TECNICHE DI CRITTOGRAFIA PER L'INTERNET SECURITY

SISTEMI E RETI

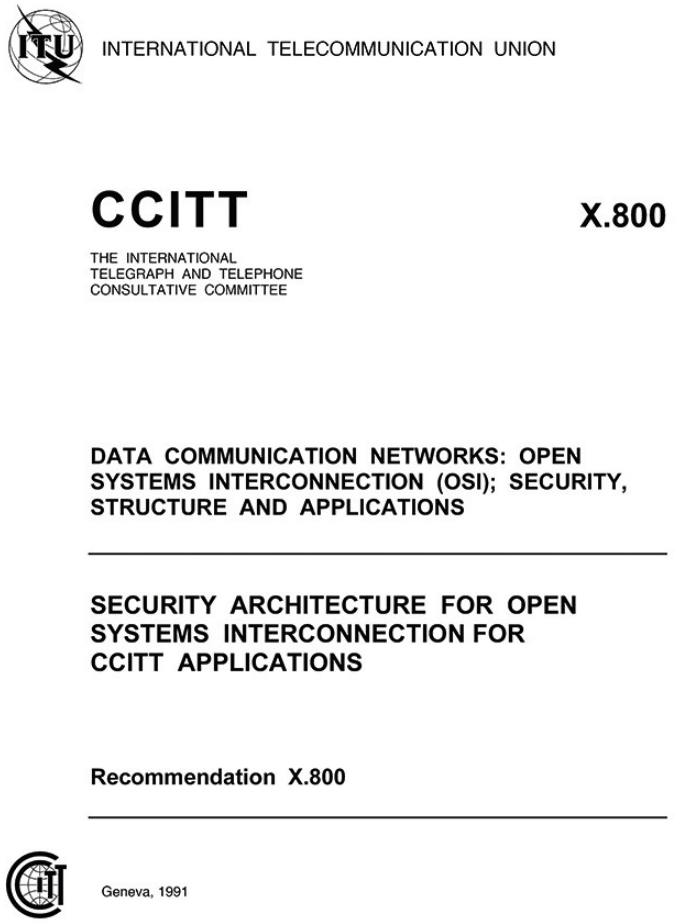
Prof. Verga - Prof.ssa Dalbesio

A.S. 2023/24

L'INTERNET SECURITY

Internet Security: insieme di misure utilizzate per proteggere i dati durante la loro trasmissione sulla rete Internet.

Alla base dell'Internet Security c'è la **Recommendation X.800 Security Architecture** dell'ITU-T



INTERNATIONAL TELECOMMUNICATION UNION

CCITT X.800

THE INTERNATIONAL
TELEGRAPH AND TELEPHONE
CONSULTATIVE COMMITTEE

DATA COMMUNICATION NETWORKS: OPEN SYSTEMS INTERCONNECTION (OSI); SECURITY, STRUCTURE AND APPLICATIONS

SECURITY ARCHITECTURE FOR OPEN SYSTEMS INTERCONNECTION FOR CCITT APPLICATIONS

Recommendation X.800

Geneva, 1991

L'INTERNET SECURITY

Requisiti di sicurezza per il sistema:

1. autenticazione;
2. controllo degli accessi;
3. confidenzialità;
4. integrità;
5. non ripudiabilità (paternità).

L'INTERNET SECURITY

Requisiti di sicurezza per il sistema:

1. **Autenticazione**:

Assicurazione dell'identità dei soggetti coinvolti nella trasmissione

L'INTERNET SECURITY

Requisiti di sicurezza per il sistema:

2. Controllo degli accessi:

Inibizione dell'uso di una risorsa da parte di soggetti non autorizzati

L'INTERNET SECURITY

Requisiti di sicurezza per il sistema:

3. Confidenzialità:

Protezione della riservatezza dei dati

(nessun soggetto terzo deve accedere ai dati dei soggetti coinvolti nella trasmissione)

L'INTERNET SECURITY

Requisiti di sicurezza per il sistema:

4. Integrità:

Assicurazione che i dati non siano stati alterati da soggetti non autorizzati

L'INTERNET SECURITY

Requisiti di sicurezza per il sistema:

5. Non-ripudiabilità:

Protezione contro la negazione di

un soggetto coinvolto nella comunicazione (paternità)

L'INTERNET SECURITY

Di seguito alcuni esempi di violazioni della sicurezza nelle trasmissioni:

- attacco passivo (*sniffing)*: la comunicazione viene ascoltata in modo non autorizzato;
- falsificazione dell'identità (*spoofing)*: *A* comunica con *B* spacciandosi per *C*;
- negazione della paternità: *A* nega di aver inviato un precedente messaggio;
- attacco attivo: nella comunicazione tra *A* e *B*, *C* intercetta i messaggi e li sostituisce con altri da esso creati;
- steganografia: informazioni celate all'interno di una comunicazione;
- rifiuto di servizio: compromissione o disabilitazione in modo non autorizzato di alcuni servizi di rete.

