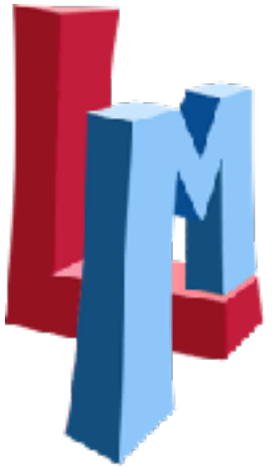
Seminario Nazionale sui Licei Matematici

3ª edizione

Fisciano, 19 settembre 2019



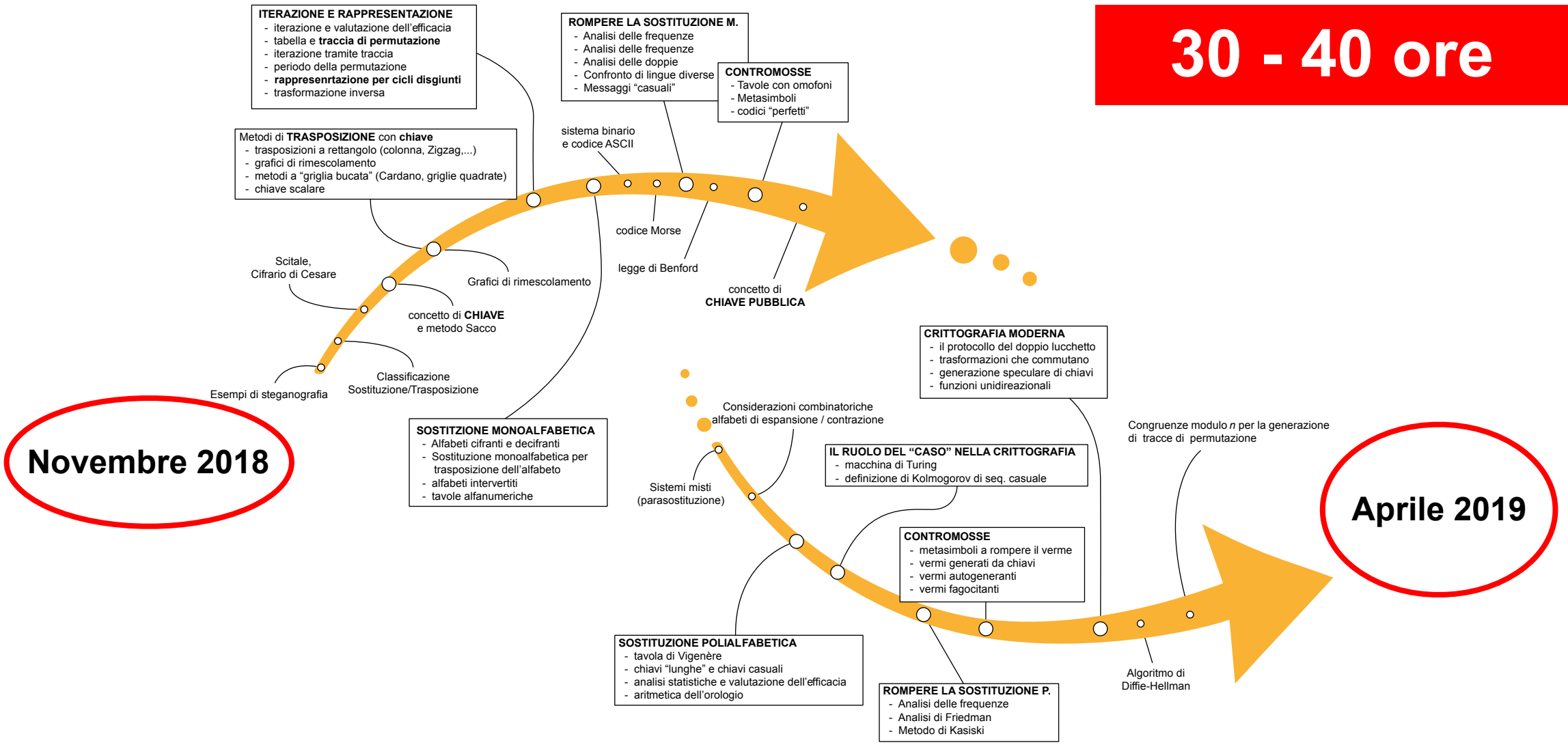
La Crittografia al Liceo Matematico

prof. Alex Saltuari

Liceo Majorana, Roma

Percorso di Crittografia svolto al Liceo Majorana di Roma

30 - 40 ore



Percorso di Crittografia svolto al Liceo Majorana di Roma

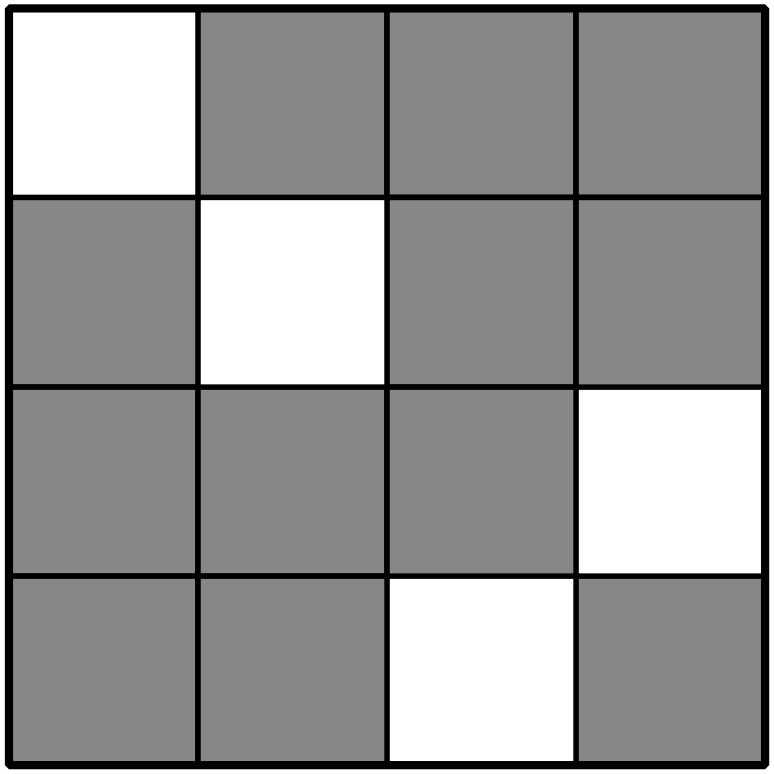
GRIGLIE DI ROTAZIONE

B	R	E	D
T	U	I	N
V	T	I	O
O	E	N	M

Percorso di Crittografia svolto al Liceo Majorana di Roma

GRIGLIE DI ROTAZIONE

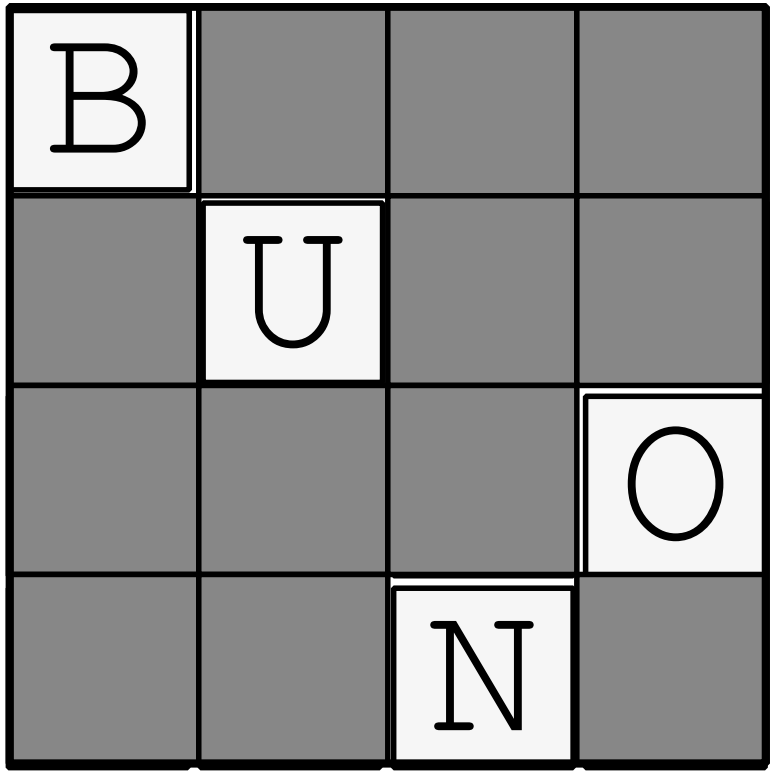
B	R	E	D
T	U	I	N
V	T	I	O
O	E	N	M



GRIGLIA DI ROTAZIONE

Percorso di Crittografia svolto al Liceo Majorana di Roma

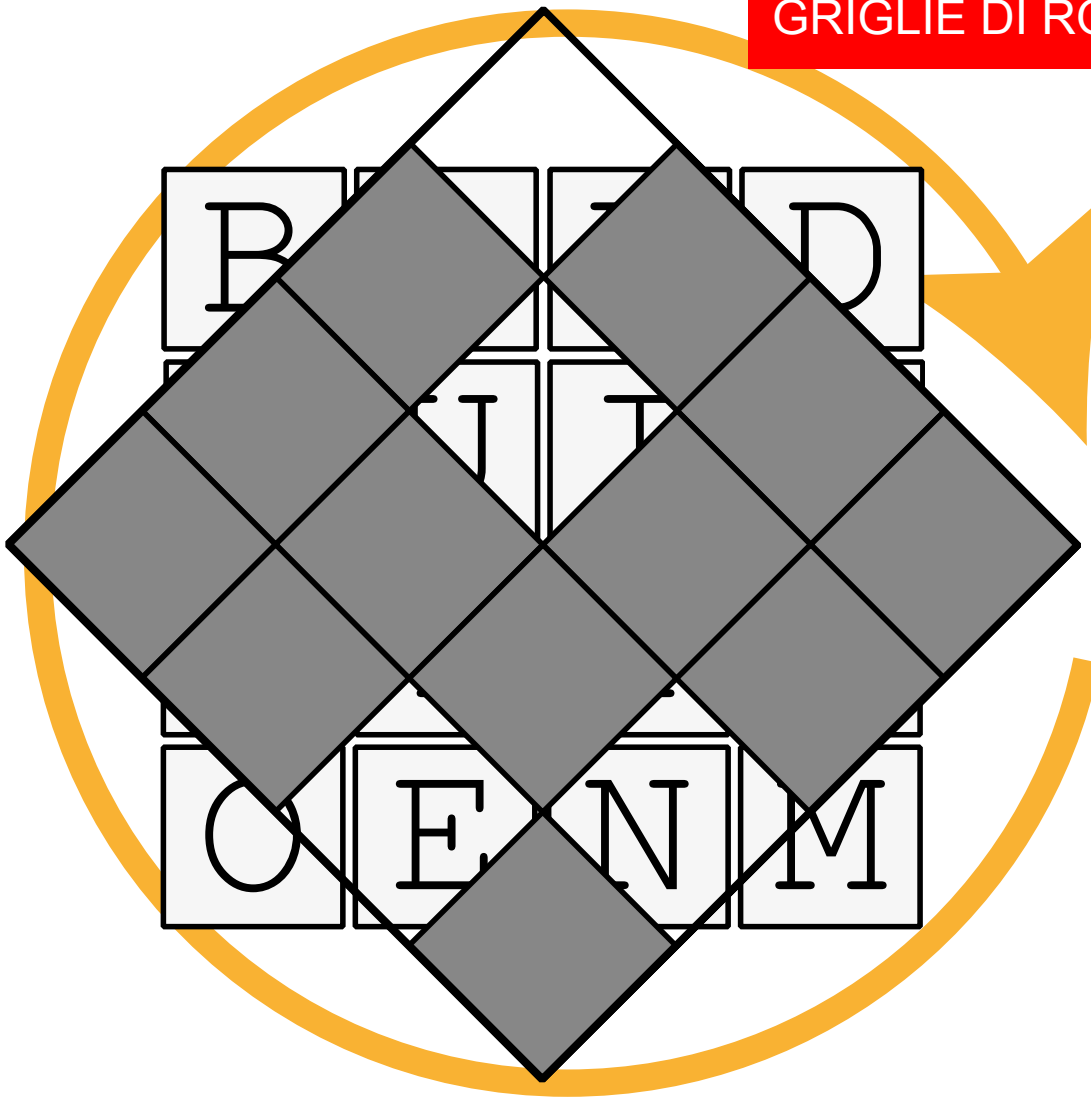
GRIGLIE DI ROTAZIONE



B U O N

Percorso di Crittografia svolto al Liceo Majorana di Roma

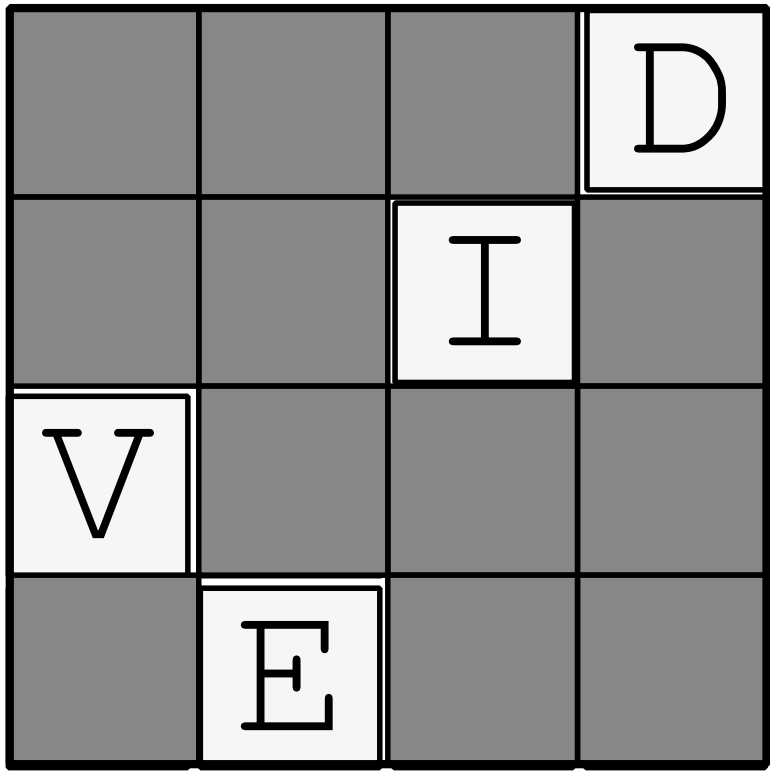
GRIGLIE DI ROTAZIONE



B U O N

Percorso di Crittografia svolto al Liceo Majorana di Roma

GRIGLIE DI ROTAZIONE

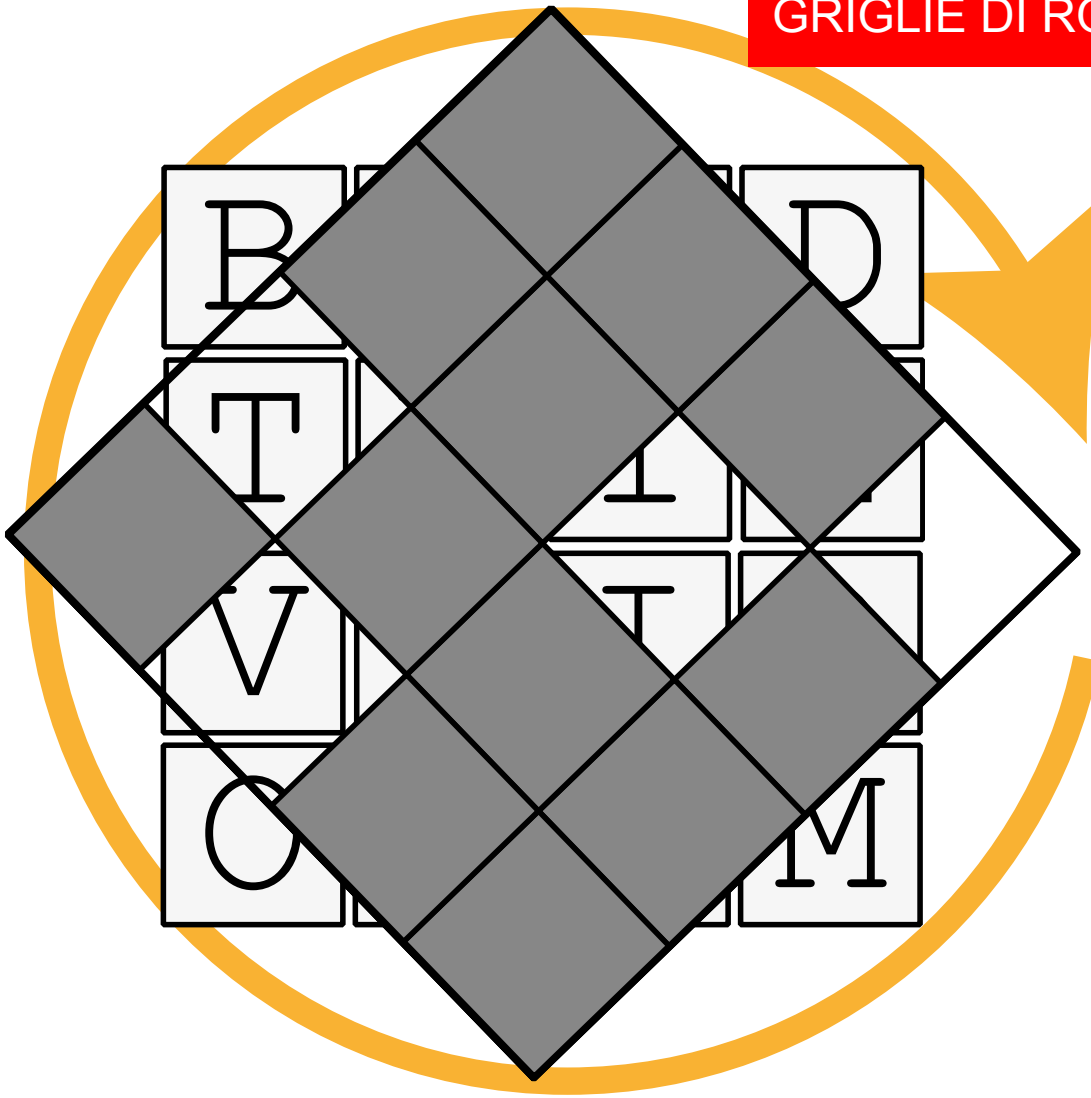


B U O N

D I V E

Percorso di Crittografia svolto al Liceo Majorana di Roma

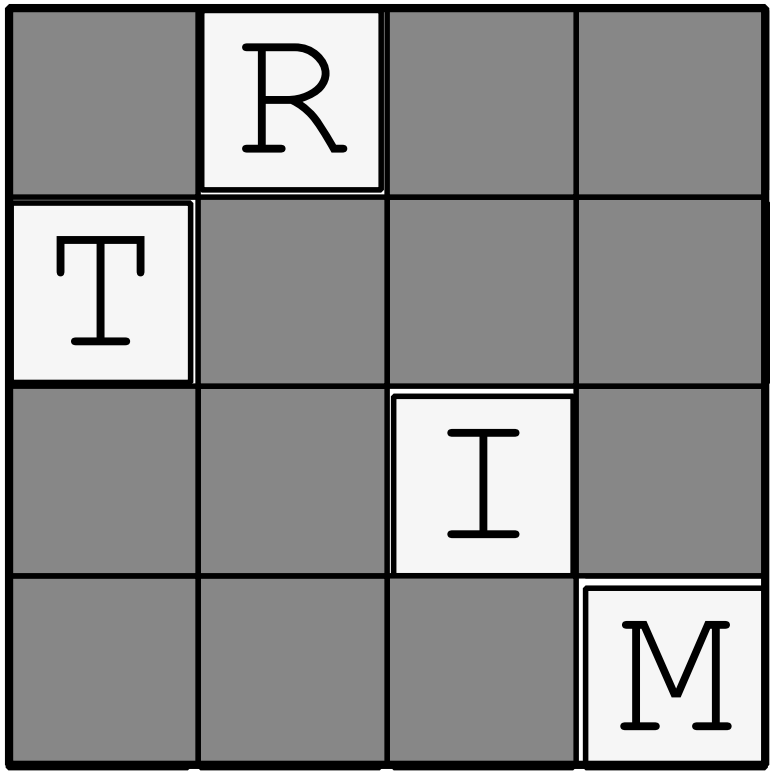
GRIGLIE DI ROTAZIONE



B U O N
D I V E

Percorso di Crittografia svolto al Liceo Majorana di Roma

GRIGLIE DI ROTAZIONE



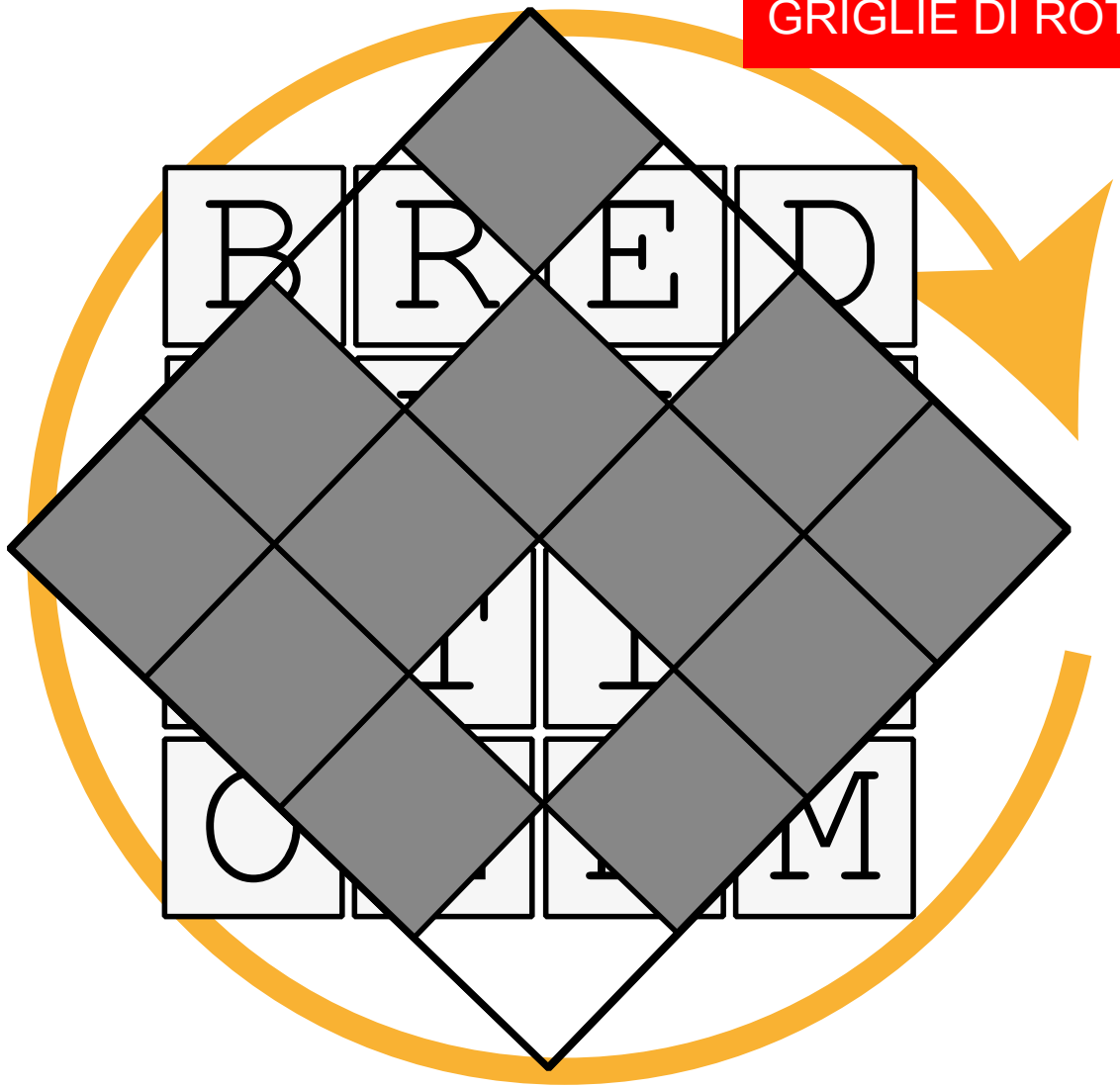
B U O N

D I V E

R T I M

Percorso di Crittografia svolto al Liceo Majorana di Roma

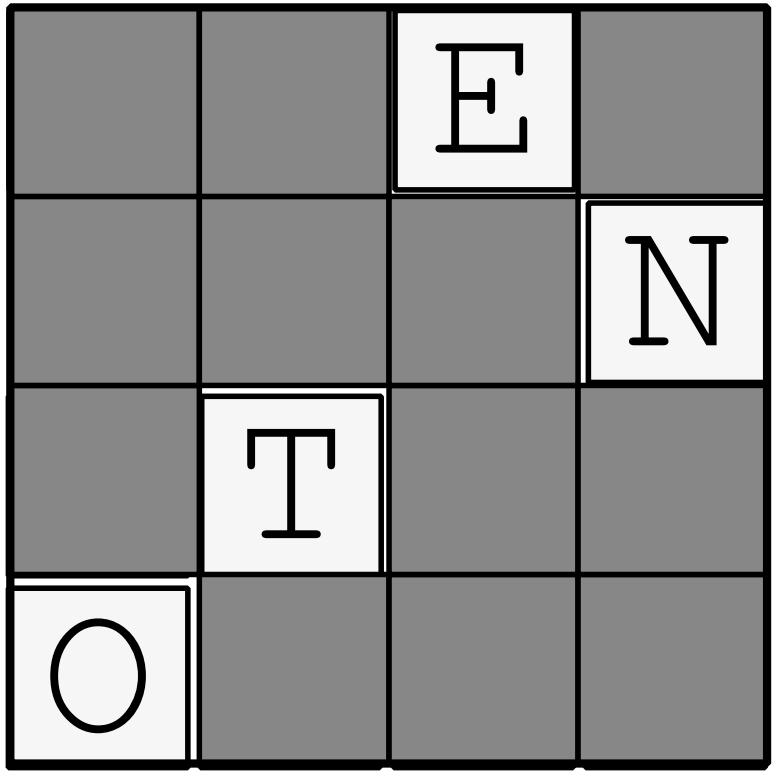
GRIGLIE DI ROTAZIONE



B U O N
D I V E
R T I M

Percorso di Crittografia svolto al Liceo Majorana di Roma

GRIGLIE DI ROTAZIONE



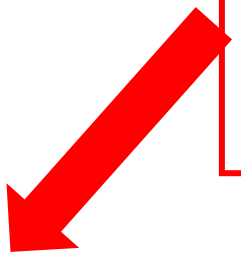
B U O N
D I V E
R T I M
E N T O

Percorso di Crittografia svolto al Liceo Majorana di Roma

GRIGLIE DI ROTAZIONE

B	R	E	D
T	U	I	N
V	T	I	O
O	E	N	M

B	U	O	N
D	I	V	E
R	T	I	M
E	N	T	O



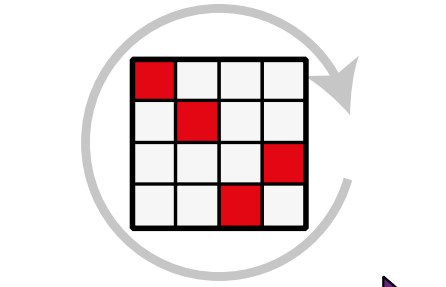
BUON DIVERTIMENTO

GRIGLIE DI ROTAZIONE

La griglia viene usata sia per decifrare che per cifrare.

