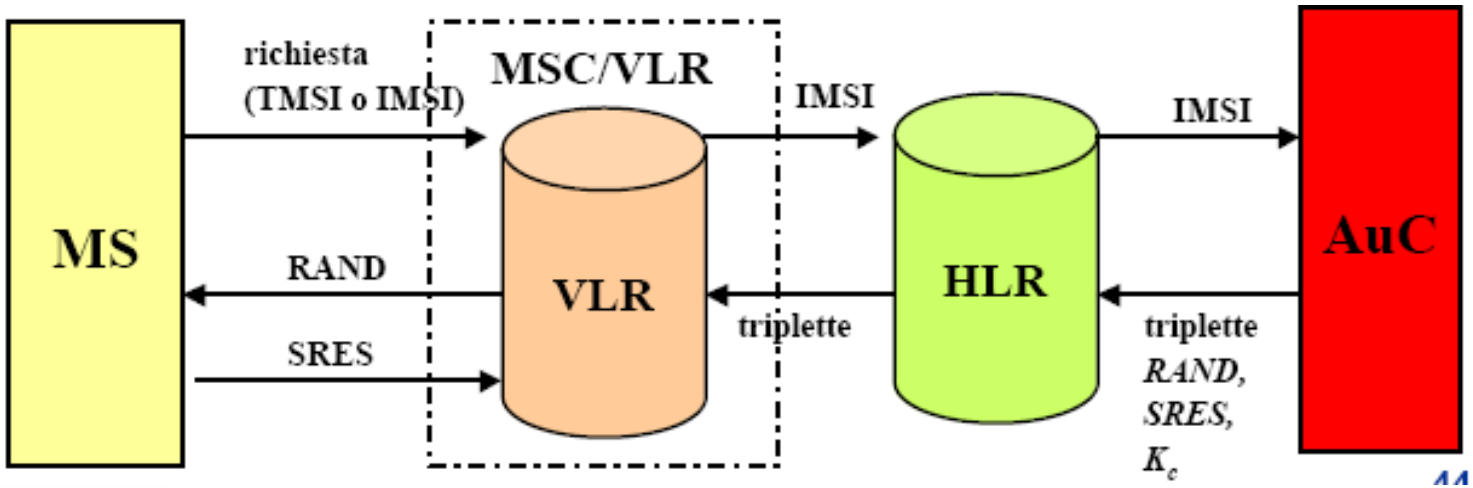
- **Cifratura:**



TechnoLabs

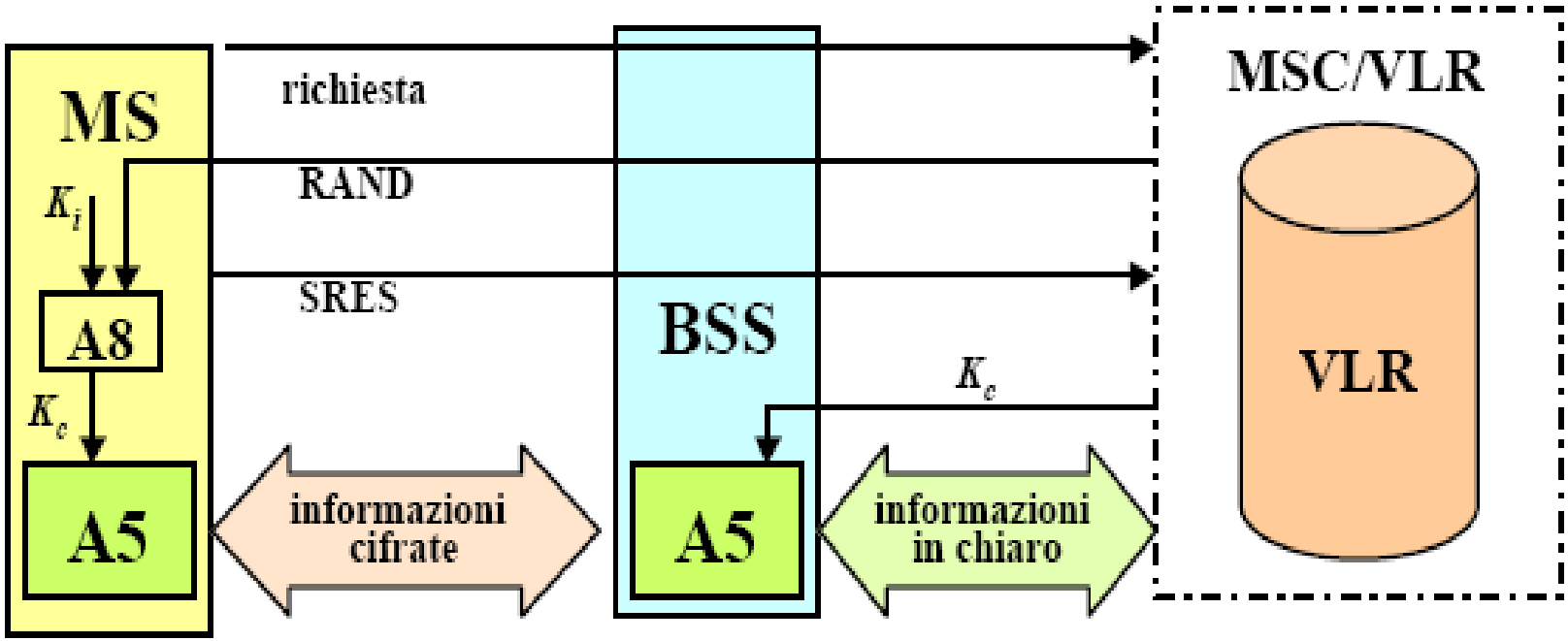
Procedure di sicurezza

- Ruolo di Autentication Centre (AuC)
  - memorizza in modo sicuro le chiavi segrete Ki di ciascun utente
  - genera i numeri casuali e calcola gli SRES e la chiave di crittazione Kc
  - Fornisce le triplette agli altri elementi di rete



Procedure di sicurezza

Ruolo del BSS nella cifratura:



Case Study

STEGANOGRAFIA

TechnoLabs

STEGANOGRAFIA

- La parola steganografia deriva dal greco e significa scrittura nascosta
- Individua una tecnica per nascondere la comunicazione tra due interlocutori
- Fu teorizzata dall'abate Tritemio attorno al 1500

STEGANOGRAFIA

- Si pone come obiettivo di mantenere nascosta l'esistenza di dati a chi non conosce la chiave adatta per estrarli
- Si differenzia dalla crittografia perché questa ha come obiettivo non rendere accessibili i dati a chi non conosce la chiave

STEGANOGRAFIA

- Può trovare uso in ogni forma di comunicazione
- Necessario che mittente e destinatario si accordino su di un codice
- È caratterizzata dalla presenza di un "contenitore" all'interno del quale è nascosto il messaggio

STEGANOGRAFIA

- La steganalisi è il procedimento mediante il quale è possibile stabilire se un dato elemento contiene dati steganografati
- La steganalisi è volta a dimostrare l'esistenza dei dati nascosti e non ad estrarli

STEGANOGRAFIA

Queste tecniche di occultamento di dati vengono suddivise in tre categorie:

- Steganografia sostitutiva
- Steganografia selettiva
- Steganografia costruttiva

STEGANOGRAFIA SOSTITUTIVA

- È la tecnica di gran lunga più diffusa
- Si basa sul fatto che la maggior parte dei canali di comunicazione (linee telefoniche, radio…) sono sempre accompagnati da un qualche tipo di rumore
- Questo rumore può essere sostituito da un segnale (il messaggio segreto) che viene trasformato in modo tale che, a meno di conoscere la chiave segreta, è indistinguibile dal rumore vero e proprio