L'INTERNET SECURITY

Qualunque strategia si adotti, nella progettazione del servizio di sicurezza, si deve:

1. utilizzare un algoritmo per la trasformazione dei dati in chiaro in dati crittografati mediante una o più **chiavi** (la chiave è un parametro dell'algoritmo);
2. generare le chiavi da utilizzare per crittografare e decrittografare;
3. sviluppare metodi per la condivisione sicura delle chiavi;
4. specificare un protocollo che permetta di utilizzare l'algoritmo di crittografia e le chiavi segrete per comunicare in modo sicuro.

LA CRITTOGRAFIA

Crittografia: insieme di procedure con lo scopo di nascondere un messaggio a tutti tranne al destinatario.

Testo in chiaro: messaggio originale.

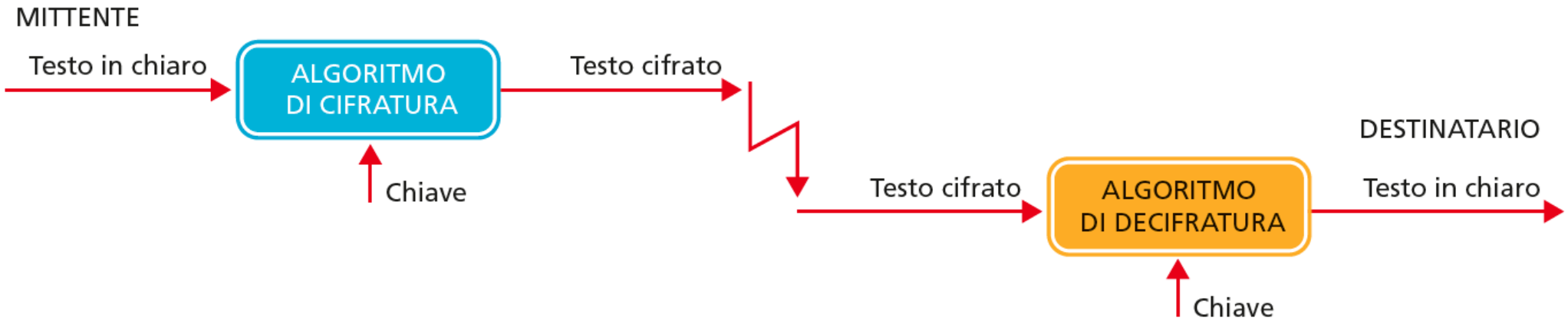
Testo cifrato: messaggio che viene trasmesso.

Chiave: sequenza finita di bit impiegata come ingresso di un **algoritmo crittografico**.

LA CRITTOGRAFIA

Per cifrare un testo occorrono essenzialmente due cose:

1. **un algoritmo di cifratura** (pubblico);
2. **una chiave** (segreta).



LA CRITTOGRAFIA

Il **testo in chiaro** è il messaggio originale, non modificato e quindi comprensibile da chiunque lo intercettasse se venisse trasmesso così com'è.

Il **testo cifrato** è il messaggio che viene trasmesso sulla rete, modificato (ma reversibile) allo scopo di renderlo incomprensibile.

La **chiave** è una sequenza di bit di lunghezza finita, generata in modo casuale e impiegata come ingresso di un algoritmo crittografico, avente un'uscita dipendente da essa.

LA CRITTOGRAFIA

Uno dei cardini della teoria della crittografia è infatti il **Principio di Kerckhoffs** che dice:
«La sicurezza di un sistema crittografico è basata esclusivamente sulla conoscenza della chiave, in pratica si presuppone noto a priori l'algoritmo di cifratura e decifratura».

La sicurezza dunque consiste nella:
1. bontà dell'algoritmo crittografico;
2. difficoltà a scoprire la chiave.

LO SAI CHE

Un sistema è sicuro quanto lo è il suo punto più debole.