BUON DIVERTIMENTO

B	U	O	N
D	I	V	E
R	T	I	M
E	N	T	O



B	R	E	D
T	U	I	N
V	T	I	O
O	E	N	M

BREDTUINVTIOENNM

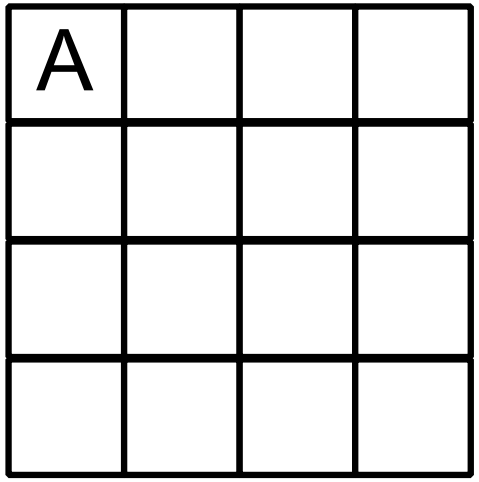
GRIGLIE DI ROTAZIONE

- Come bisogna bucare la griglia affinché sia «di rotazione»?
- Quante griglie di rotazione esistono?
- Quante griglie di rotazione esistono?
- Come posso informare il mio interlocutore della posizione dei «fori» nel modo più conciso possibile?
- Le griglie di rotazione «mescolano» bene le lettere?
- Come posso migliorare il metodo?

GRIGLIE DI ROTAZIONE

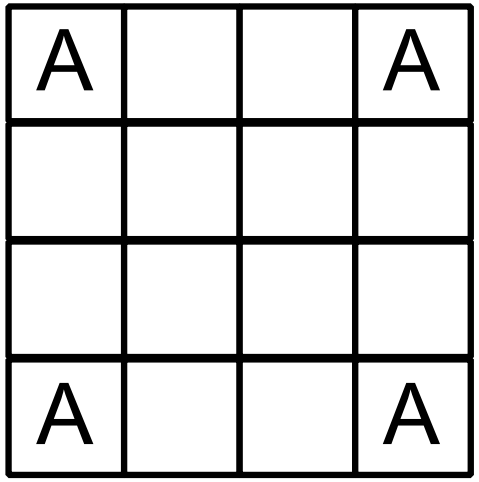
- **Come bisogna bucare la griglia affinché sia «di rotazione»?**
- Quante griglie di rotazione esistono?
- Quante griglie di rotazione esistono?
- Come posso informare il mio interlocutore della posizione dei «fori» nel modo più conciso possibile?
- Le griglie di rotazione «mescolano» bene le lettere?
- Come posso migliorare il metodo?

GRIGLIE DI ROTAZIONE



Creazione dello schema base

GRIGLIE DI ROTAZIONE



Creazione dello schema base

GRIGLIE DI ROTAZIONE

A	B		A
			B
B			
A		B	A

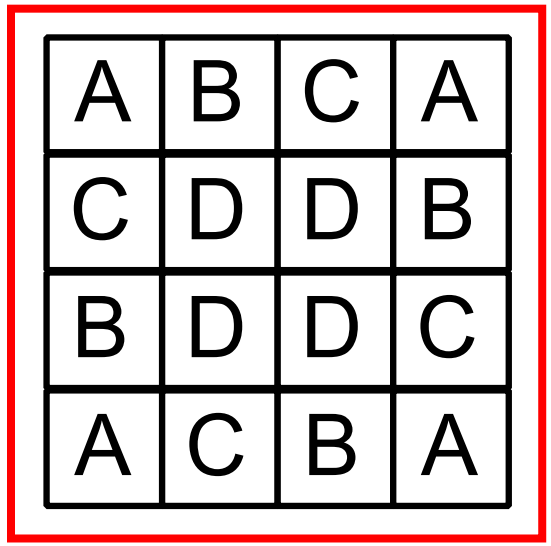
Creazione dello schema base

GRIGLIE DI ROTAZIONE

A	B	C	A
C			B
B			C
A	C	B	A

Creazione dello schema base

GRIGLIE DI ROTAZIONE



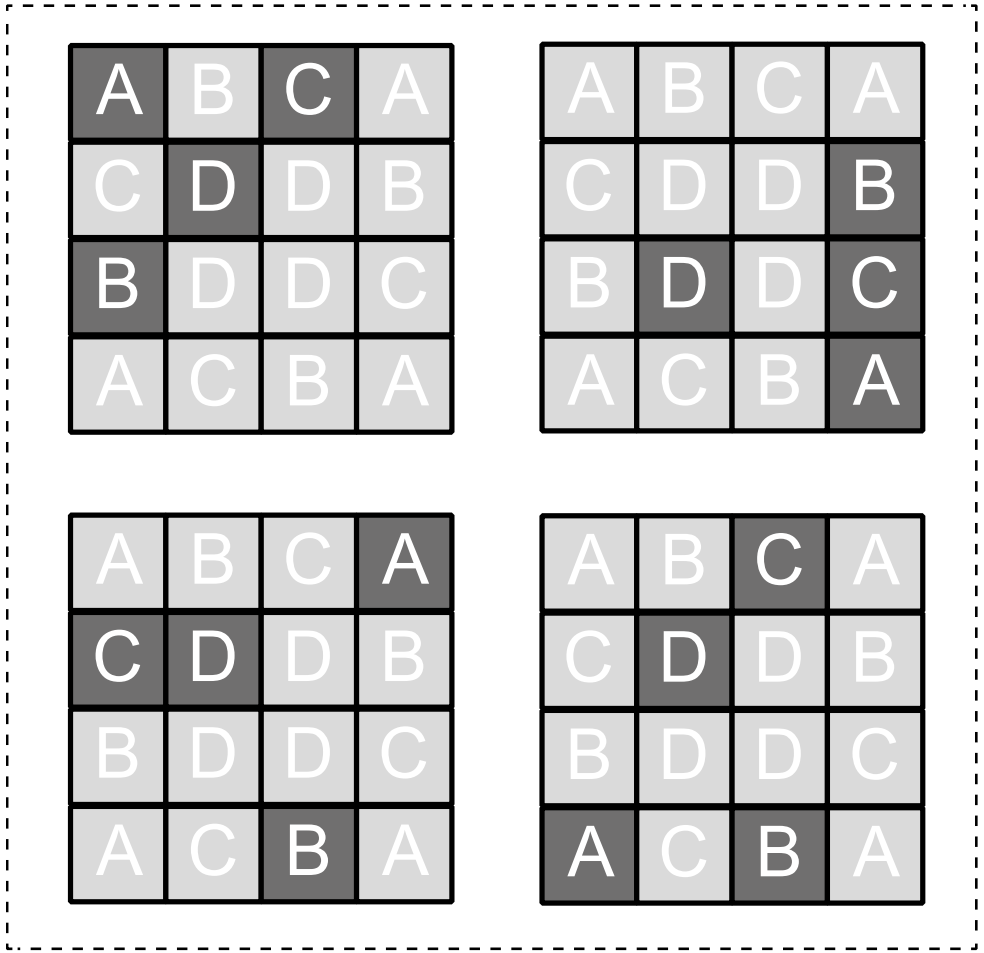
Schema base

GRIGLIE DI ROTAZIONE

A	B	C	A
C	D	D	B
B	D	D	C
A	C	B	A

Schema base

Esempi



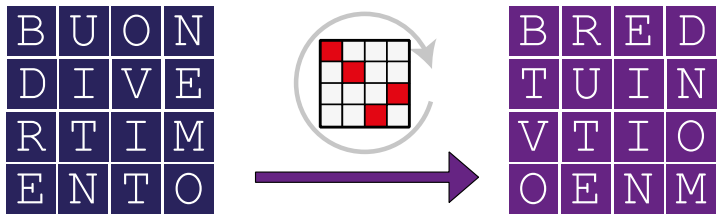
GRIGLIE DI ROTAZIONE

- Come bisogna bucare la griglia affinché sia «di rotazione»?
- Quante griglie di rotazione esistono?
- Quante griglie di rotazione esistono?
- Come posso informare il mio interlocutore della posizione dei «fori» nel modo più conciso possibile?
- Le griglie di rotazione «mescolano» bene le lettere?
- **Come posso migliorare il metodo?**

Percorso di Crittografia svolto al Liceo Majorana di Roma

GRIGLIE DI ROTAZIONE

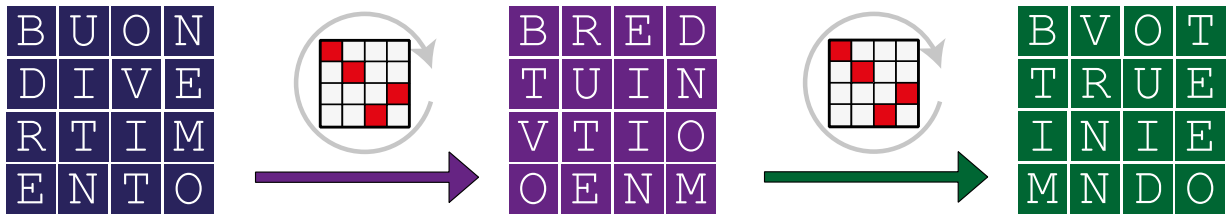
B	U	O	N	D	I	V	E	R	T	I	M	E	N	T	O
B	R	E	D	T	U	I	N	V	T	I	O	E	N	N	M



