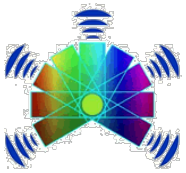
LABORATORIO

NUMERI, CODICI, CRITTOGRAFIA

presentazione



Piano Lauree Scientifiche

TOR VERGATA
UNIVERSITÀ DEGLI STUDI DI ROMA

PROBLEMA

- Comunicare in modo sicuro
- L'aggettivo 'sicuro' può avere significati differenti: vogliamo che il nostro messaggio arrivi al destinatario, che possa essere letto rapidamente dal destinatario, ma non da chi non è autorizzato.

Il problema è estremamente attuale: lo sviluppo dei sistemi elettronici facilita le comunicazioni,

ma le rende vulnerabili se non vengono adeguatamente protette.

TELECOMUNICAZIONI: TEORIA DELLA INFORMAZIONE E TEORIA DEI CODICI

- La teoria della comunicazione è lo studio teorico sui fondamenti della trasmissione di segnali tra un sistema e un altro

- La teoria dell'informazione cura l'analisi e l'elaborazione su base matematica dei fenomeni relativi alla misurazione e alla trasmissione di informazioni su un canale fisico di comunicazione

- I codici vengono usati per proteggere una certa informazione da possibili errori che potrebbero avvenire durante la trasmissione

TELECOMUNICAZIONI: TEORIA DELLA INFORMAZIONE E TEORIA DEI CODICI

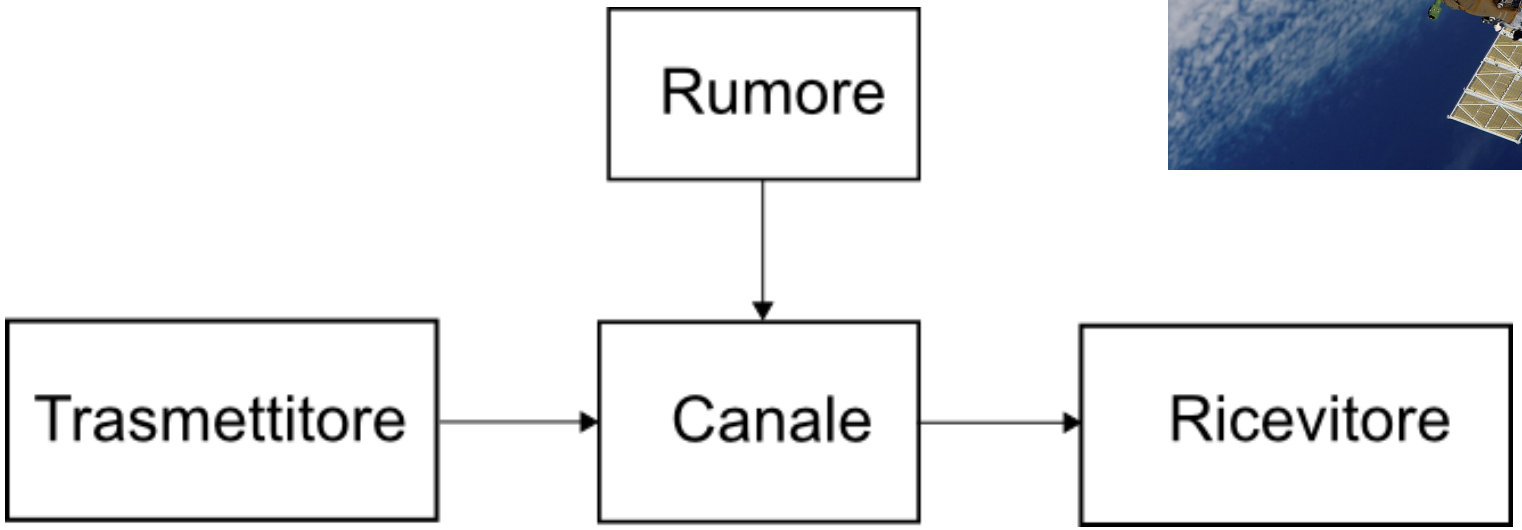


Foto: Soyuz (TMA version) Spacecraft, Wikimedia Commons,
https://commons.wikimedia.org/wiki/File:Soyuz_TMA-7_spacecraft2edit1.jpg

Esempio: La scacchiera di Polibio

Nel libro X delle Storie, (circa 200-118 a. C.)
Polibio attribuisce ai suoi contemporanei Cleoxeno e Democleito l'introduzione di un sistema di telecomunicazione (telegrafo ottico trasmesso con due gruppi di 5 torce).
Qui il sistema è adattato all'alfabeto italiano, con l'aggiunta di alcuni segni di interpunzione

a	b	c	d	e
f	g	h	i	l
m	n	o	p	q
r	s	t	u	v
z	.	,	:	?