LA CRITTOGRAFIA

I sistemi crittografici sono classificati in base al:

- Tipo di operazioni per trasformare il testo in chiaro in cifrato (crittografia **a sostituzione** o **a trasposizione**);
- Modo in cui il testo in chiaro è elaborato (crittografia **a blocchi** o **a flusso**);
- Numero di chiavi (a **chiave simmetrica** o **asimmetrica**).

LA CRITTOGRAFIA

I sistemi crittografici possono essere classificati in vario modo, in base al:

1. tipo di operazioni usate per trasformare il testo in chiaro in testo cifrato:
   - **crittografia a sostituzione**: ogni elemento del testo in chiaro è trasformato in un altro elemento;
   - **crittografia a trasposizione** (o permutazione): gli elementi del testo in chiaro sono riorganizzati;
2. modo in cui il testo in chiaro è elaborato:
   - **crittografia a blocchi**: il testo viene suddiviso in blocchi di N bit (dimensione fissa) e ogni blocco viene elaborato in modo indipendente dagli altri;
   - **crittografia a flusso**: elabora un quantitativo di bit variabile, senza una lunghezza predefinita;
3. numero di chiavi (distinte) utilizzate:
   - **crittografia a chiave simmetrica**: le chiavi del mittente e del destinatario sono identiche, quindi si ha una sola chiave;
   - **crittografia a chiave asimmetrica**: le chiavi sono diverse, una pubblica e una privata per ogni soggetto.

CRITTOGRAFIA A SOSTITUZIONE

Cifrario di Giulio Cesare con chiave = 5.

Alfabeto non cifrato	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
Alfabeto cifrato (chiave=5)	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E

Il Cifrario di Cesare è il più semplice esempio di crittografia a sostituzione. Scelta una chiave numerica, supponiamo 5, ogni lettera in chiaro va sostituita dalla lettera che la segue di cinque posizioni nell'alfabeto.

NB. La tabella va intesa in modo circolare: dopo la Z c'è la A.
La tecnica può essere facilmente violata
perché le chiavi possibili sono solo 26

CRITTOGRAFIA A SOSTITUZIONE

La **generalizzazione del Cifrario di Giulio Cesare** permette di rendere il cifrario più sicuro associando a ciascuna lettera del testo in chiaro una lettera scelta a caso. In questo modo la chiave, anziché un solo numero, è una sequenza di 26 numeri: ciascuno indica le posizioni da scorrere nell'alfabeto per trovare la lettera da sostituire. Per esempio: 3 (da A a D) - 9 (da B a K) - 10 (da C a M) - …; Chiave = 3-9-10-…
Il cifrario in tabella 2 è il risultato finale di 26 sostituzioni a caso.

Tabella 2 Cifrario di Giulio Cesare generalizzato

Alfabeto non cifrato	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
Alfabeto cifrato random	D	K	M	U	L	A	J	S	R	G	Q	V	H	P	I	O	E	N	X	W	Z	C	F	Y	T	B

Vi sono ora 26! possibili chiavi, cioè più di 4 miliardi di diverse sequenze da 26 cifre. La situazione è migliorata ma rimane un punto debole: ogni lettera viene sempre ancora sostituita con la stessa lettera (al posto di tutte le A del testo in chiaro ci sarà sempre una D nel testo cifrato). Questo, unito alle caratteristiche dei linguaggi naturali (Italiano, Inglese, ecc.) come la maggiore o minore frequenza di certe lettere o le ripetizioni di certi gruppi di lettere, rende questi cifrari ancora deboli.

CRITTOGRAFIA A SOSTITUZIONE

Cifrario di Vigenère supera l'ostacolo utilizzando una chiave che opera su un gruppo di lettere della stessa lunghezza della chiave (messaggio lungo come la chiave). Esso sostituisce ogni lettera in chiaro con una lettera cifrata scorrendo di tante posizioni quante sono indicate dal corrispondente numero della chiave.

CRITTOGRAFIA A SOSTITUZIONE

Cifrario di Vigenère

Con una chiave lunga 6 cifre: 3-15-2-6-21-8, otteniamo:

Testo in chiaro	O	T	T	O	B	I	T	F	A	N	N	O	U	N	B	Y	T	E
Chiave ripetuta	3	15	2	6	21	8	3	15	2	6	21	8	3	15	2	6	21	8
Testo cifrato	R	I	V	U	W	Q	W	U	C	T	I	W	X	C	D	E	0	M

In questo modo una lettera non viene sostituita sempre dalla medesima lettera, superando così il punto debole legato alle caratteristiche dei linguaggi. Il fatto che la chiave si ripeta a blocchi fissi però rende possibile violare questa cifratura.