Percorso di Crittografia svolto al Liceo Majorana di Roma

GRIGLIE DI ROTAZIONE

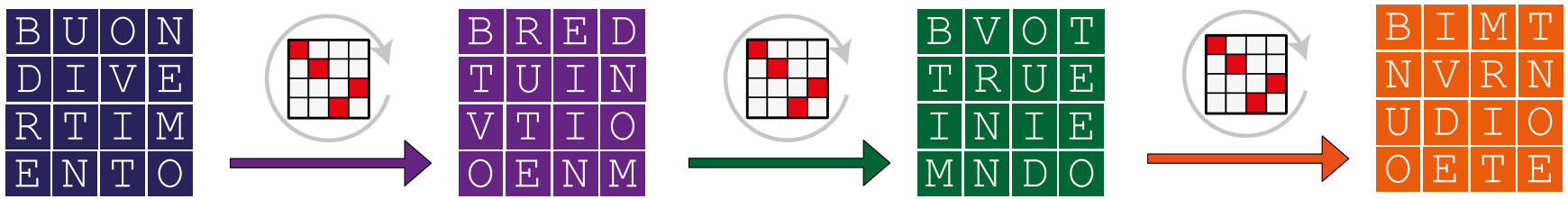
B	U	O	N	D	I	V	E	R	T	I	M	E	N	T	O
B	R	E	D	T	U	I	N	V	T	I	O	E	N	N	M
B	V	O	T	T	R	U	E	I	N	I	E	M	N	D	O



Percorso di Crittografia svolto al Liceo Majorana di Roma

GRIGLIE DI ROTAZIONE

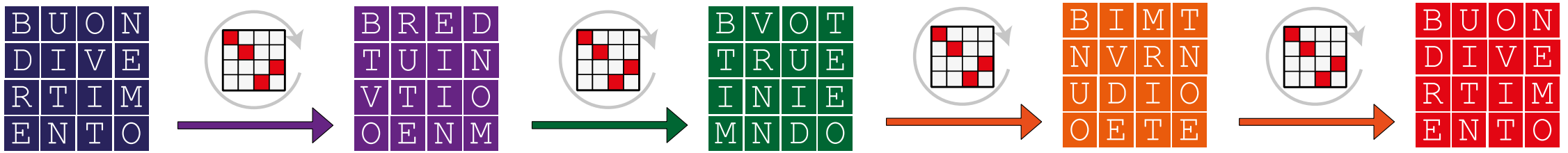
B	U	O	N	D	I	V	E	R	T	I	M	E	N	T	O
B	R	E	D	T	U	I	N	V	T	I	O	E	N	N	M
B	V	O	T	T	R	U	E	I	N	I	E	M	N	D	O
B	I	M	T	N	V	R	N	U	D	I	O	O	E	T	E



Percorso di Crittografia svolto al Liceo Majorana di Roma

GRIGLIE DI ROTAZIONE

B	U	O	N	D	I	V	E	R	T	I	M	E	N	T	O
B	R	E	D	T	U	I	N	V	T	I	O	E	N	N	M
B	V	O	T	T	R	U	E	I	N	I	E	M	N	D	O
B	I	M	T	N	V	R	N	U	D	I	O	O	E	T	E
B	U	O	N	D	I	V	E	R	T	I	M	E	N	T	O



GRIGLIE DI ROTAZIONE

B U O N D I V E R T I M E N T O

Disastro!

B U O N D I V E R T I M E N T O

Applicando il metodo 4 volte le lettere si rimettono in ordine. **Perché è successo?**

Percorso di Crittografia svolto al Liceo Majorana di Roma

GRIGLIE DI ROTAZIONE

T^0	B	U	O	N	D	I	V	E	R	T	I	M	E	N	T	O
T^1	B	R	E	D	T	U	I	N	V	T	I	O	E	N	N	M
T^2	B	V	O	T	T	R	U	E	I	N	I	E	M	N	D	O
T^3	B	I	M	T	N	V	R	N	U	D	I	O	O	E	T	E
T^4	B	U	O	N	D	I	V	E	R	T	I	M	E	N	T	O

Studiamo la permutazione

Percorso di Crittografia svolto al Liceo Majorana di Roma

GRIGLIE DI ROTAZIONE

T^0	B	U	O	N	D	I	V	E	R	T	I	M	E	N	T	O
T^1	B	R	E	D	T	U	I	N	V	T	I	O	E	N	N	M
T^2	B	V	O	T	T	R	U	E	I	N	I	E	M	N	D	O
T^3	B	I	M	T	N	V	R	N	U	D	I	O	O	E	T	E
T^4	B	U	O	N	D	I	V	E	R	T	I	M	E	N	T	O

LA B NON CAMBIA MAI POSIZIONE

Percorso di Crittografia svolto al Liceo Majorana di Roma

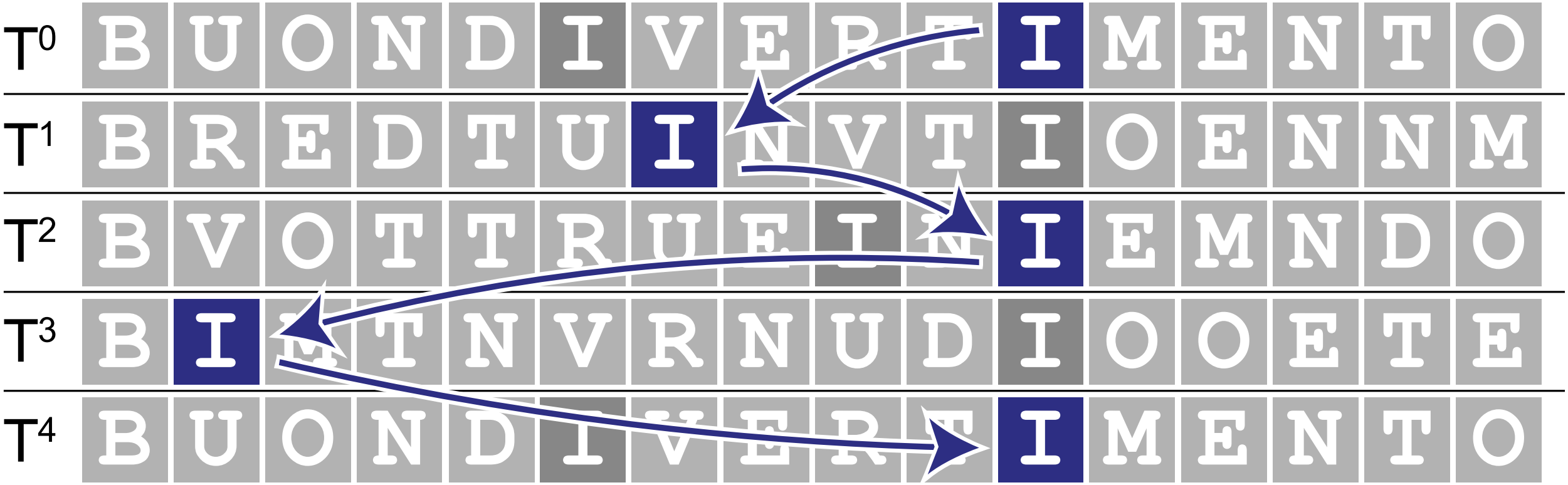
GRIGLIE DI ROTAZIONE

T^0	B	U	O	N	D	I	V	E	R	T	I	M	E	N	T	O
T^1	B	R	E	D	T	U	I	N	V	T	I	O	E	N	N	M
T^2	B	V	O	T	T	R	U	E	I	N	I	E	M	N	D	O
T^3	B	I	M	T	N	V	R	N	U	D	I	O	O	E	T	E
T^4	B	U	O	N	D	I	V	E	R	T	I	M	E	N	T	O

ANCHE LA I NON CAMBIA MAI POSIZIONE

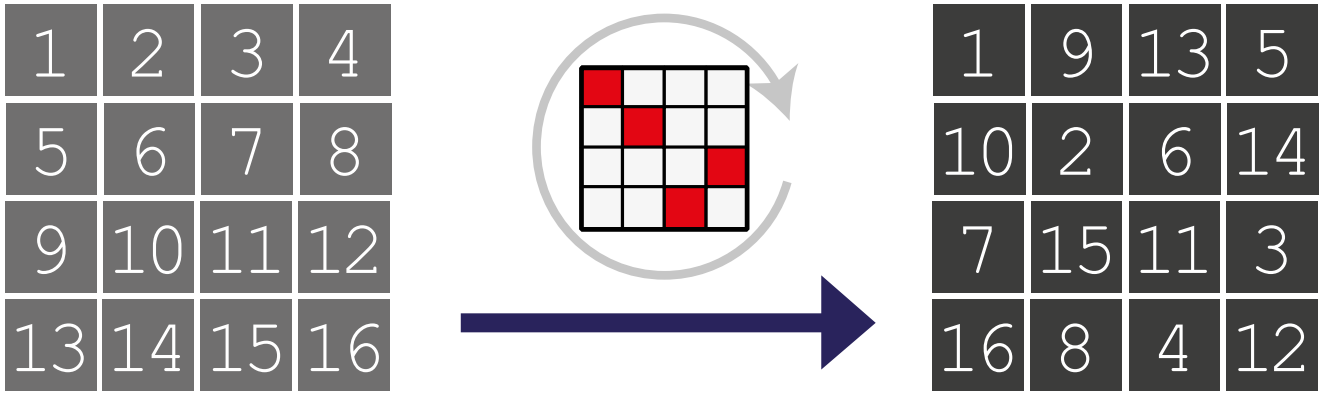
Percorso di Crittografia svolto al Liceo Majorana di Roma

GRIGLIE DI ROTAZIONE



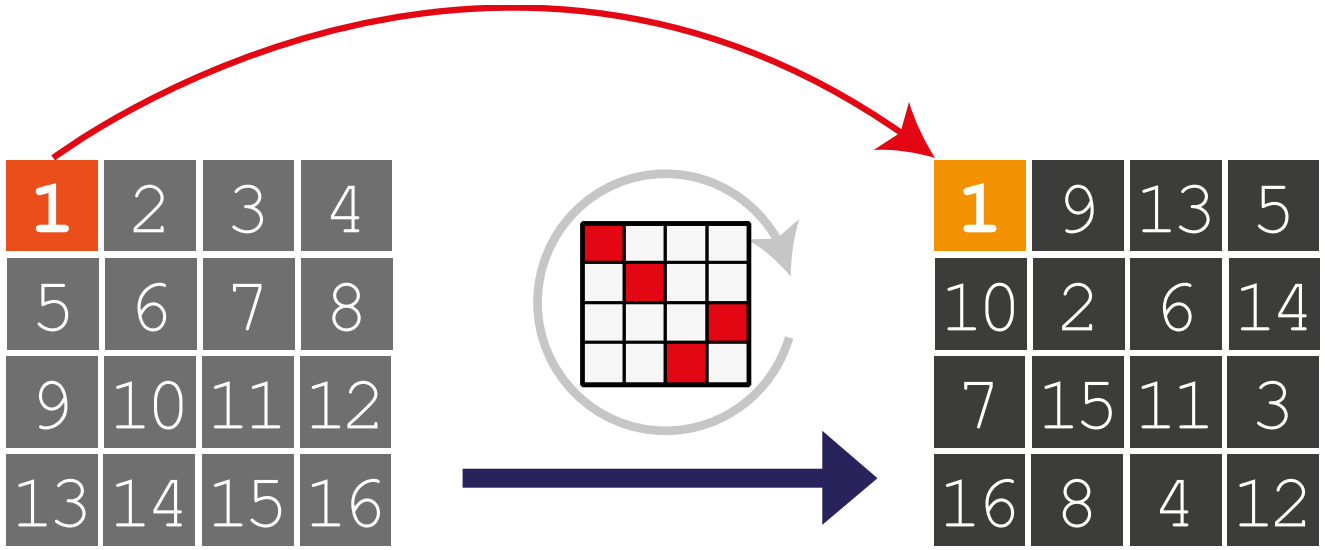
OPPURE SÌ?

GRIGLIE DI ROTAZIONE



Studiamo la permutazione applicando la trasformazione al messaggio «1,2,3,4,…,16»

GRIGLIE DI ROTAZIONE

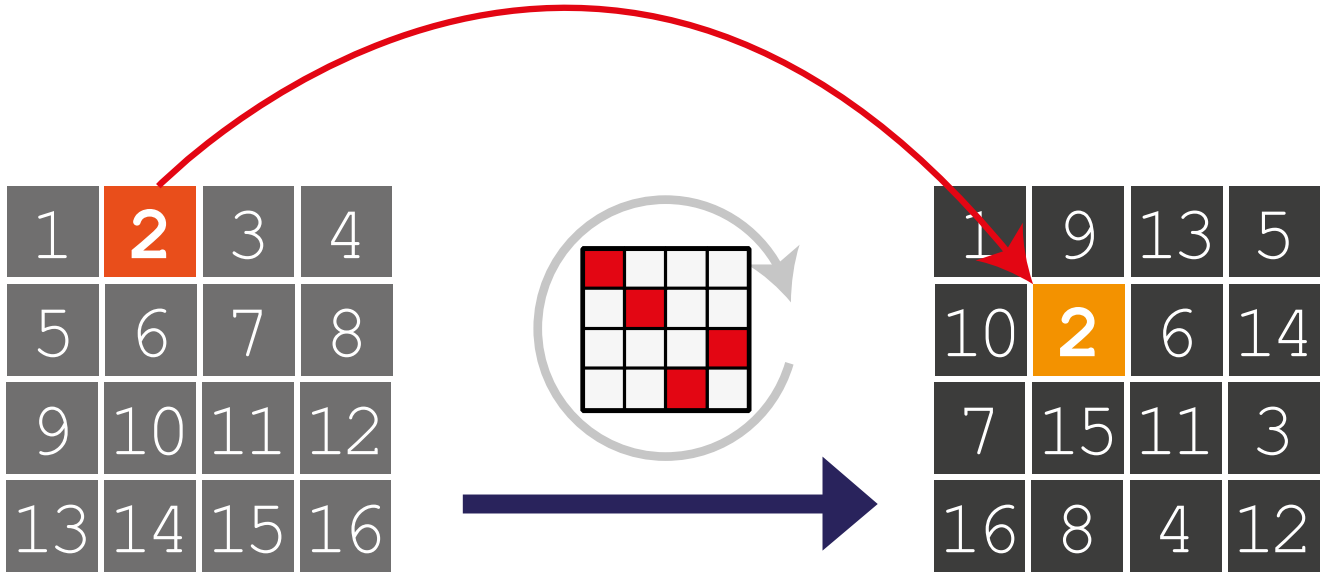


$$\begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

L’elemento che occupa la posizione **1** resta nella posizione **1**.

Percorso di Crittografia svolto al Liceo Majorana di Roma

GRIGLIE DI ROTAZIONE

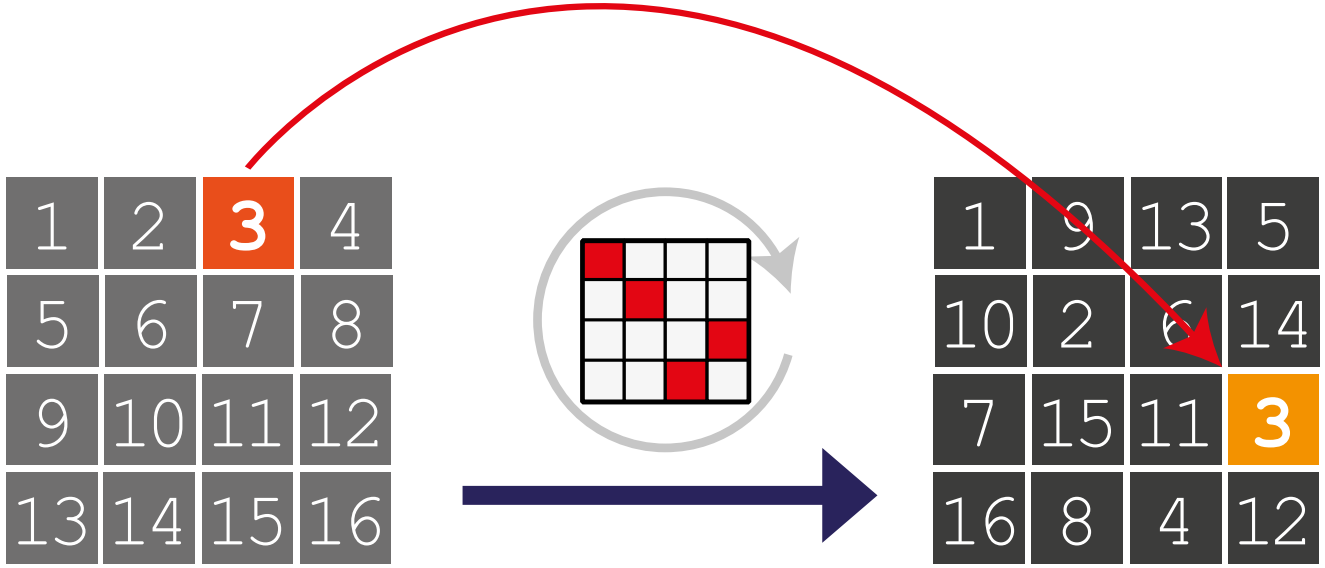


$$\begin{bmatrix} 1 & 2 \\ 1 & 6 \end{bmatrix}$$

L'elemento che prima occupa la posizione **2** poi finisce nella posizione **6**.

Percorso di Crittografia svolto al Liceo Majorana di Roma

GRIGLIE DI ROTAZIONE

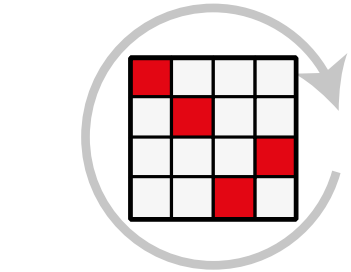


$$\begin{bmatrix} 1 & 2 & 3 \\ 1 & 6 & 12 \end{bmatrix}$$

L'elemento che prima occupa la posizione **3** poi finisce nella posizione **12**.