STEGANOGRAFIA SOSTITUTIVA

- La tecnica base impiegata dalla maggior parte dei programmi, consiste nel sostituire i "bit meno significativi" delle immagini digitalizzate con i bit che costituiscono il file segreto
- I bit meno significativi sono assimilabili ai valori meno significativi di una misura, cioè quelli che tendono a essere affetti da errori
- Spesso l'immagine che ne risulta non è distinguibile a occhio nudo da quella originale

ESEMPIO PRATICO

- Prendiamo un'immagine che consiste di una matrice MxN di punti colorati (pixel) e ogni punto è rappresentato da 3 byte, che indicano rispettivamente i livelli dei colori primari rosso, verde e blu che costituiscono il colore.
- Supponiamo che uno specifico pixel di un'immagine sia rappresentato dalla tripla (12, 241, 19) in notazione binaria, le tre componenti sono:

- 12 = 00001100
- 241 = 11110001
- 19 = 00010011

ESEMPIO PRATICO

- I "bit meno significativi" dell'immagine sono gli ultimi a destra, cioè 0-1-1, e sono proprio quelli che si utilizzano per nascondere il messaggio segreto.
- Per nascondere in quel pixel l'informazione data dalla sequenza binaria 101, allora bisogna effettuare la seguente trasformazione:

00001100 --> 00001101 = 13

11110001 --> 11110000 = 240

00010011 --> 00010011 = 19

- La tripla è così diventata (13, 240, 19); si noti che questo tipo di trasformazione consiste nel sommare 1, sottrarre 1 o lasciare invariato ciascun livello di colore primario, quindi il colore risultante differisce in misura minima da quello originale.

LE ALTRE TECNICHE DI STEGANOGRAFIA

- La Steganografia selettiva ha valore solo teorico e per quanto si sappia non viene utilizzata nella pratica

- La Steganografia costruttiva tenta di sostituire il rumore presente nel medium utilizzato con l'informazione segreta opportunamente modificata in modo da imitare le caratteristiche del rumore originale

FONTI

- Wikipedia
- Articoli e riviste on line

TechnoLabs