CRITTOGRAFIA A SOSTITUZIONE

Cifrario One-Time Pad (**OTP**)
con chiave di lunghezza variabile e pari alla lunghezza del testo in chiaro;
prevede che la chiave venga utilizzata una sola volta.

Un cifrario è perfetto quando:

LunghezzaChiave ≥ LunghezzaMessaggio

Testo in chiaro	O	T	T	O	B	I	T	F	A	N	N	O	U	N	B	Y	T	E
Chiave NON ripetuta	2	16	3	6	21	2	4	14	1	6	20	8	1	15	7	6	19	5
Testo cifrato	Q	J	W	U	W	K	X	T	B	T	H	W	V	C	I	E	P	J

CRITTOGRAFIA A SOSTITUZIONE

Cifrario One-Time Pad (OTP)

Usando una chiave aleatoria lunga quanto il messaggio casuale e che cambia ogni volta si ottiene un **cifrario perfetto**.

***NB**. La chiave va cambiata ad ogni messaggio altrimenti comincerebbero ad apparire ripetizioni e somiglianze tra i messaggi inviati rompendo di fatto la sicurezza di OTP.*

La difficoltà diventa dunque da un lato generare chiavi sempre diverse, dall'altra distribuire chiavi così lunghe in modo sicuro.

CRITTOGRAFIA A TRASPOSIZIONE

Cifrario a matrice: mittente e destinatario si accordano su una chiave segreta. Il mittente scrive il testo in una matrice avente tante colonne quante sono le lettere della chiave e tante righe fino a contenere tutto il testo (riempiendo eventualmente la matrice con asterischi). Il messaggio cifrato finale si ottiene prendendo le colonne della tabella secondo l'ordine alfabetico della chiave.

CRITTOGRAFIA A TRASPOSIZIONE

Cifrario a matrice

gli elementi del testo in chiaro non sono sostituiti, ma riorganizzati.

Chiave	C	I	F	R	A
Testo	O	T	T	O	B
	I	T	F	A	N
	N	O	U	N	B
	Y	T	E	E	D
	U	E	B	Y	T
	E	F	A	N	N
	O	U	N	A	W
	O	R	D	*	*

Il messaggio cifrato da inviare risulta:

BNBDTNW*OINYUEOOTFUEBANDTTOTEFUROANEYNA*

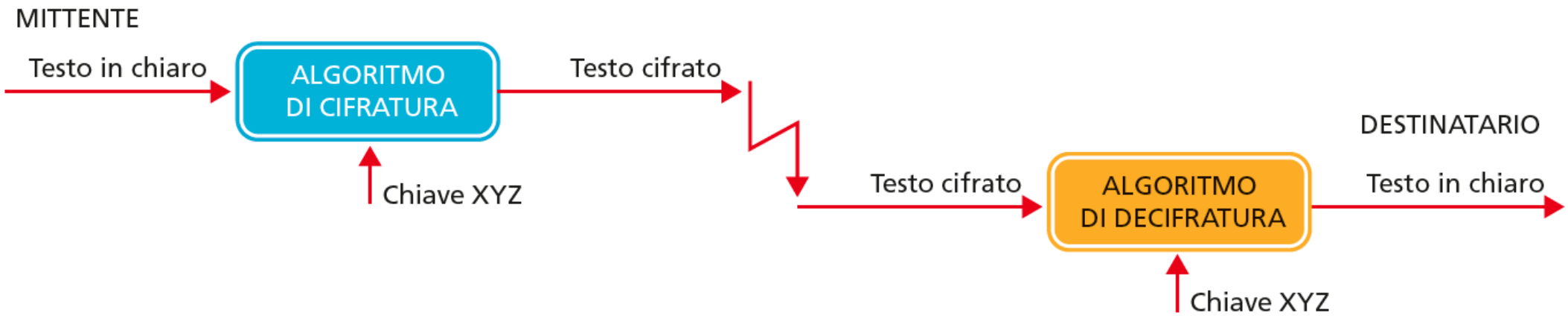
CRITTOGRAFIA A TRASPOSIZIONE

Cifrario a matrice

Il destinatario, usando la stessa chiave, è in grado di ricostruire il messaggio individuando le colonne e posizionandole correttamente.
Anche questa tecnica crittografica può facilmente essere violata: i cifrari a trasposizione non sono sicuri. L'algoritmo può essere reso più robusto effettuando due o più trasposizioni (o permutazioni) successive anziché una sola.
Tuttavia una sostituzione seguita da una trasposizione rendono il cifrario molto più resistente. I moderni sistemi crittografici sfruttano questo risultato.