GRIGLIE DI ROTAZIONE

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16



1	9	13	5
10	2	6	14
7	15	11	3
16	8	4	12

… e così via …

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 1 & 6 & 12 & 15 & 4 & 7 & 9 & 14 & 2 & 5 & 11 & 16 & 3 & 8 & 10 & 13 \end{bmatrix}$$

GRIGLIE DI ROTAZIONE

TABELLA DI PERMUTAZIONE

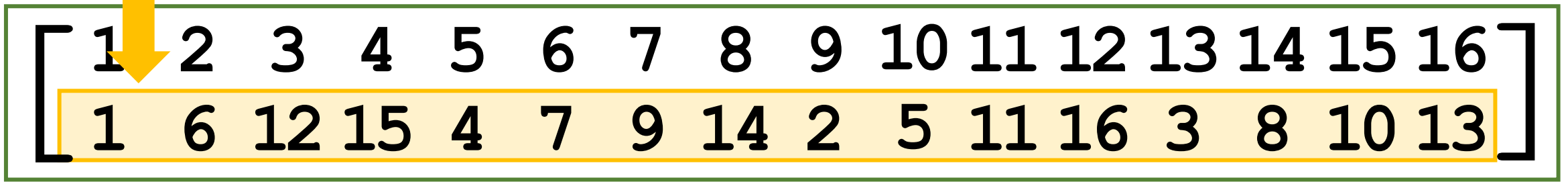
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	6	12	15	4	7	9	14	2	5	11	16	3	8	10	13

GRIGLIE DI ROTAZIONE

Successione numerica che definisce in modo completo la permutazione

TRACCIA DI PERMUTAZIONE

TABELLA DI PERMUTAZIONE

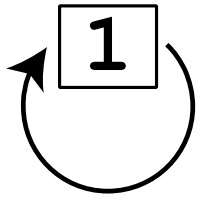


GRIGLIE DI ROTAZIONE

Seguiamo gli spostamenti dei vari elementi

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	6	12	15	4	7	9	14	2	5	11	16	3	8	10	13

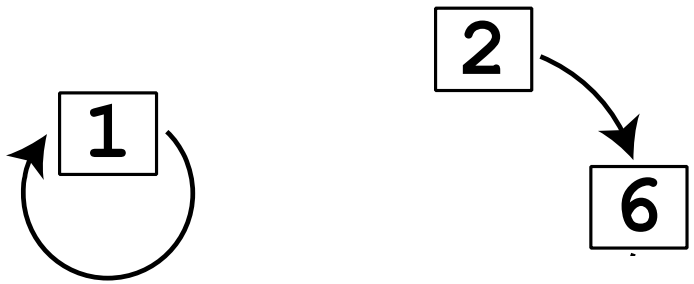
GRIGLIE DI ROTAZIONE



Seguiamo gli spostamenti dei vari elementi

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	6	12	15	4	7	9	14	2	5	11	16	3	8	10	13

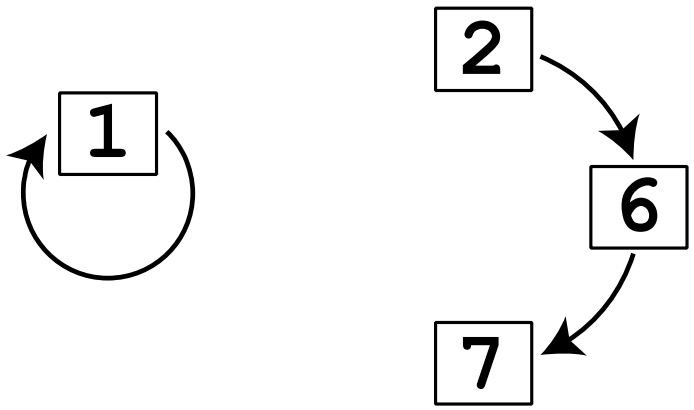
GRIGLIE DI ROTAZIONE



Seguiamo gli spostamenti dei vari elementi

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	6	12	15	4	7	9	14	2	5	11	16	3	8	10	13

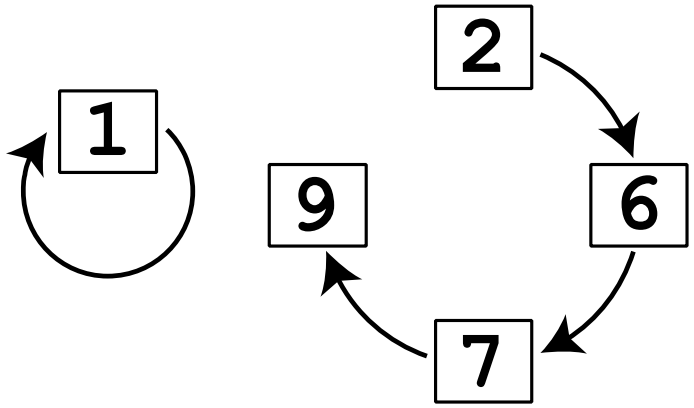
GRIGLIE DI ROTAZIONE



Seguiamo gli spostamenti dei vari elementi

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	6	12	15	4	7	9	14	2	5	11	16	3	8	10	13

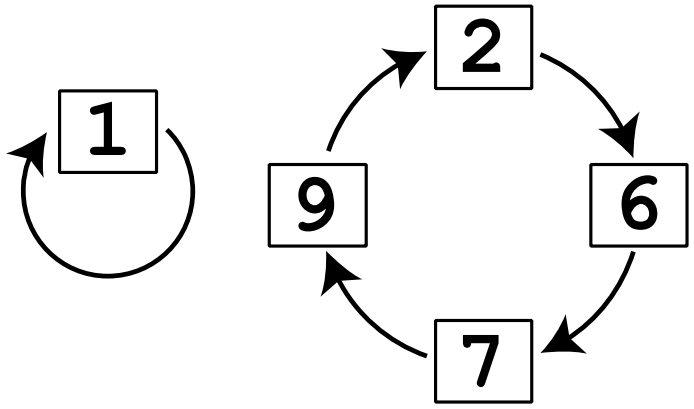
GRIGLIE DI ROTAZIONE



Seguiamo gli spostamenti dei vari elementi

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	6	12	15	4	7	9	14	2	5	11	16	3	8	10	13

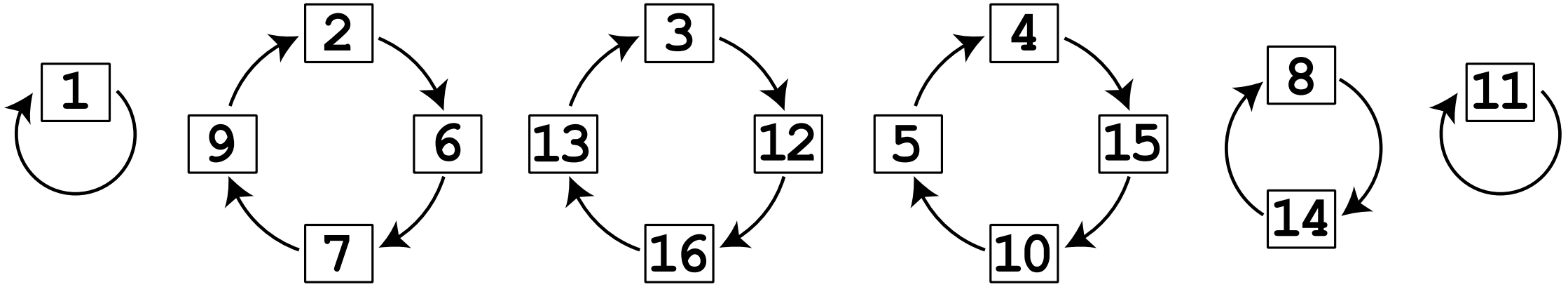
GRIGLIE DI ROTAZIONE



Seguiamo gli spostamenti dei vari elementi

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	6	12	15	4	7	9	14	2	5	11	16	3	8	10	13

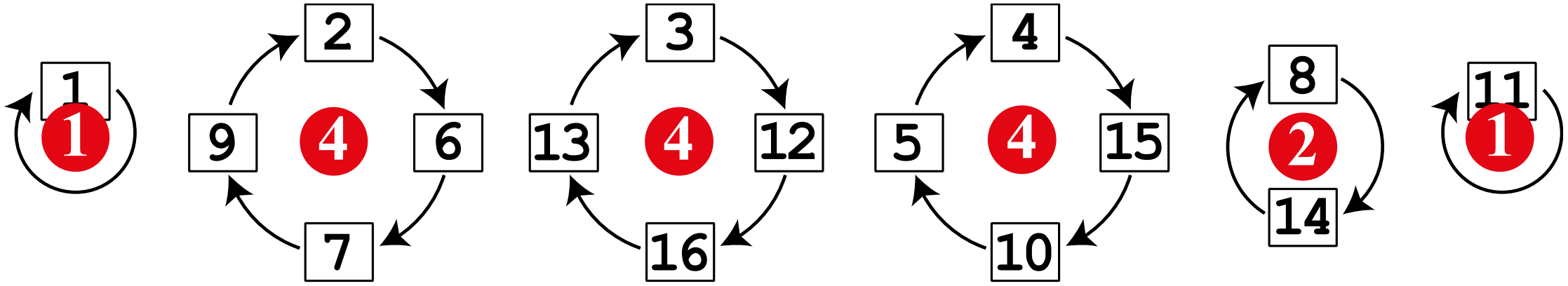
GRIGLIE DI ROTAZIONE



… e così via …

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	6	12	15	4	7	9	14	2	5	11	16	3	8	10	13

GRIGLIE DI ROTAZIONE

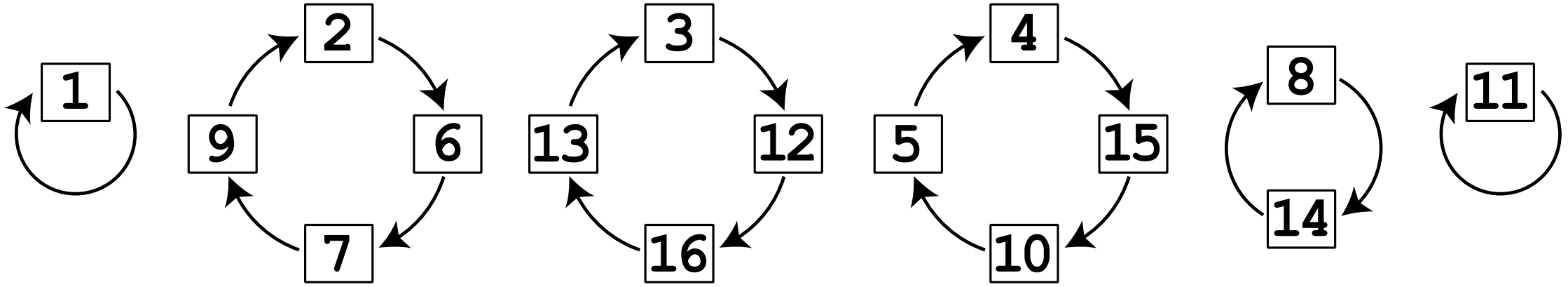


periodi delle singole orbite

periodo complessivo

mcm(1,4,4,4,2,1)=4

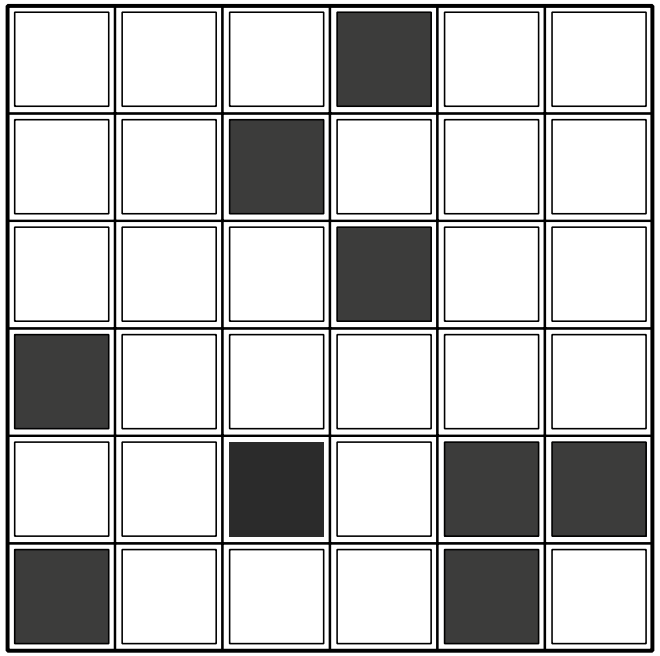
GRIGLIE DI ROTAZIONE



(1) (2,6,7,9) (3,12,16,13) (4,15,10,5) (8,14) (11)

RAPPRESENTAZIONE PER CICLI DISGIUNTI

GRIGLIA 6x6

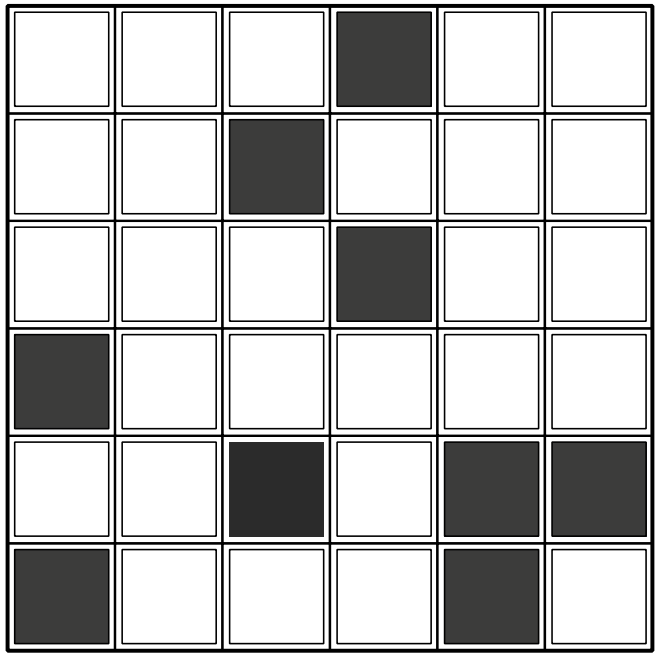


Definisce una trasformazione ***T***
(indipendente dal messaggio)

Mettiamo in pratica quanto visto finora…

Percorso di Crittografia svolto al Liceo Majorana di Roma

GRIGLIA 6x6



Definisce una trasformazione ***T***
(indipendente dal messaggio)

Tabella di permutazione della trasformazione ***T***

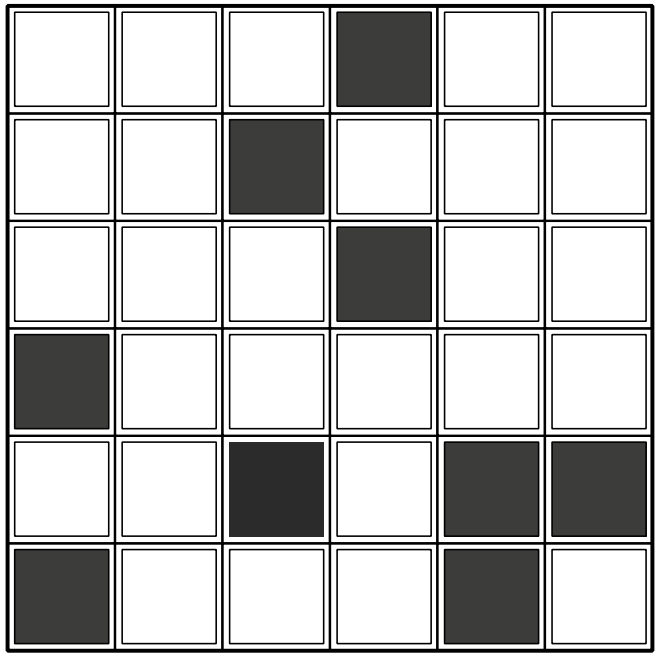
$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & \cdots & 28 & 29 & 30 & 31 & 32 & 33 & 34 & 35 & 36 \\ 4 & 9 & 16 & 19 & 27 & 29 & 31 & 35 & 1 & \cdots & 5 & 11 & 12 & 13 & 15 & 20 & 23 & 34 & 36 \end{bmatrix}$$

Rappresentazione per cicli disgiunti di ***T***

$$(1 \;\; 4 \;\; 19 \;\; 2 \;\; 9 \;\; 35 \;\; 34 \;\; 23 \;\; 10)$$
$$(3 \;\; 16 \;\; 25 \;\; 21 \;\; \ldots \;\; \ldots \;\; 20 \;\; 6 \;\; 29 \;\; 11)$$
$$(15 \;\; 24 \;\; 18 \;\; 32)$$
$$(36)$$

Percorso di Crittografia svolto al Liceo Majorana di Roma

GRIGLIA 6x6



Definisce una trasformazione ***T***
(indipendente dal messaggio)

Tabella di permutazione della trasformazione ***T***

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & \dots & 28 & 29 & 30 & 31 & 32 & 33 & 34 & 35 & 36 \\ 4 & 9 & 16 & 19 & 27 & 29 & 31 & 35 & 1 & \dots & 5 & 11 & 12 & 13 & 15 & 20 & 23 & 34 & 36 \end{bmatrix}$$

Rappresentazione per cicli disgiunti di ***T***

$(1\ \ 4\ \ 19\ \ 2\ \ 9\ \ 35\ \ 34\ \ 23\ \ 10)$ → **9** elementi

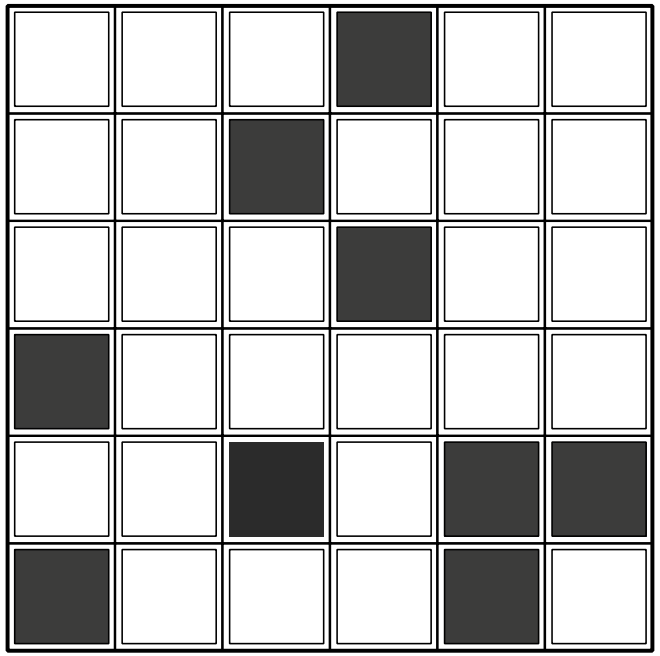
$(3\ \ 16\ \ 25\ \ 21\ \ \dots\ \ \dots\ \ 20\ \ 6\ \ 29\ \ 11)$ → **22** elementi