La scacchiera di Polibio è la base per un **cifrario a colpi**. Ogni lettera è rappresentata dalla coppia di numeri che indica la sua posizione nella scacchiera, cominciando dalla prima riga:

B è 12, P è 34, V è 45

Il messaggio viene battuto lasciando una pausa più breve tra i due numeri che si riferiscono ad una lettera e una pausa più lunga tra una lettera e l'altra.

a	b	c	d	e
f	g	h	i	l
m	n	o	p	q
r	s	t	u	v
z	.	,	:	?

domani piove

143331113224 3424334515

a	b	c	d	e
f	g	h	i	l
m	n	o	p	q
r	s	t	u	v
z	.	,	:	?

Decifrate:

11 32 14 11 43 15 11 13 11 34 33 52

a n d a t e a c a p o .

Tavola 1.0 Prima parte

1) Considera la scacchiera di Polibio

a	b	c	d	e
f	g	h	i	l
m	n	o	p	q
r	s	t	u	v
z	.	,	:	?

2) Nella prima riga, scrivi un messaggio breve.
Nella seconda riga, cifra il messaggio, utilizzando la scacchiera.

3) Ricopia il messaggio cifrato nella griglia seguente:

Messaggio cifrato (Polibio)

Tavola 1.0 Prima parte: svolgimento

1) Considera la scacchiera di Polibio

a	b	c	d	e
f	g	h	i	l
m	n	o	p	q
r	s	t	u	v
z	.	,	:	?

2) Nella prima riga, scrivi un messaggio breve.
Nella seconda riga, cifra il messaggio, utilizzando la scacchiera.

a	t	t	e	n	t	o			
11	43	43	15	32	43	33			

3) Ricopia il messaggio cifrato nella griglia seguente:

Messaggio cifrato (Polibio)

Tavola 1.0 Seconda parte

4) Completa la scacchiera, inserendo l'alfabeto in modo diverso rispetto alla scacchiera di Polibio

c	m	a	r	i

5) Nella prima riga, scrivi lo stesso messaggio che avevi considerato in 3). Nella seconda riga, cifra il messaggio, utilizzando la nuova scacchiera.

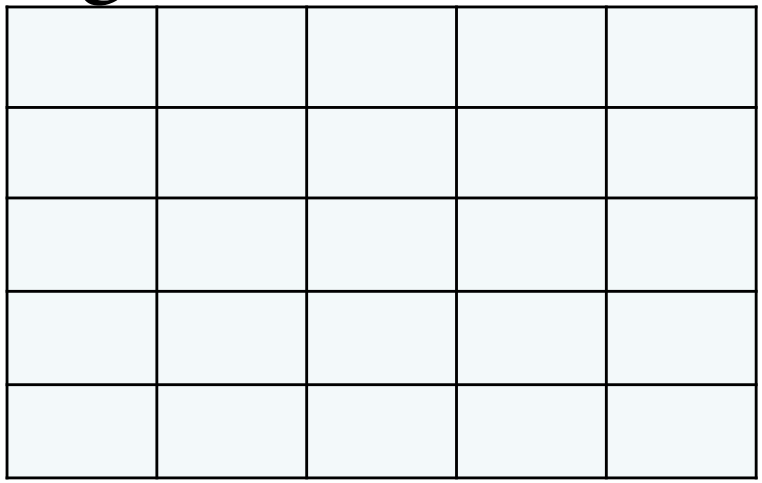
m	a	r	t	i	n	a												

3) Ricopia il messaggio cifrato nella griglia seguente:

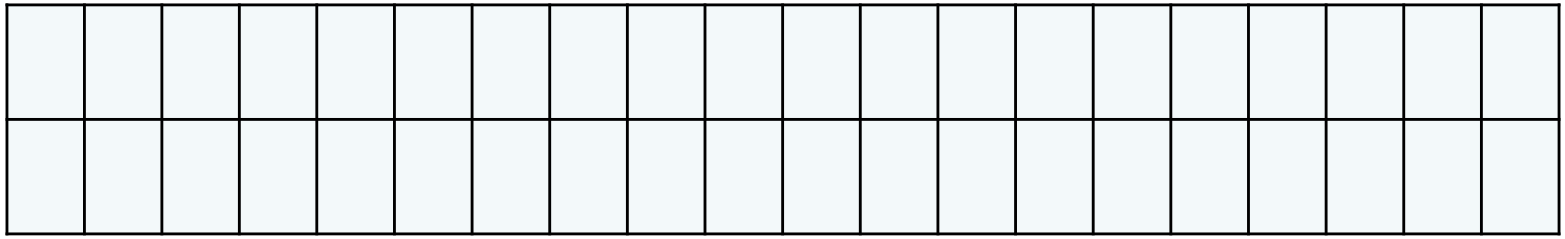
Messaggio cifrato (nuova scacchiera)

Tavola 1.0 Seconda parte: svolgimento

4) Completa la scacchiera, inserendo l'alfabeto in modo diverso rispetto alla scacchiera di Polibio



5) Nella prima riga, scrivi lo stesso messaggio che avevi considerato in 3). Nella seconda riga, cifra il messaggio, utilizzando la nuova scacchiera.



3) Ricopia il messaggio cifrato nella griglia seguente:

Messaggio cifrato (nuova scacchiera)

Tavola 1.0 Terza parte

7) La prima riga contiene il testo originario (in chiaro) del messaggio che ti è stato inviato.
La seconda riga contiene il testo cifrato

n	e	l	m	e	z	z	o	d	e	l	c	a	m	m	i	n
44	23	42	43	23	51	51	45	24	23	42	34	32	43	43	41	44

8) Riesci a ricostruire la scacchiera utilizzata per cifrare?
Inserisci tutte le lettere di cui conosci la posizione

Tavola 1.0 Terza parte: svolgimento

7) La prima riga contiene il testo originario (in chiaro) del messaggio che ti è stato inviato.
La seconda riga contiene il testo cifrato

n	e	l	m	e	z	z	o	d	e	l	c	a	m	m	i	n
44	23	42	43	23	51	51	45	24	23	42	34	32	43	43	41	44

8) Riesci a ricostruire la scacchiera utilizzata per cifrare?
Inserisci tutte le lettere di cui conosci la posizione

		e	d	
	a		c	
i	l	m	n	o
z				

Abbiamo usato:

- **Alfabeto del messaggio in chiaro**
- **Alfabeto del messaggio cifrato**
- Una **corrispondenza biunivoca tra i due alfabeti**, definita dalla forma della scacchiera e dalla distribuzione dell'alfabeto in essa (tale scelta è detta "chiave")

Caratteristiche:

- Una lettera viene cifrata sempre allo stesso modo (cifrario monoalfabetico)
- La regola che mi permette di cifrare mi spiega anche come decifrare (e viceversa)

a	b	c	d	e
f	g	h	i	l
m	n	o	p	q
r	s	t	u	v
z	.	,	:	?

- Nell'esempio della scacchiera di Polibio, abbiamo usato il seguente alfabeto per cifrare:

a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	v	z	.	,	:	?
11	12	13	14	15	21	22	23	24	25	31	32	33	34	35	41	42	43	44	45	51	52	53	54	55

- In quanti modi diversi avremmo potuto disporre il nostro alfabeto nella scacchiera?

LA CRITTOGRAFIA

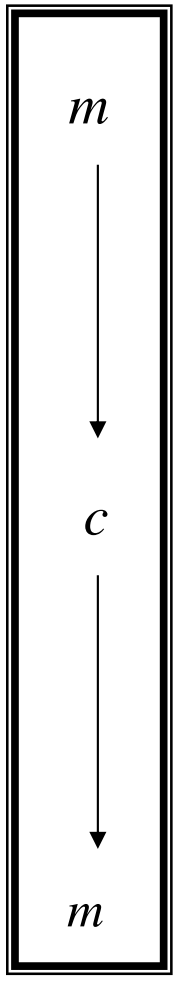
È l'arte (o una scienza?) che studia come rendere segreta e sicura la comunicazione tra due persone o entità nascondendo il significato del messaggio

canale insicuro

A

B

- Supponiamo che A voglia mandare a B un messaggio *m* (detto **messaggio in chiaro**)
- A **cifra** il messaggio *m* ottenendo un messaggio *c* (detto **messaggio cifrato**) che invia a B
- B riceve *c* e lo **decifra** riottenendo il messaggio *m*



- **Il processo di cifratura deve poter essere invertito**, in modo da permettere di ritrovare il messaggio originale
- Chi riceve il messaggio *c* deve essere in grado di interpretare ("**decifrare, decriptare**") *c*
- A e B si devono mettere d'accordo prima su come "cifrare" e "decifrare", scegliendo un metodo efficace

Segretezza: il messaggio non deve essere leggibile a terzi.