CRITTOGRAFIA A CHIAVE SIMMETRICA

Si basa sull'utilizzo di una sola chiave, usata dal mittente per cifrare e dal destinatario per decifrare



CRITTOGRAFIA A CHIAVE SIMMETRICA

Metodo XOR con chiave K = 10100101

M	1	1	0	0	1	0	1	0
K	1	0	1	0	0	1	0	1
C	0	1	1	0	1	1	1	1

XOR

MITTENTE

DESTINATARIO

C	0	1	1	0	1	1	1	1
K	1	0	1	0	0	1	0	1
M	1	1	0	0	1	0	1	0

XOR

L'algoritmo di decifratura è identico a quello di cifratura

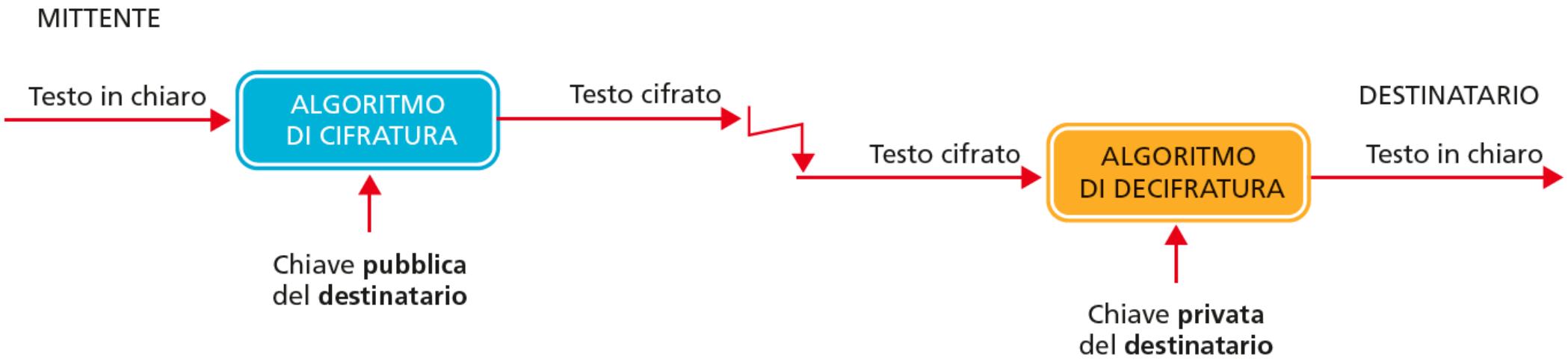
CRITTOGRAFIA A CHIAVE ASIMMETRICA

La crittografia a chiave asimmetrica (o pubblica) nasce per risolvere il problema della **distribuzione sicura** delle chiavi.

Essa utilizza due chiavi per ciascun soggetto, una **privata**, nota solo al soggetto, l'altra **pubblica**, distribuita a tutti.