$(15\ \ 24\ \ 18\ \ 32)$ → **4** elementi

(36) → **1** elementi

T ha un **periodo** pari a mcd(9,22,4,1) = **396**

GRIGLIA 6x6



Definisce una trasformazione ***T***
(indipendente dal messaggio)

Tabella di permutazione della trasformazione ***T***

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & \cdots & 28 & 29 & 30 & 31 & 32 & 33 & 34 & 35 & 36 \\ 4 & 9 & 16 & 19 & 27 & 29 & 31 & 35 & 1 & \cdots & 5 & 11 & 12 & 13 & 15 & 20 & 23 & 34 & 36 \end{bmatrix}$$

Rappresentazione per cicli disgiunti di ***T***

$(1\ 4\ 19\ 2\ 9\ 35\ 34\ 23\ 10)$ → **9** elementi

$(3\ 16\ 25\ 21\ \ldots\ \ldots\ 20\ 6\ 29\ 11)$ → **22** elementi

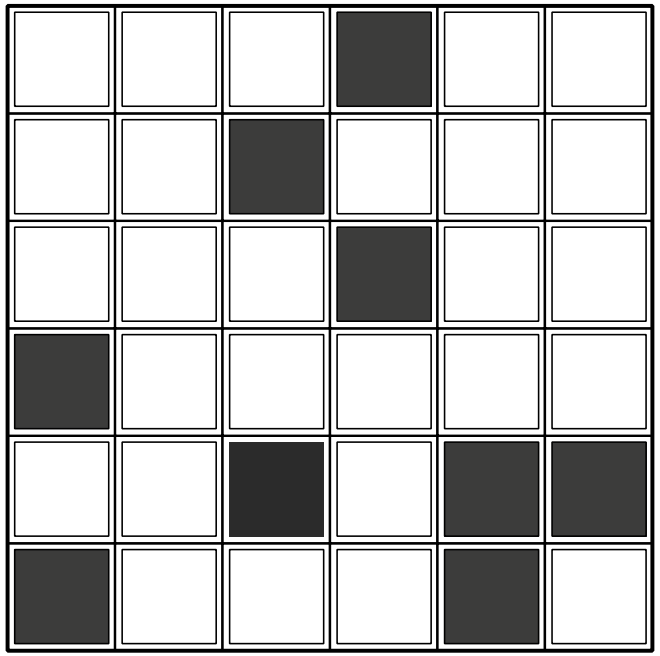
$(15\ 24\ 18\ 32)$ → **4** elementi

(36) → **1** elementi

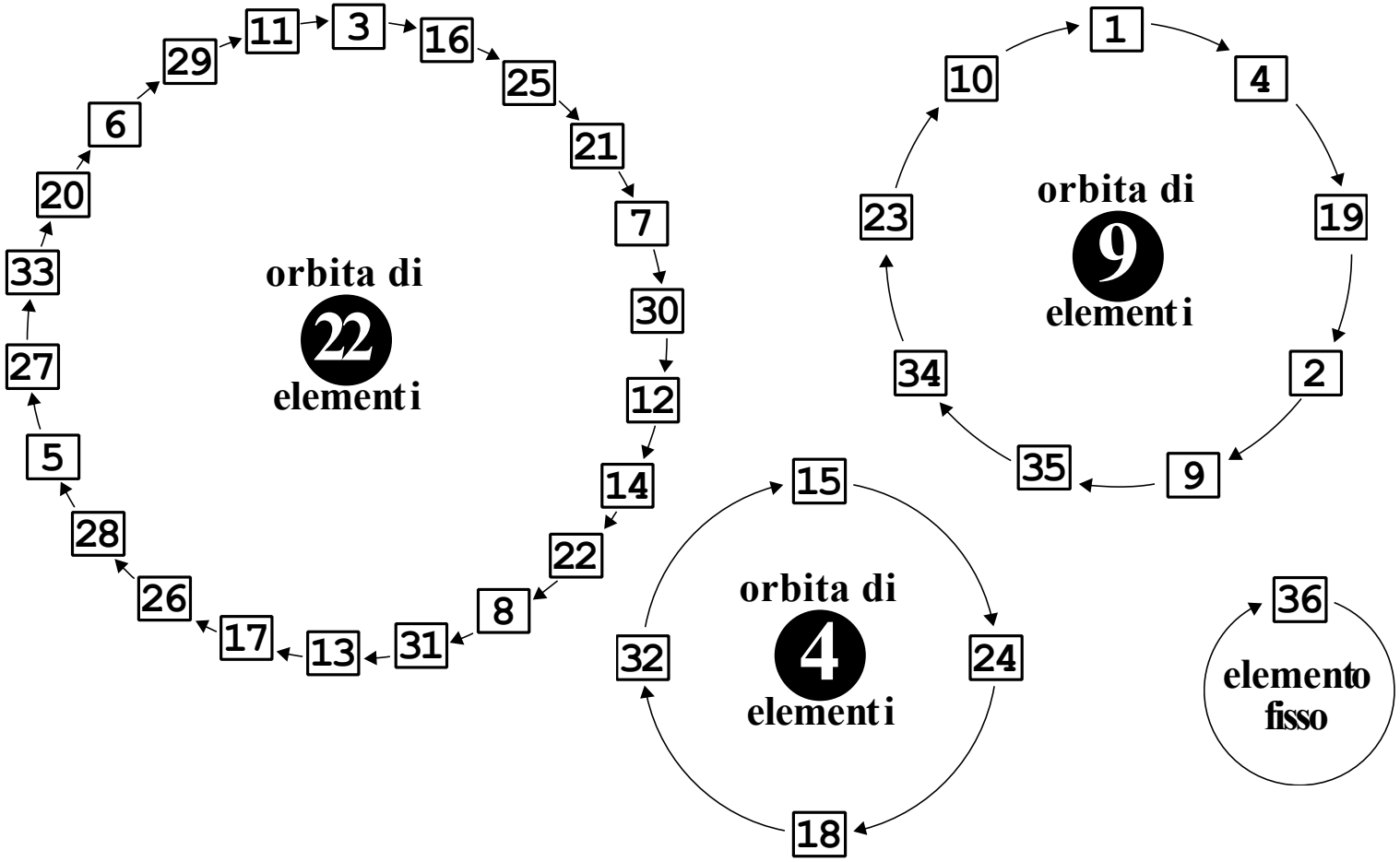
T ha un **periodo** pari a mcd(9,22,4,1) = **396**

Trova la traccia di permutazione della trasformazione .

GRIGLIA 6x6

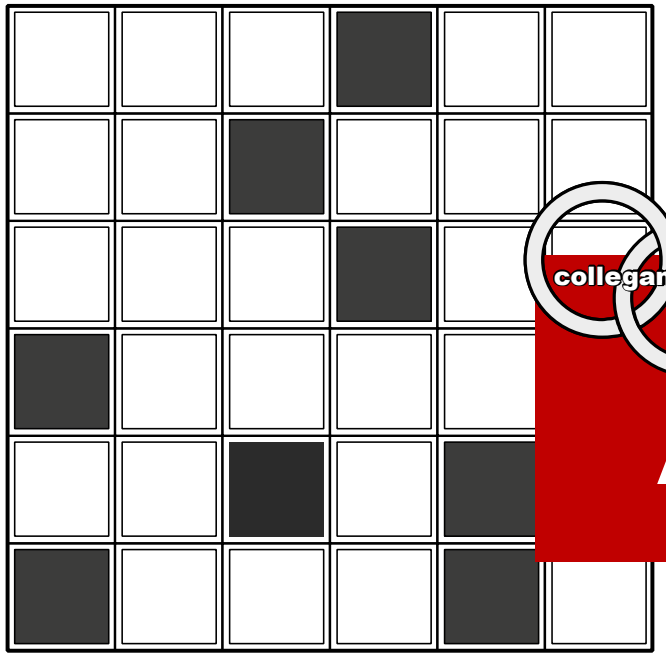


Definisce una trasformazione ***T***
(indipendente dal messaggio)

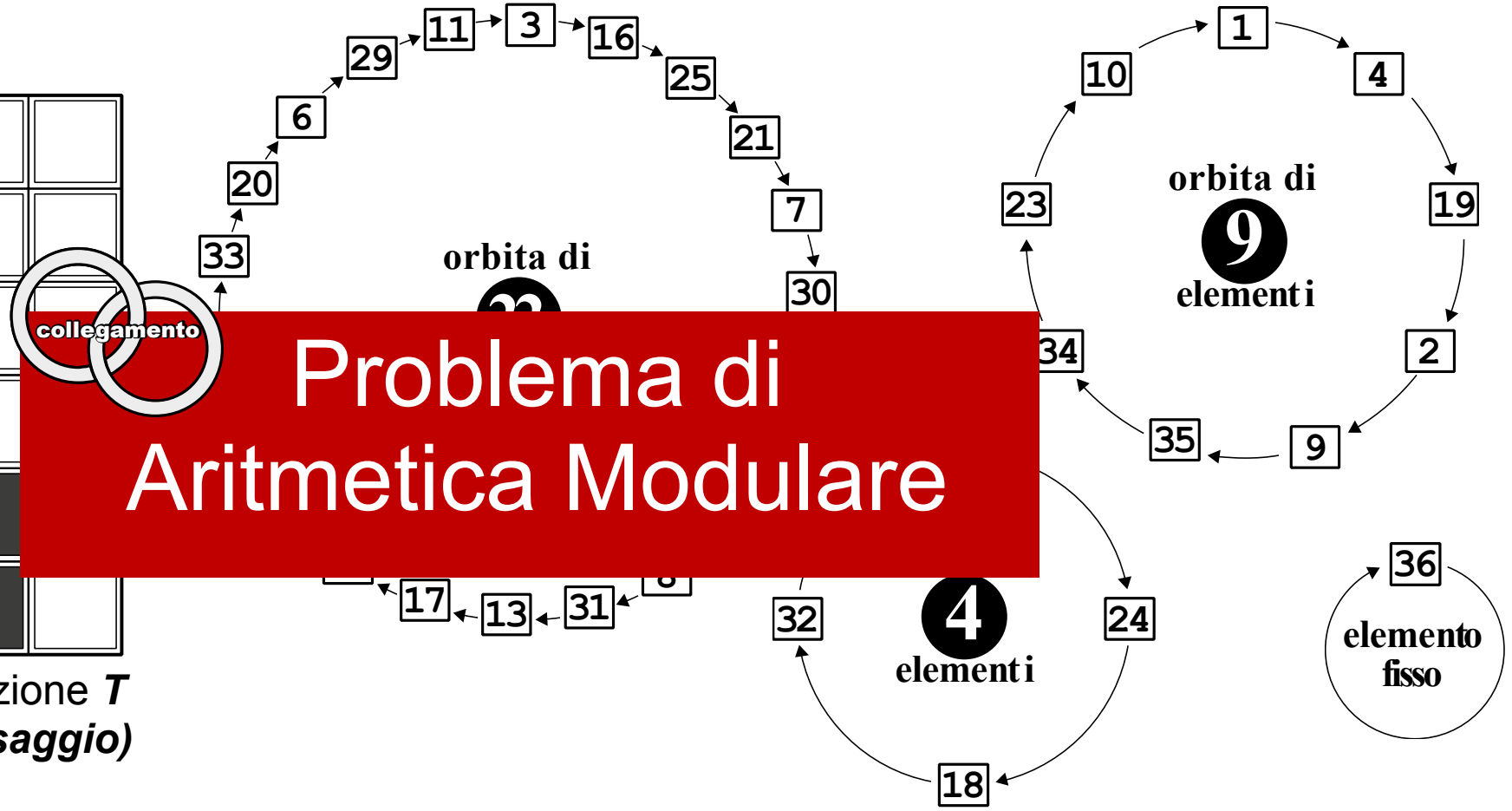


Trova la traccia di permutazione della trasformazione

GRIGLIA 6x6



Definisce una trasformazione ***T***
(indipendente dal messaggio)

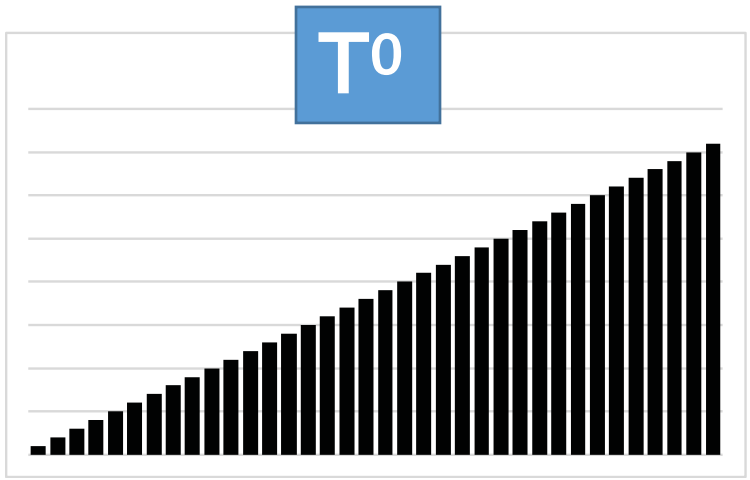


collegamento

Problema di Aritmetica Modulare

Trova la traccia di permutazione della trasformazione

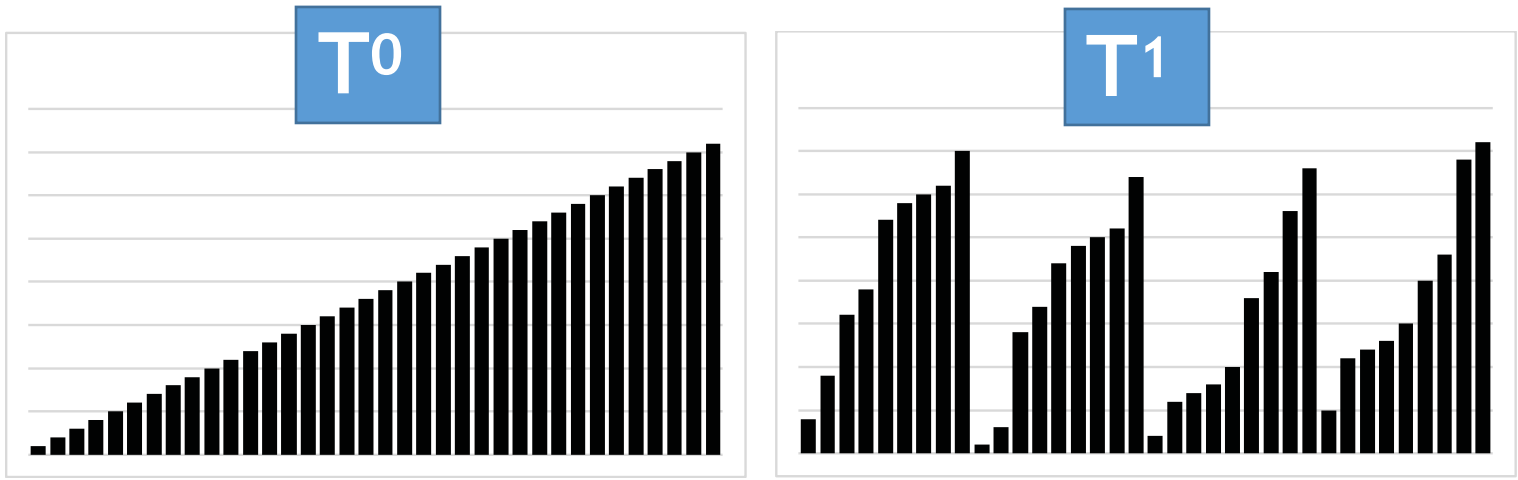
Rappresentazione grafica delle diverse **tracce di permutazione**



Ancora sulle rappresentazioni delle trasposizioni

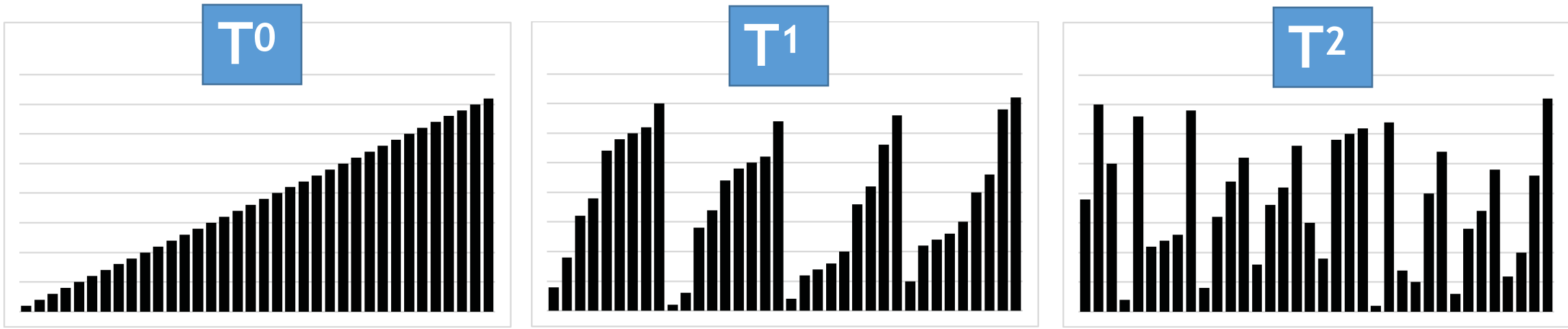
Percorso di Crittografia svolto al Liceo Majorana di Roma