Autenticazione: il destinatario deve poter essere sicuro di chi sia il mittente.

Integrità: il destinatario deve poter essere sicuro che il messaggio non sia stato modificato.

- La crittografia fornisce **metodi effettivi** per effettuare cifratura e decifratura dei messaggi
- **Il processo di trasformazione dal messaggio in chiaro al messaggio cifrato e viceversa è spesso noto, ma si basa su una informazione specifica (detta "chiave"), senza la quale non si è in grado di operare**
- I metodi di cifratura si sono estremamente evoluti nell'arco della storia

IL CRITTOSISTEMA DI CESARE

Svetonio, nella Vita dei dodici Cesari, racconta che Giulio Cesare utilizzava un sistema di cifrazione molto semplice: ogni lettera va sostituita con quella che si trova tre posti dopo

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

Ad esempio la frase

domani attaccheremo (testo in chiaro),

diventerà

GR P DQN DZZDFFMHUHPR

Il crittosistema di Cesare

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

La decifrazione è altrettanto semplice, basta sostituire ad ogni lettera quella che si trova tre posti prima

Tavola per decifrare

A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z
u	v	z	a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t

Generalizzazione

- E' possibile **generalizzare il sistema di Cesare usando uno spostamento di k posti**, anzichè di 3.
- k deve essere un numero compreso tra 1 e 20
- Il numero k è detto "chiave"
- Ad esempio con k=7

a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	v	z
H	I	L	M	N	O	P	Q	R	S	T	U	V	Z	A	B	C	D	E	F	G

La frase dell'esempio precedente diventa

domani attaccheremo

MVTHUR HDDHLLQNBNTV

Tavola 1.1 Prima parte

1) Prepara l'alfabeto cifrante (in lettere maiuscole), spostando di 7 lettere e aiutandoti con la griglia. Il numero 7 è la chiave cifrante.

a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	v	z

2) Nella prima riga, scrivi un messaggio.
Nella seconda riga, cifra il messaggio, utilizzando l'alfabeto preparato.

3) Ricopia il messaggio cifrato nella griglia seguente:

Messaggio cifrato (Cesare, chiave 7)

Tavola 1.1 Prima parte: svolgimento

1) Prepara l'alfabeto cifrante (in lettere maiuscole), spostando di 7 lettere e aiutandoti con la griglia. Il numero 7 è la chiave cifrante.

a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	v	z
H	I	L	M	N	O	P	Q	R	S	T	U	V	Z	A	B	C	D	E	F	G

2) Nella prima riga, scrivi un messaggio.
Nella seconda riga, cifra il messaggio, utilizzando l'alfabeto preparato.

3) Ricopia il messaggio cifrato nella griglia seguente:
Messaggio cifrato (Cesare, chiave 7)

Tavola 1.1 Seconda parte

4) Hai ricevuto il seguente messaggio, cifrato mediante un cifrario di Cesare con chiave cifrante 5.
Messaggio cifrato

M	P	G	Z	F		T	B	B	P	H	F

5) A partire dalla chiave cifrante, ricava la chiave per decifrare, e decifra il messaggio, aiutandoti con la griglia con l'alfabeto.
CHIAVE CIFRANTE 5
CHIAVE PER DECIFRARE ….
Alfabeto per decifrare:

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

6) Decifra il messaggio, aiutandoti con la griglia con l'alfabeto, e riporta il messaggio decifrato nella griglia seguente

Messaggio decifrato

Tavola 1.1 Seconda parte: svolgimento

4) Hai ricevuto il seguente messaggio, cifrato mediante un cifrario di Cesare con chiave cifrante 5.
Messaggio cifrato

M	P	G	Z	F		T	B	B	P	H	F

5) A partire dalla chiave cifrante, ricava la chiave per decifrare, e decifra il messaggio, aiutandoti con la griglia con l'alfabeto.
CHIAVE CIFRANTE 5
CHIAVE PER DECIFRARE ….
Alfabeto per decifrare:

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

6) Decifra il messaggio, aiutandoti con la griglia con l'alfabeto, e riporta il messaggio decifrato nella griglia seguente

Messaggio decifrato