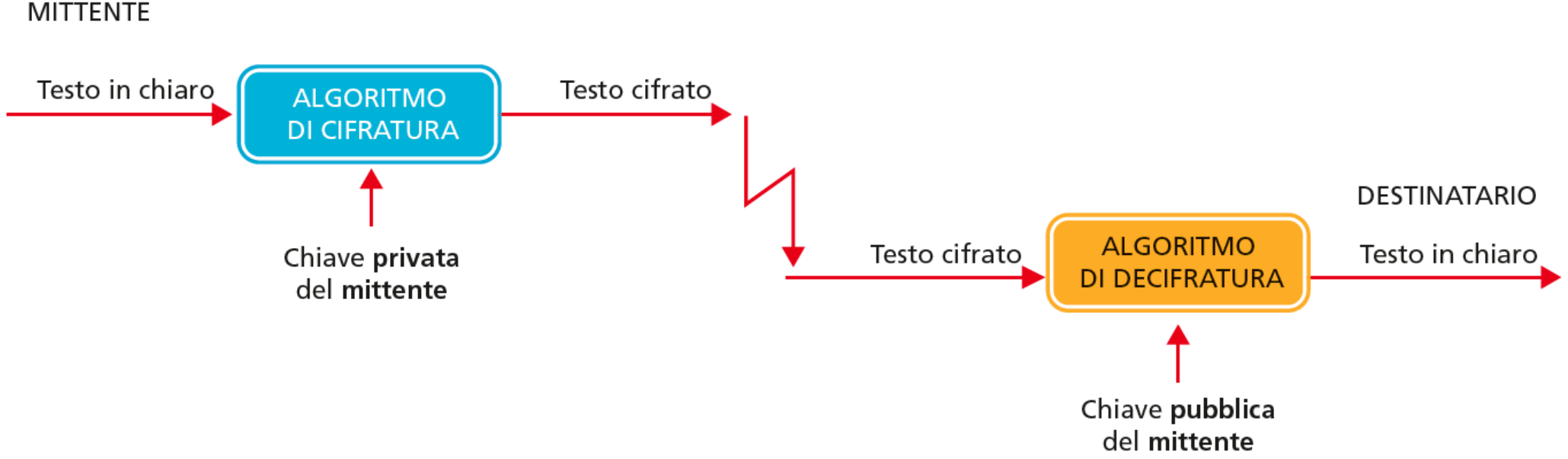
CRITTOGRAFIA A CHIAVE ASIMMETRICA

1. Assicura la riservatezza del dialogo: **confidenzialità**.



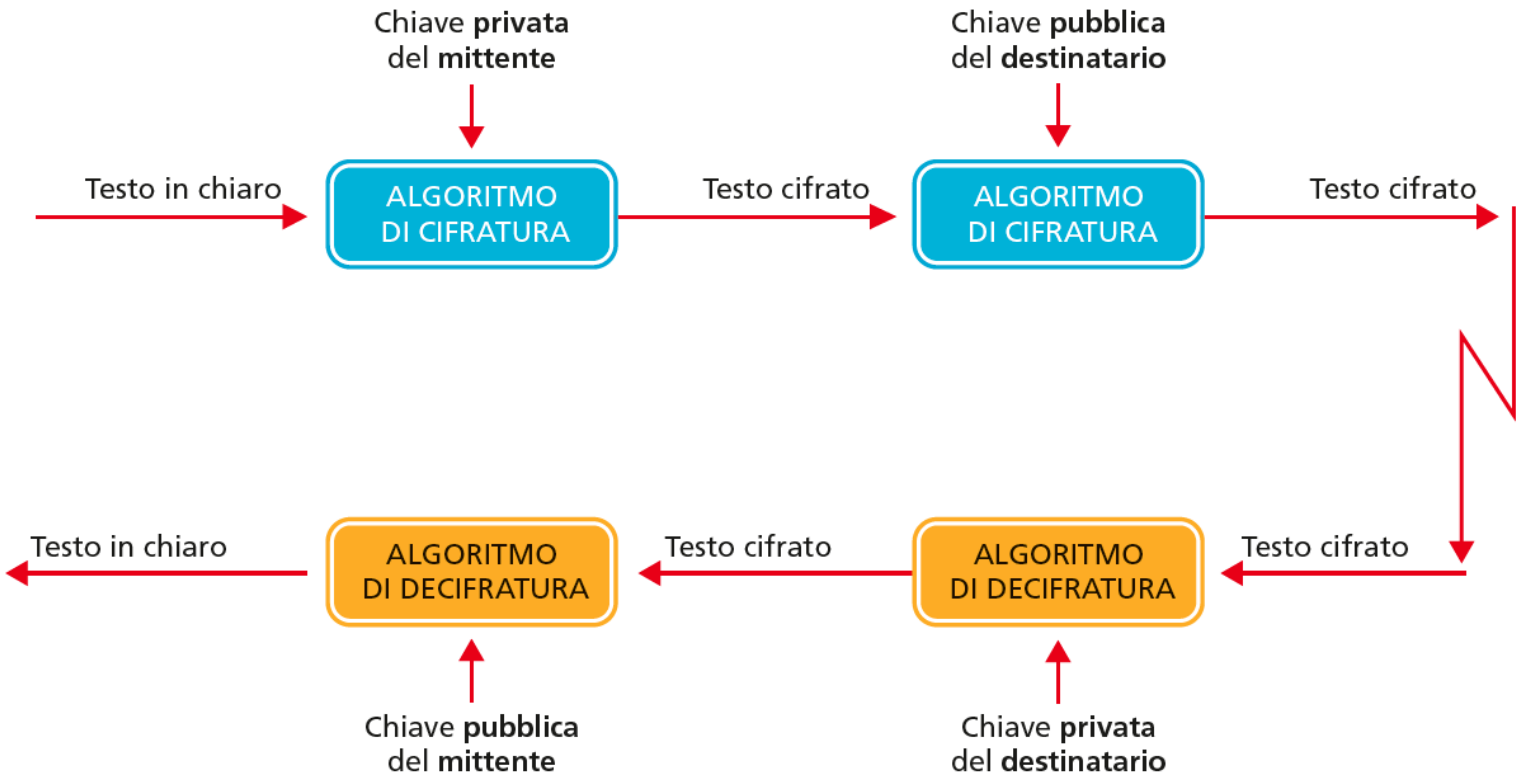
CRITTOGRAFIA A CHIAVE ASIMMETRICA

2. Garantisce l'identità del mittente: **autenticazione**.



CRITTOGRAFIA A CHIAVE ASIMMETRICA

3. Garantisce: **confidenzialità**, **autenticazione** e **integrità**.



CRITTOGRAFIA A CHIAVE ASIMMETRICA

- Per leggere un testo cifrato inviato da qualcuno occorre soltanto la chiave privata del destinatario (confidenzialità).
- Per scrivere e inviare a qualcuno un testo cifrato occorre soltanto la chiave privata del mittente (autenticazione).
- Occorre che le chiavi siano matematicamente correlate.