Rappresentazione grafica delle diverse **tracce di permutazione**



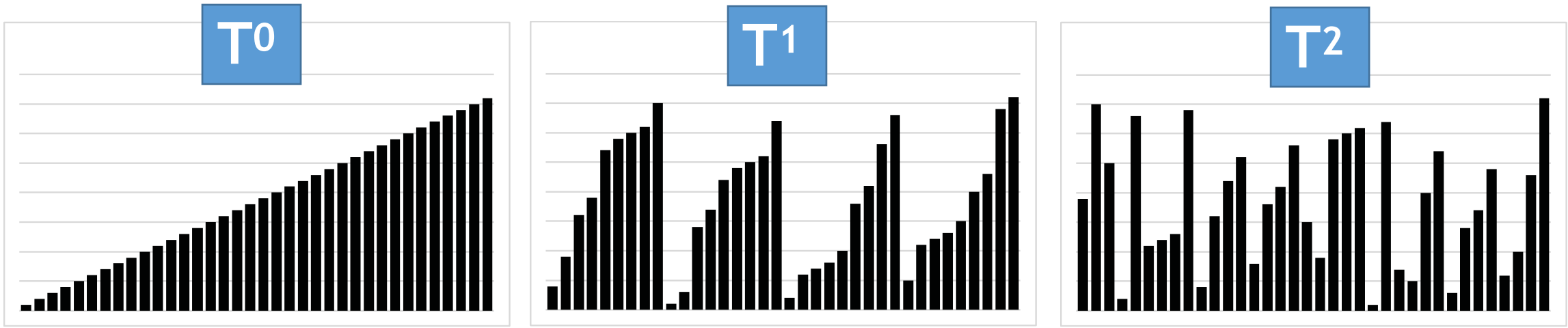
Percorso di Crittografia svolto al Liceo Majorana di Roma

Rappresentazione grafica delle diverse **tracce di permutazione**



Percorso di Crittografia svolto al Liceo Majorana di Roma

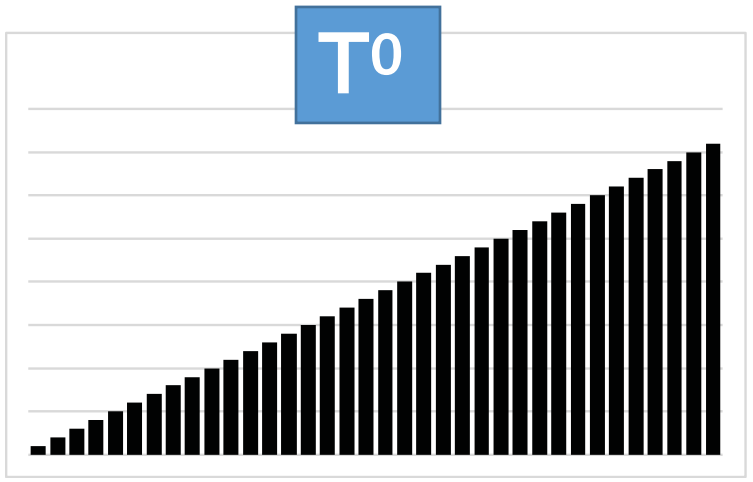
Rappresentazione grafica delle diverse **tracce di permutazione**

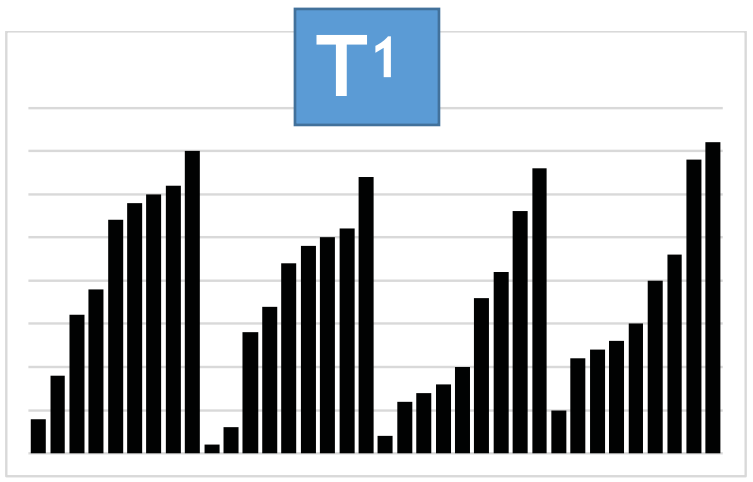


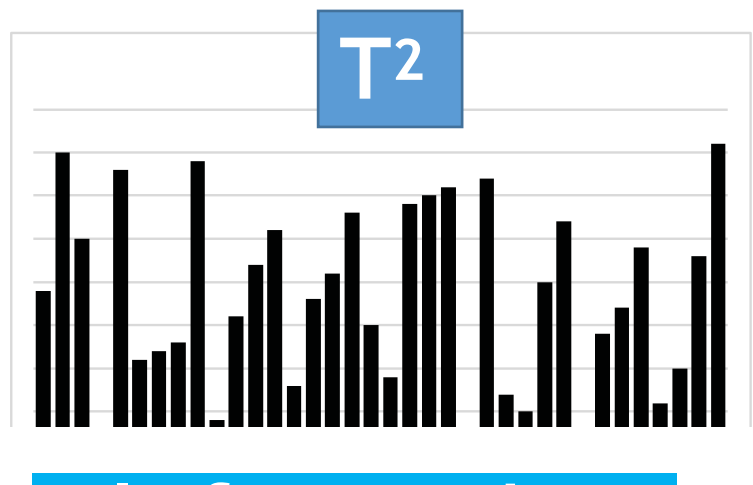
L’iterazione pare funzionare, rendendo la permutazione **apparentemente** più irregolare. **Come si può quantificare il disordine**?

Percorso di Crittografia svolto al Liceo Majorana di Roma

Rappresentazione grafica delle diverse **tracce di permutazione**







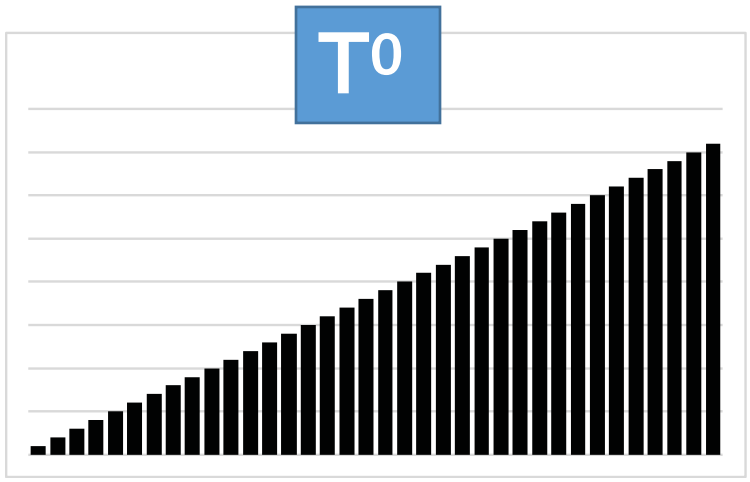
L'iterazione pare funzionare, rendendo la permutazio
irregolare. **Come si può quantificare il disordi**

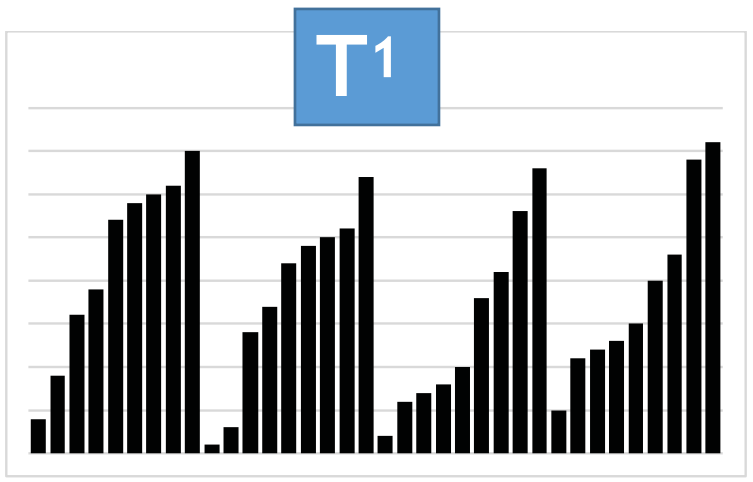
Possibile soluzione

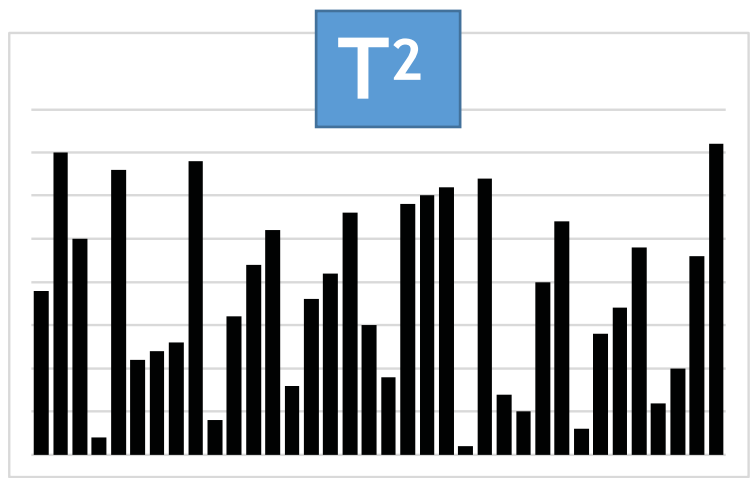
Fissato un **algoritmo di ordinamento**, misuriamo il disordine con il **numero di operazioni necessarie** a rimettere la sequenza in ordine.

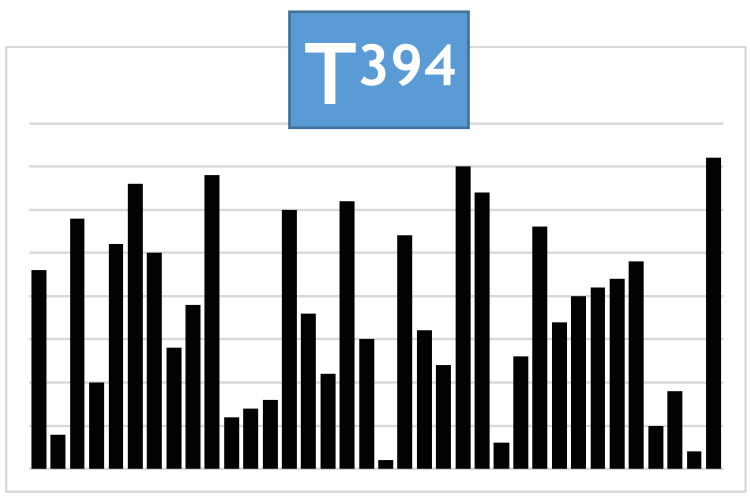
Percorso di Crittografia svolto al Liceo Majorana di Roma

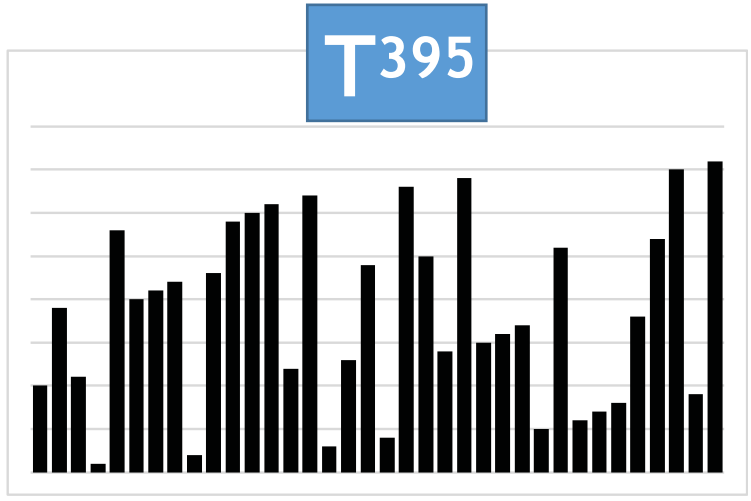
Rappresentazione grafica delle diverse **tracce di permutazione**

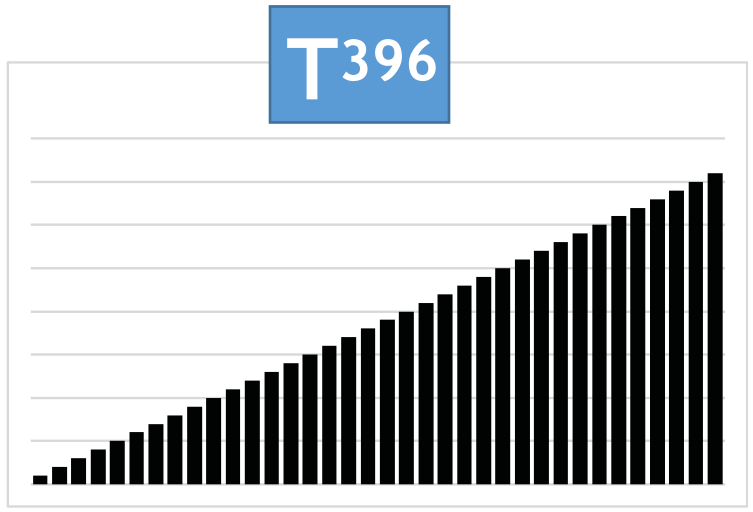






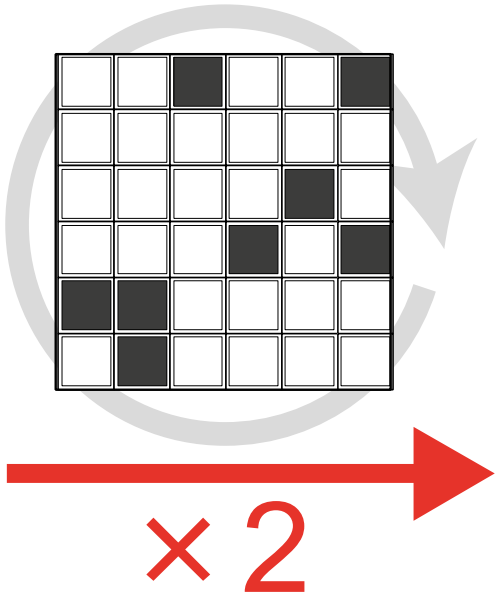






Percorso di Crittografia svolto al Liceo Majorana di Roma

La tecnica di **sostituzione**

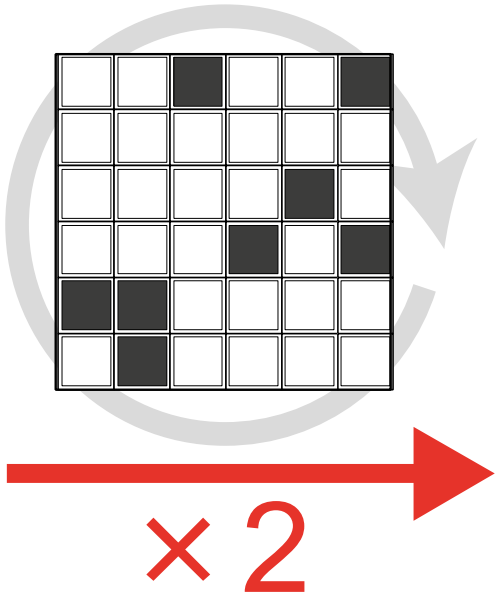


Vediamo un altro modo di usare la trasposizione per cifrare un messaggio

Percorso di Crittografia svolto al Liceo Majorana di Roma

La tecnica di **sostituzione**

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	Ø	1	2	3
4	5	6	7	8	9

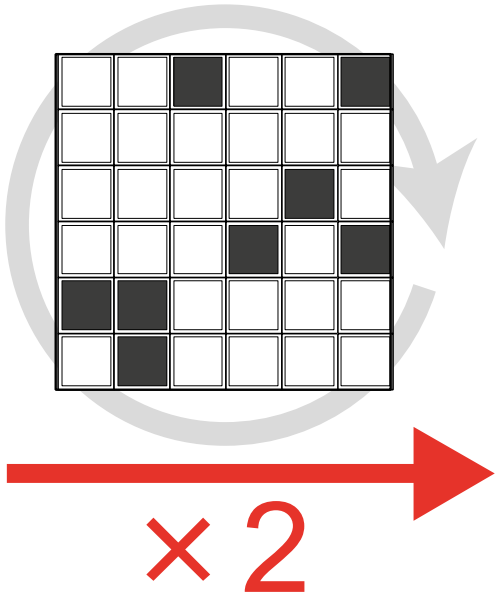


Vediamo un altro modo di usare la trasposizione per cifrare un messaggio

Percorso di Crittografia svolto al Liceo Majorana di Roma

La tecnica di **sostituzione**

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	Ø	1	2	3
4	5	6	7	8	9



Alfabeto cifrante

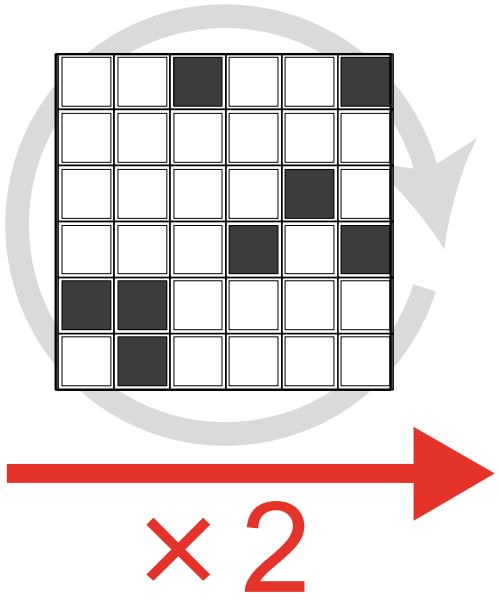
W	D	2	J	Z	6
Y	N	S	7	F	G
H	3	R	K	4	O
A	Ø	P	L	8	5
C	M	1	Q	T	U
V	X	E	I	B	9