ALGORITMI A CHIAVE SIMMETRICA: DES

Confusione e **diffusione**

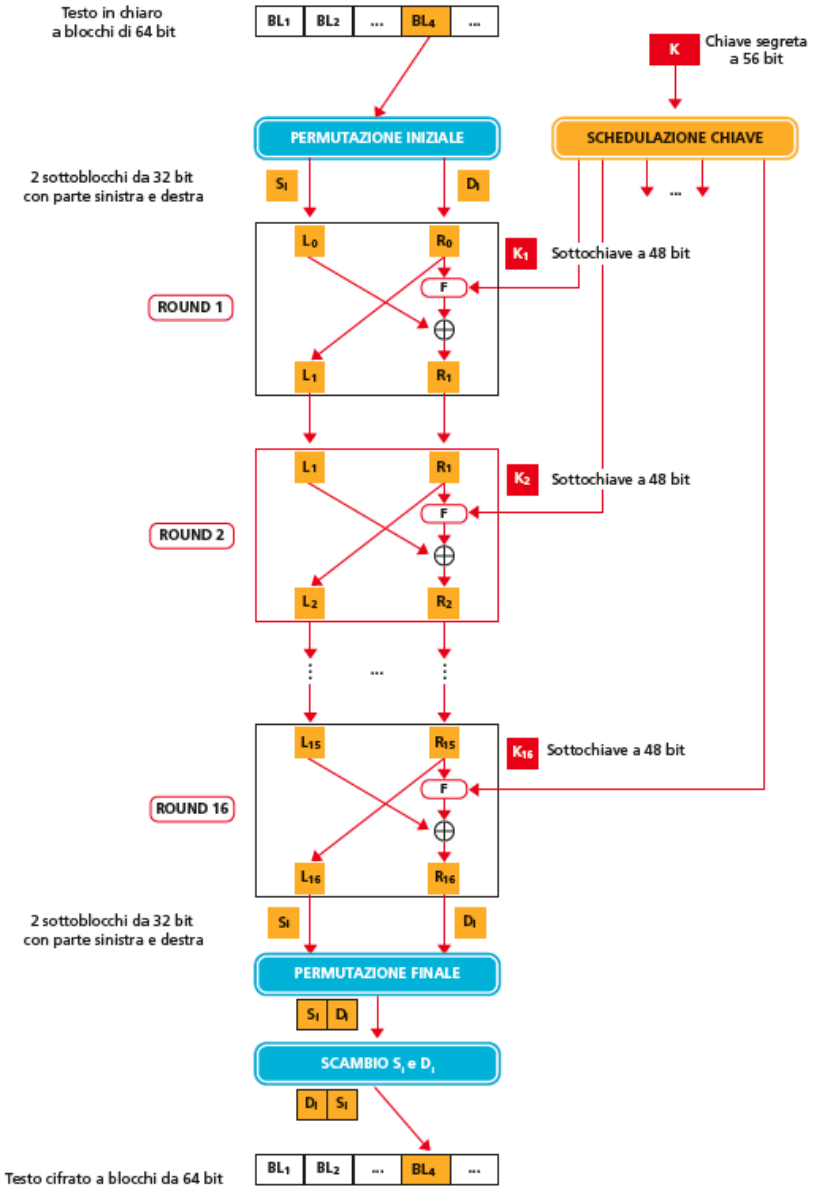
sono soddisfatte attraverso

round di permutazioni

e combinazioni

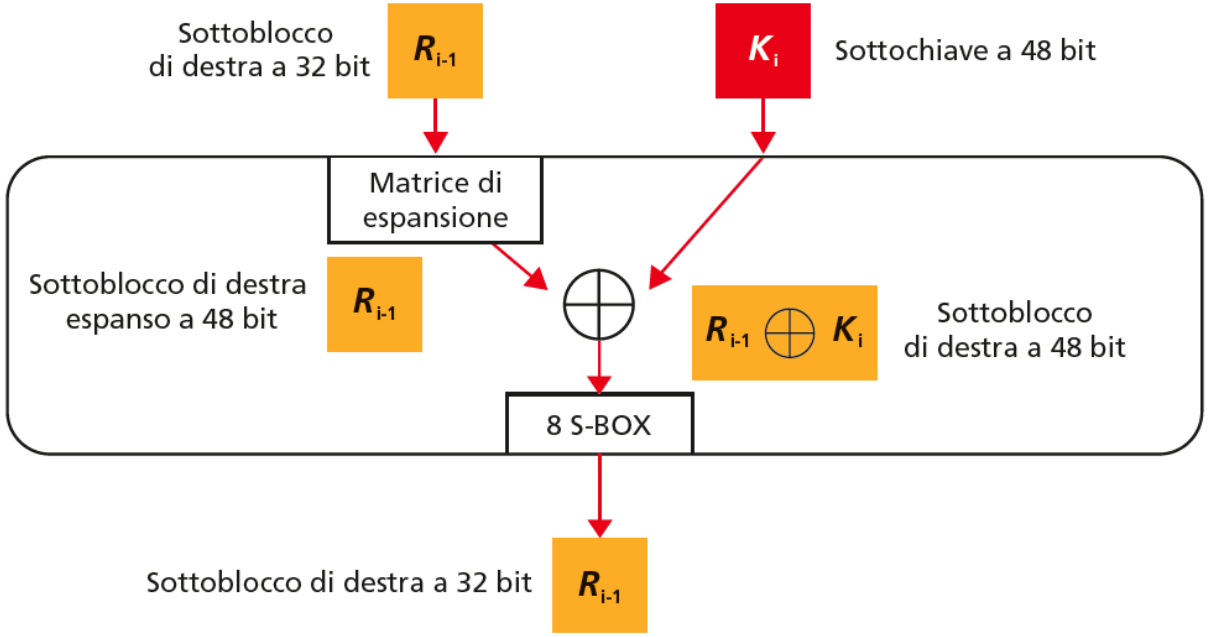
del messaggio

con la chiave.



ALGORITMI A CHIAVE SIMMETRICA: DES

Il cuore di tutto l'algoritmo è la funzione F eseguita ogni round e il cuore della funzione F è la **sostituzione S-BOX**.



ALGORITMI A CHIAVE ASIMMETRICA: RSA

Si basa sulla difficoltà nel **fattorizzare** un numero intero N ottenuto dal prodotto di due numeri che restano segreti.

TESTO IN CHIARO	m	$m^{N_{PUB}}$	TESTO CIFRATO $c = m^{N_{PUB}} \bmod N$
B	2	8.192	32
Y	25	1.490.116.119.384.765.625	60
T	20	81.920.000.000.000.000	80
E	5	1.220.703.125	20

LA FIRMA DIGITALE E GLI ENTI CERTIFICATORI

La **firma digitale**, equivalente elettronico della firma autografa su carta, è associata stabilmente al documento elettronico sulla quale è apposta e ne attesta con certezza l'**integrità**, l'**autenticità** e la **non ripudiabilità**.

Per generare una firma digitale è necessario un **kit** (dispositivo + software).

LA FIRMA DIGITALE E GLI ENTI CERTIFICATORI

Il file firmato digitalmente deve essere certificato dall'**ente certificatore** prima dell'invio.

Con il certificato il destinatario ottiene la **chiave pubblica** sicura per verificare **identità** del mittente e **integrità** del documento.

LA FIRMA DIGITALE E GLI ENTI CERTIFICATORI

L'algoritmo di apposizione della firma digitale prevede la creazione di un'**impronta** (message digest) attraverso la **funzione di hash**.