Vediamo un altro modo di usare la trasposizione per cifrare un messaggio

Percorso di Crittografia svolto al Liceo Majorana di Roma

La tecnica di **sostituzione**

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	Ø	1	2	3
4	5	6	7	8	9



Alfabeto cifrante

W	D	2	J	Z	6
Y	N	S	7	F	G
H	3	R	K	4	O
A	Ø	P	L	8	5
C	M	1	Q	T	U
V	X	E	I	B	9

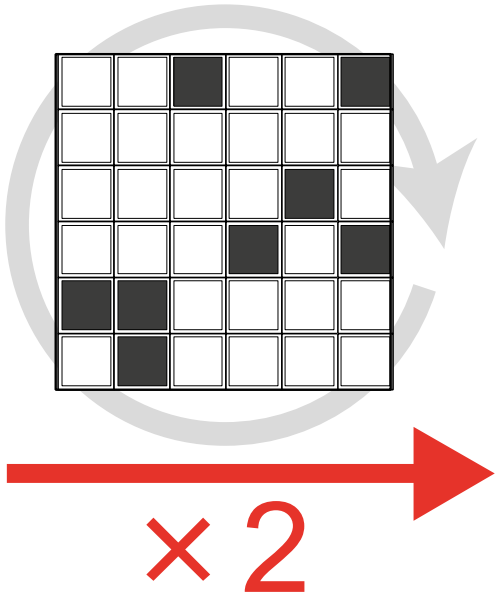
MESSAGGIO IN CHIARO

F	I	S	C	I	A	N	O	2	Ø	1	9

Percorso di Crittografia svolto al Liceo Majorana di Roma

La tecnica di **sostituzione**

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	Ø	1	2	3
4	5	6	7	8	9



Alfabeto cifrante

W	D	2	J	Z	6
Y	N	S	7	F	G
H	3	R	K	4	O
A	Ø	P	L	8	5
C	M	1	Q	T	U
V	X	E	I	B	9

MESSAGGIO IN CHIARO	F	I	S	C	I	A	N	O	2	Ø	1	9
MESSAGGIO CRITTATO	6	S	A	2	S	W	3	R	T	1	Q	9

Percorso di Crittografia svolto al Liceo Majorana di Roma

La tecnica di **sostituzione**

Alfabeto cifrante

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	Ø	1	2	3
4	5	6	7	8	9

TECNICA DI SOSTITUZIONE

×2

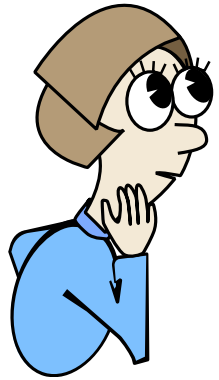
W	D	2	J	Z	6
Y	N	S	7	F	G
M	N	O	K	4	O
A	Ø	P	L	8	5
C	M	1	Q	T	U
V	X	E	I	B	9

MESSAGGIO IN CHIARO	F	I	S	C	I	A	N	O	2	Ø	1	9
MESSAGGIO CRITTATO	6	S	A	2	S	W	3	R	T	1	Q	9

Punto debole delle tecniche viste finora

È NECESSARIO LO SCAMBIO DELLA CHIAVE DI CODIFICA / DECODIFICA (per esempio la posizione dei fori della griglia)

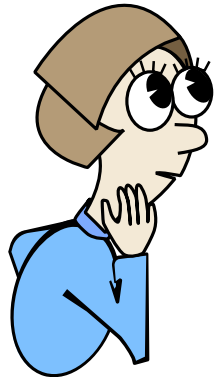
PROTOCOLLO DEL DOPPIO LUCCHETTO



ALICE

Alice e Bruno vogliono comunicare segretamente

BRUNO

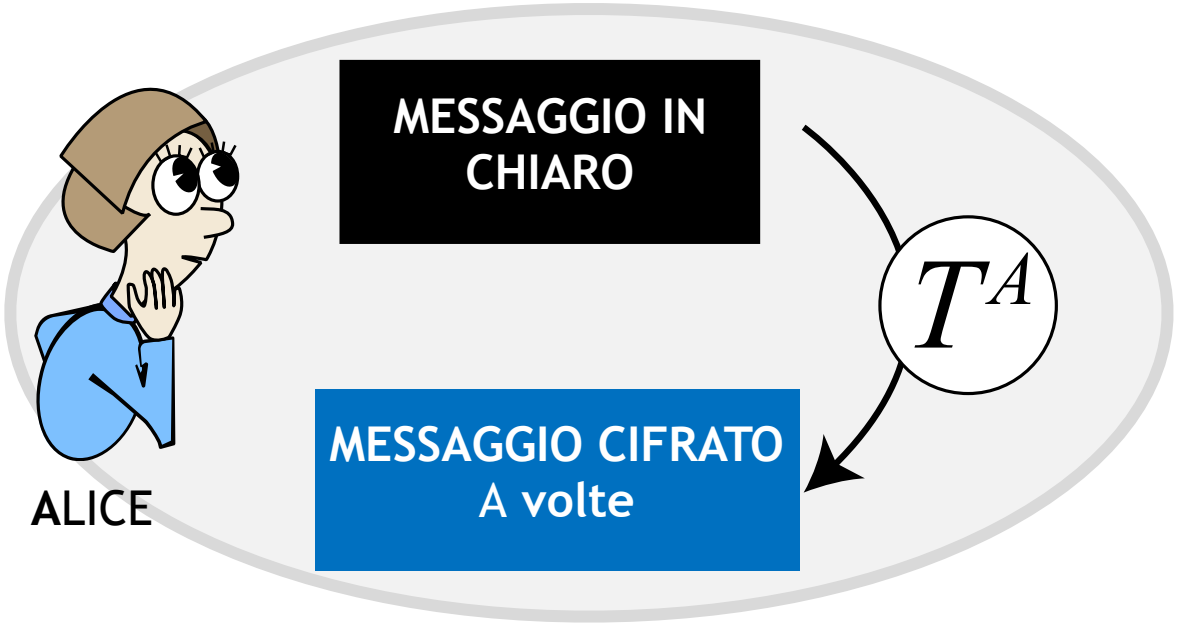


ALICE

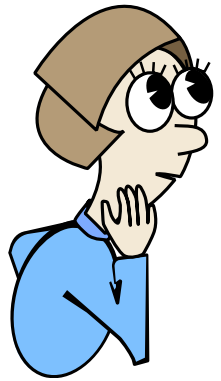
Alice e Bruno vogliono comunicare segretamente

BRUNO

Alice e Bruno concordano «pubblicamente» la trasposizione *T* che useranno.



Alice cifra il messaggio ***A*** volte. Il numero ***A*** è noto soltanto ad Alice.



ALICE

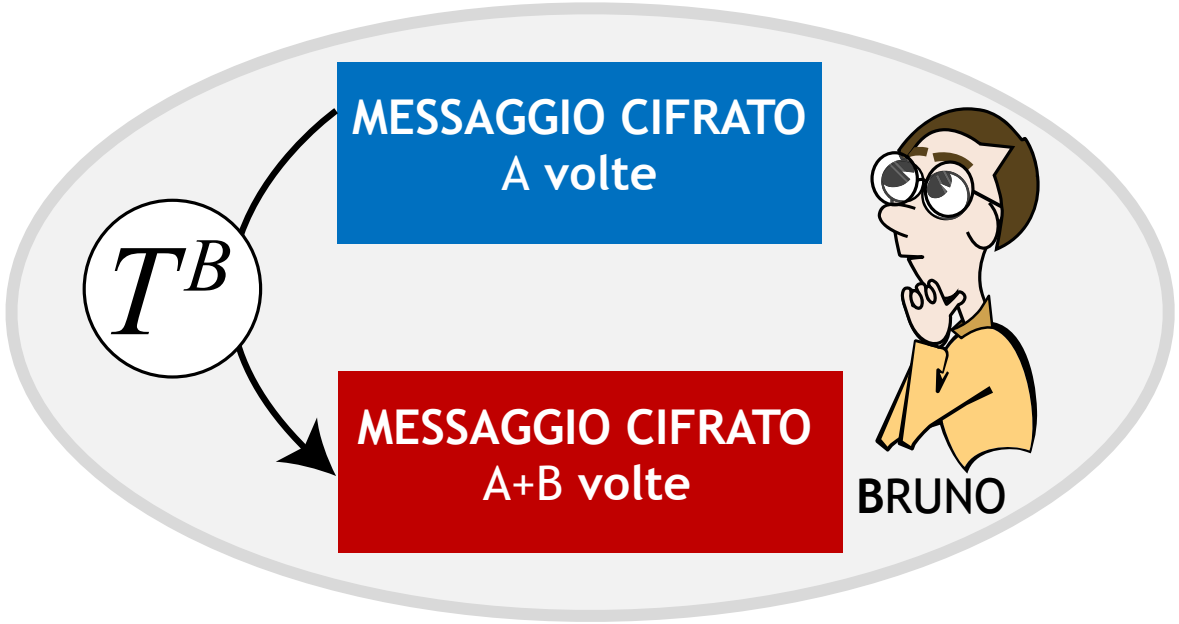
MESSAGGIO CIFRATO
A volte

T^A

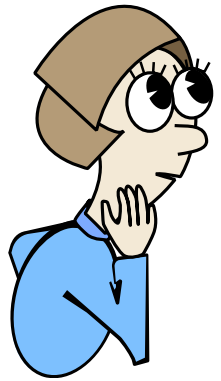
BRUNO

Alice invia il messaggio cifrato a Bruno.

ALICE



Bruno riceve un messaggio (a lui incomprensibile) e lo cifra a sua volta ***B*** volte (B è noto solo a lui)



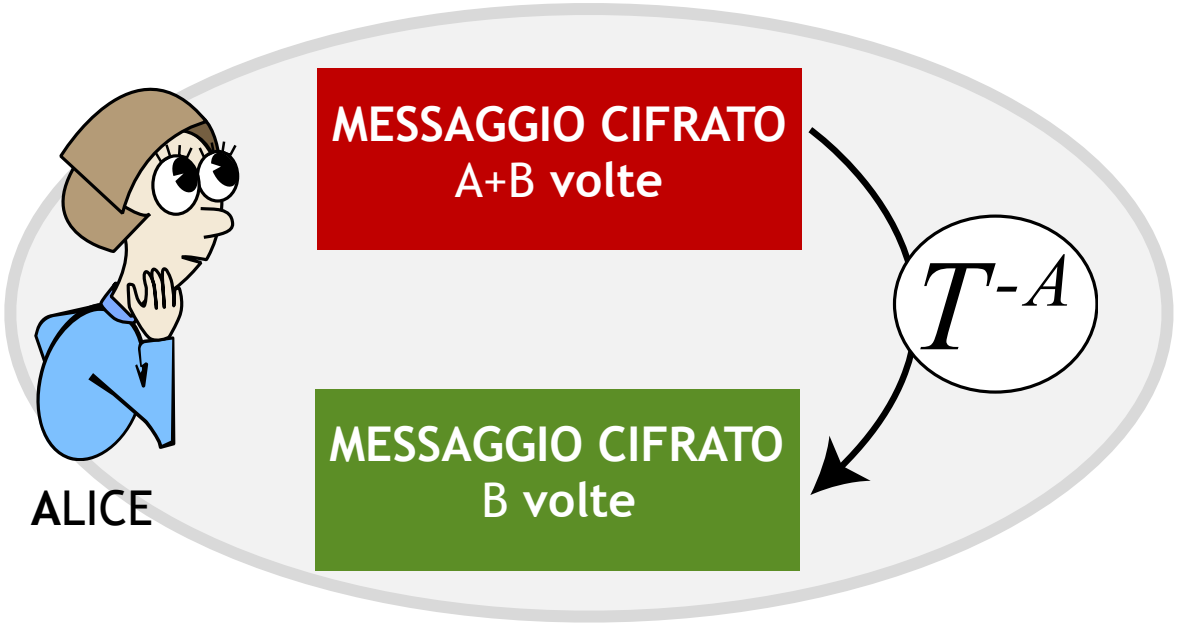
ALICE

MESSAGGIO CIFRATO
A+B volte

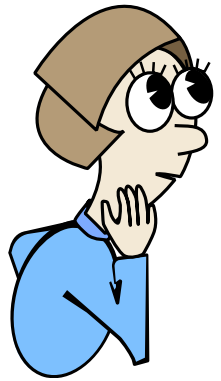
T^{A+B}

BRUNO

Bruno invia il messaggio (sovra)cifrato ad Alice.



Alice applica ***A*** volte la trasposizione T^{-1}: quello che resta è il messaggio originario cifrato ***B*** volte.



ALICE

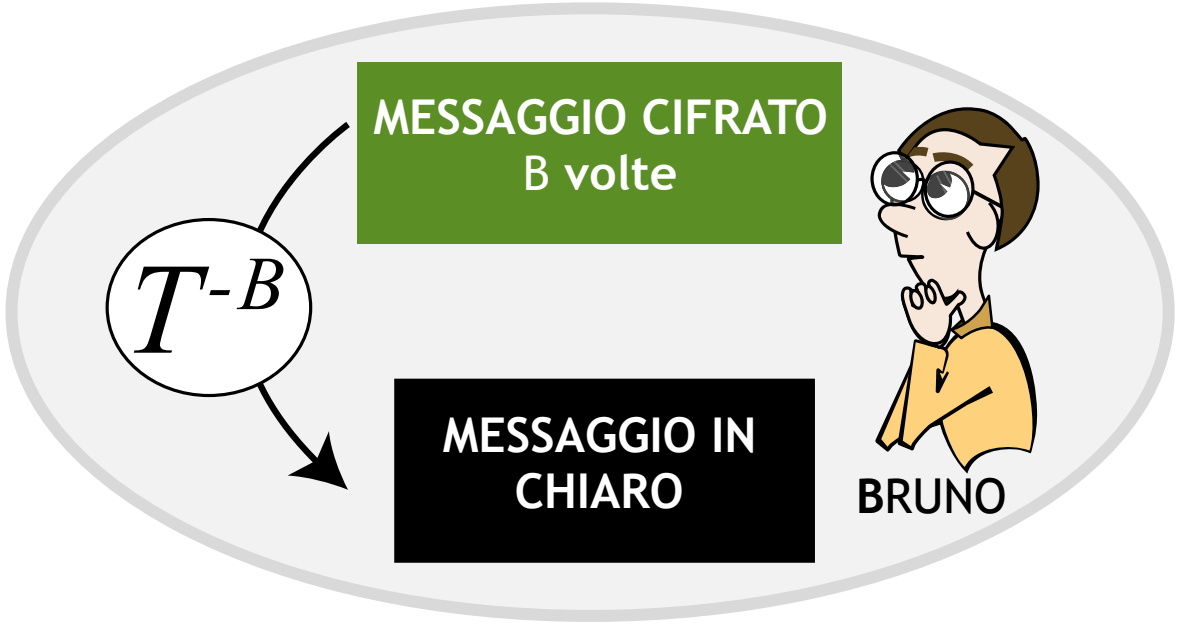
MESSAGGIO CIFRATO
B volte

T^B

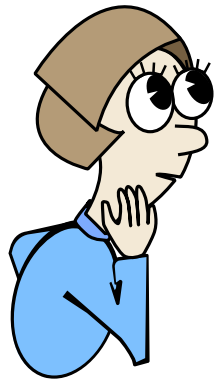
BRUNO

Alice invia il messaggio cifrato a Bruno.

ALICE



Bruno riceve il testo e applica ***B*** volte la trasposizione T^{-1}. Ciò porta il messaggio in chiaro.



ALICE

COMUNICAZIONE AVVENUTA

BRUNO

Riassunto delle ***comunicazioni intercettate***

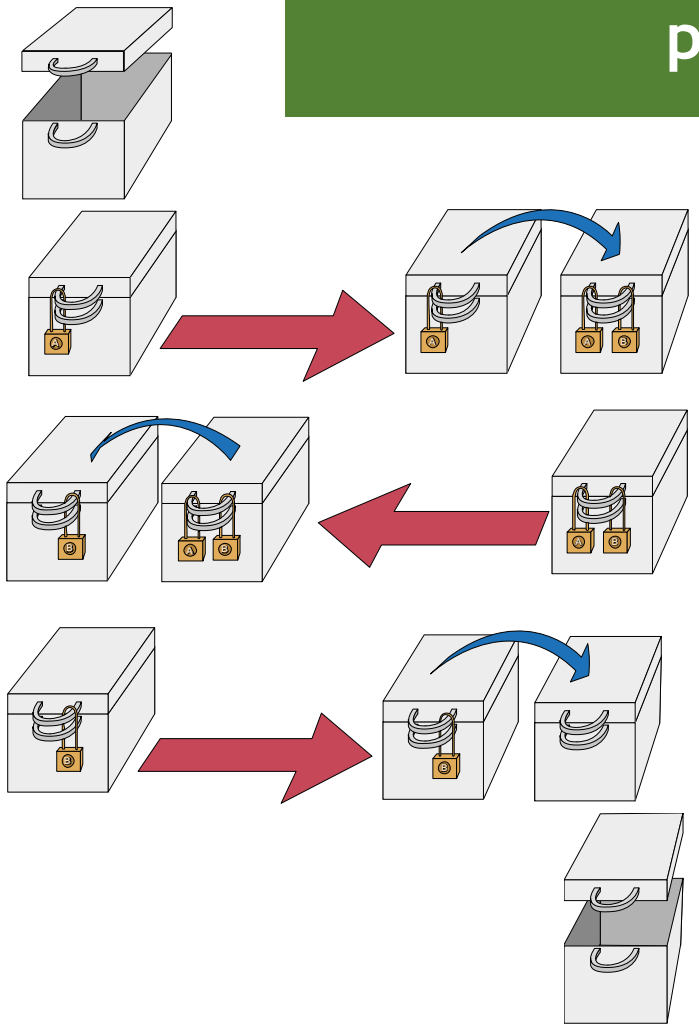
Trasformazione *T*

Messaggio cifrato A volte (mediante *T*)

Messaggio cifrato A+B volte (mediante

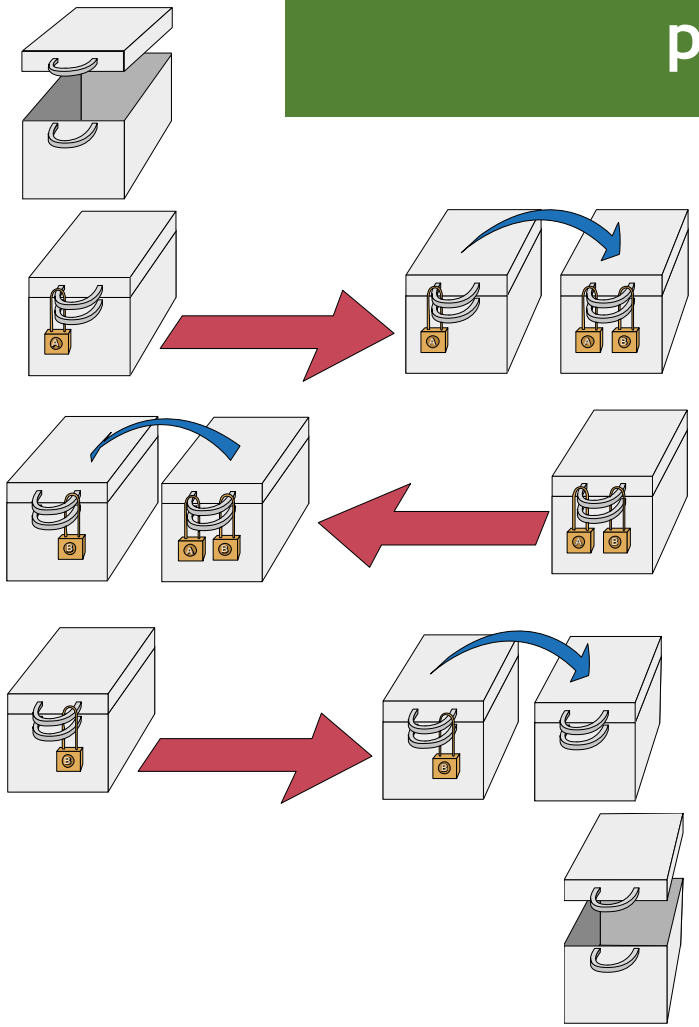
Messaggio cifrato B volte (mediante *T*)

Discussione sul **protocollo del doppio lucchetto.**



In quale dei seguenti casi il protocollo del doppio lucchetto funziona?

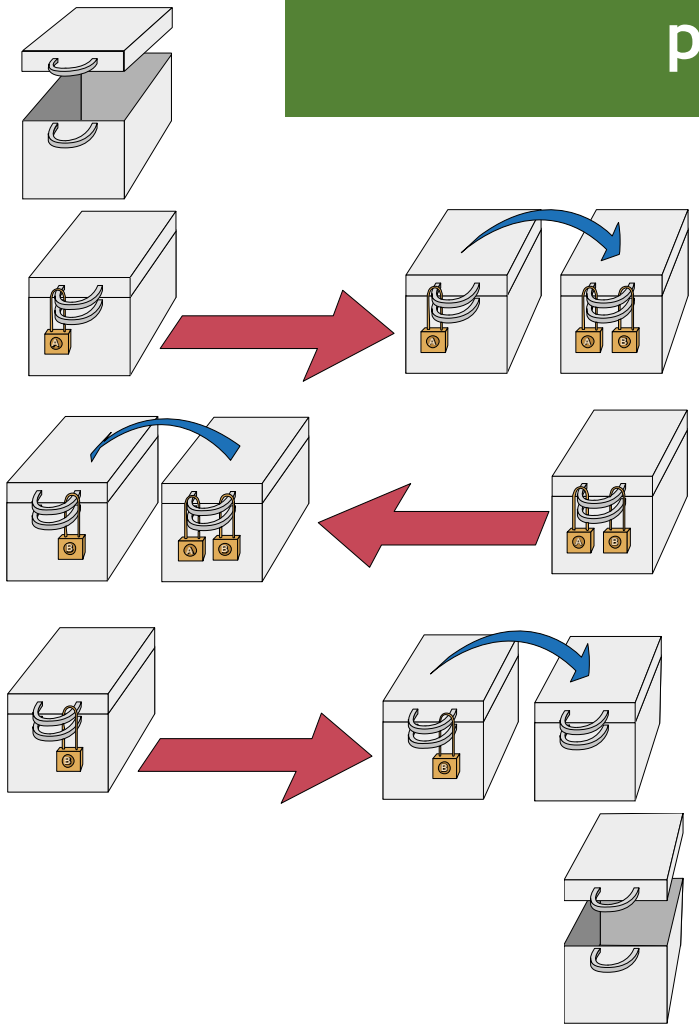
Discussione sul **protocollo del doppio lucchetto.**



In quale dei seguenti casi il protocollo del doppio lucchetto funziona?

A	B	funziona?
trasposizione T iterata Ⓐ volte	trasposizione T iterata Ⓑ volte	✓ sì
trasposizione T	trasposizione Ⓤ	
trasposizione Ⓣ	sostituzione Ⓢ	
sostituzione Ⓡ	sostituzione Ⓢ	

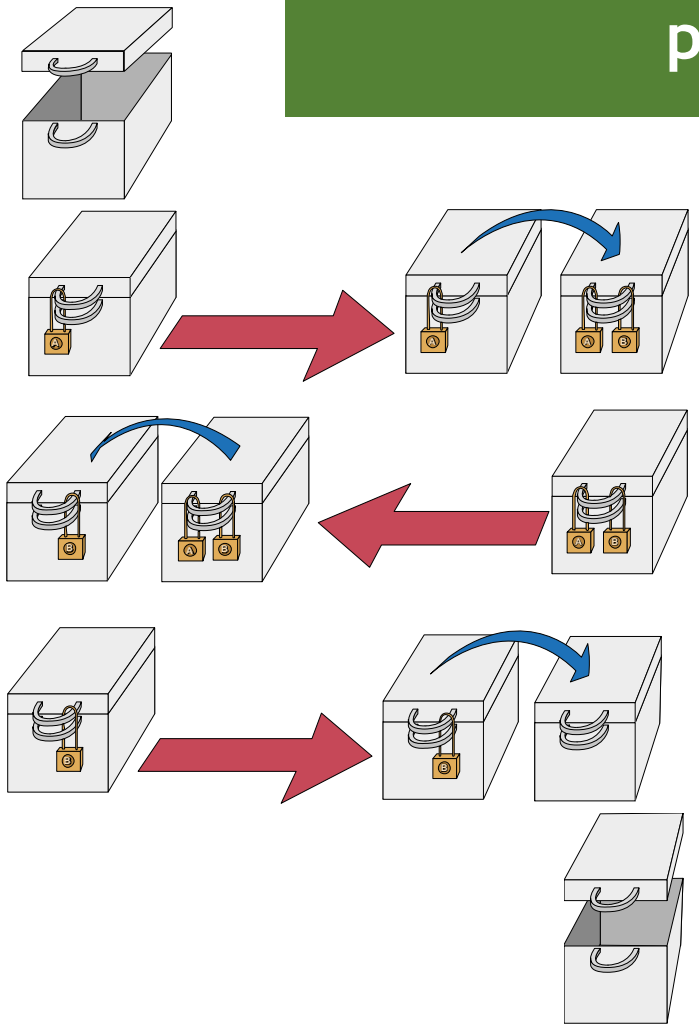
Discussione sul **protocollo del doppio lucchetto.**



In quale dei seguenti casi il protocollo del doppio lucchetto funziona?

A	B	funziona?
trasposizione T iterata Ⓐ volte	trasposizione T iterata Ⓑ volte	✓ sì
trasposizione T	trasposizione Ⓤ	✗ no
trasposizione Ⓣ	sostituzione Ⓢ	
sostituzione Ⓡ	sostituzione Ⓢ	

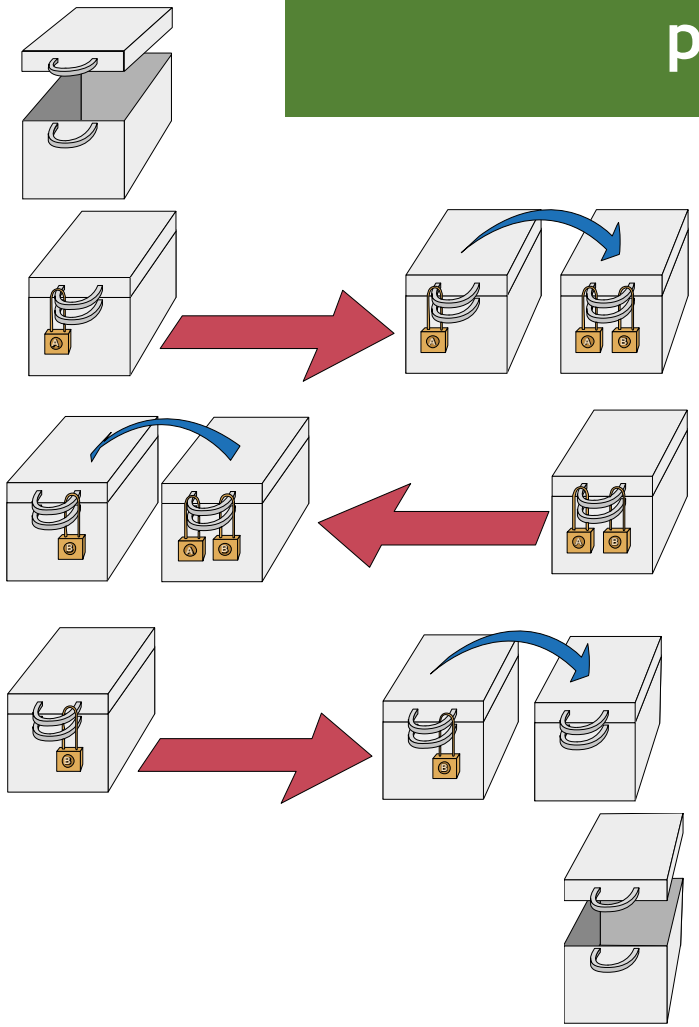
Discussione sul **protocollo del doppio lucchetto.**



In quale dei seguenti casi il protocollo del doppio lucchetto funziona?

A	B	funziona?
trasposizione T iterata Ⓐ volte	trasposizione T iterata Ⓑ volte	✓ sì
trasposizione T	trasposizione Ⓤ	✗ no
trasposizione Ⓣ	sostituzione Ⓢ	✓ sì
sostituzione Ⓡ	sostituzione Ⓢ	

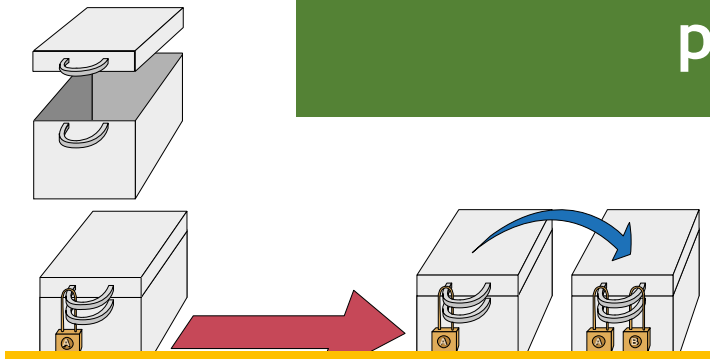
Discussione sul **protocollo del doppio lucchetto.**



In quale dei seguenti casi il protocollo del doppio lucchetto funziona?

A	B	funziona?
trasposizione T iterata Ⓐ volte	trasposizione T iterata Ⓑ volte	✓ sì
trasposizione T	trasposizione Ⓤ	✗ no
trasposizione Ⓣ	sostituzione Ⓢ	✓ sì
sostituzione Ⓡ	sostituzione Ⓢ	✗ no

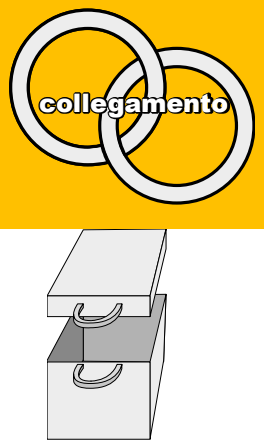
Discussione sul **protocollo del doppio lucchetto.**



Algebra

(composizione di trasformazioni)

$B^{-1} \circ A^{-1} \circ B \circ A$



In quale dei seguenti casi il protocollo del doppio lucchetto funziona?

A	B	funziona?
trasposizione T iterata Ⓐ volte	trasposizione T iterata Ⓑ volte	✓ sì
trasposizione T	trasposizione Ⓤ	✗ no
trasposizione Ⓣ	sostituzione Ⓢ	✓ sì
sostituzione Ⓡ	sostituzione Ⓢ	✗ no

Considerazioni didattiche

- **Alta motivazione** da parte degli studenti
- Grande facilità a trasformare il percorso in **attività laboratoriale**
- Grande varietà di attività (**caccia al tesoro** a scuola, visite a musei, presentazione ai compagni, Kahoot, …)

Collegamenti interdisciplinari

Argomento realmente interdisciplinare, specialmente in **Storia** e **Italiano** (per i «giochi» come i lipogrammi) , ma anche **Storia dell'Arte**, **Informatica, Religione**

Motivazioni «Matematiche»

- Percorso che permette di **applicare competenze già acquisite** (Calcolo Combinatorio, Informatica)
- Argomento «ponte» verso **argomenti difficili da raggiungere** (teoria dei Gruppi, macchina di Turing, sequenze pseudocasuali, …)

Percorso di Crittografia svolto al Liceo Majorana di Roma

Percorso di Crittografia svolto al Liceo Majorana di Roma

Poli

Foto della festa del Liceo Matematico svoltasi nel maggio del 2018

Cerca ...

ARTICOLI RECENTI

Programma del Terzo Seminario Nazionale sui Licei Matematici

Convegno dei Licei Matematici del Lazio

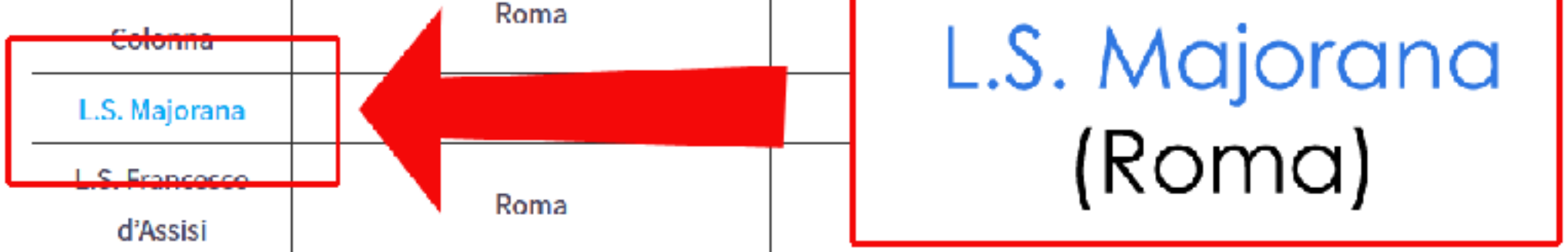
Comunicare la matematica 2

Convegno "Matematica e Filosofia": fisciano 6-7 giugno

Convegno "Contare e Raccontare. Fra matematica e Letteratura

Percorso di Crittografia svolto al Liceo Majorana di Roma

L.S. Plinio Seniore	Roma	Antonio Fanelli
L.S. Pascal	Roma	Donatella Ricalzone
L.S. Tasso	Roma	Maria Laura Monaco
L.S. Vittoria Colonna	Roma	
L.S. Majorana		
L.S. Francesco d'Assisi	Roma	
* I.I.S. Croce Alcramo	Roma	Maria Antonella Pugliese
L.S. Gullace Talotta	Roma	Stefano Volpe
L.S. Tullio Levi-Civita	Roma	Paolo Francini



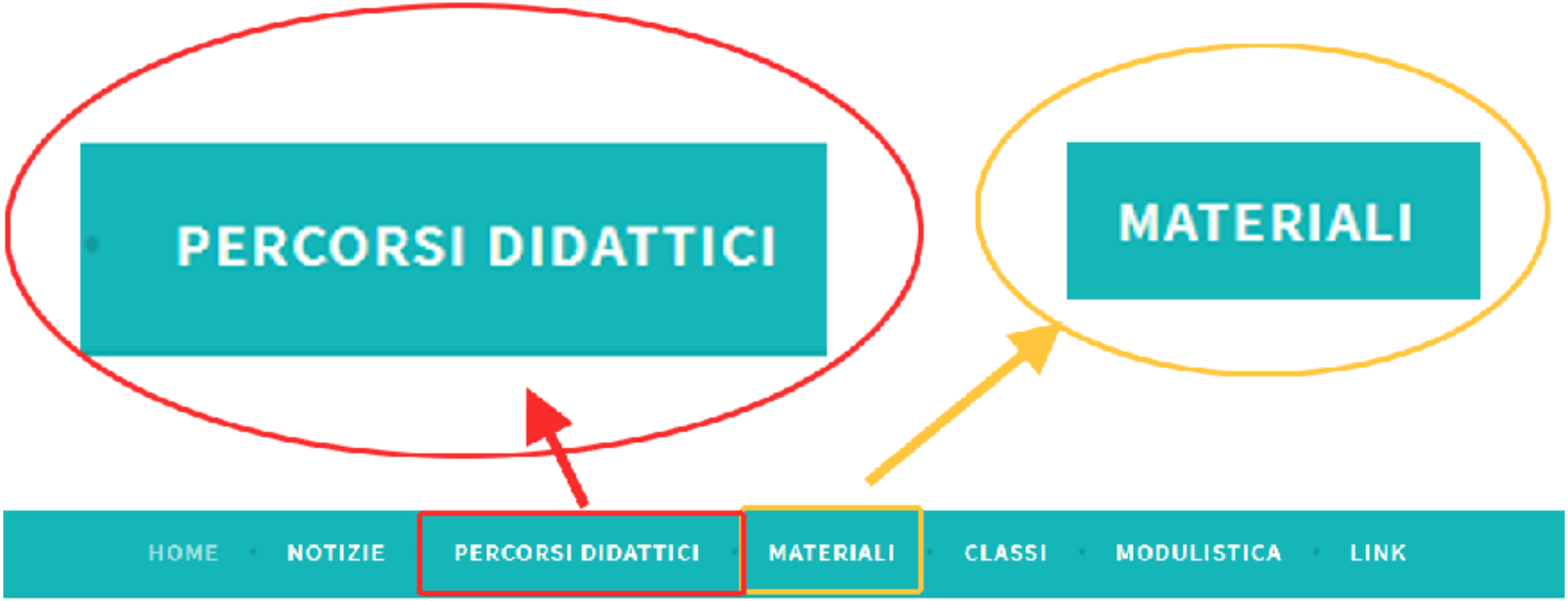
Percorso di Crittografia svolto al Liceo Majorana di Roma

Liceo Matematico Majorana – Roma

- laboratori, giochi matematici e scoperte -

HOME · NOTIZIE · PERCORSI DIDATTICI · MATERIALI · CLASSI · MODULISTICA · LINK

Percorso di Crittografia svolto al Liceo Majorana di Roma



Grazie per l’attenzione