Concludiamo la parte relativa alla trasposizione con un'idea tanto semplice quanto efficace: per migliorare un sistema veloce sia in frase di cifratura che di decifratura ma non abbastanza robusto, si può semplicemente applicarlo più di una volta allo stesso messaggio (così come il mazziere ripete molte volte una singola azione che da sola ha uno scarso potere di rimescolamento).
Nei sistemi a chiave si può immaginare di applicare chiavi diverse ad ogni ripetizione (in fase di decrittazione bisogna naturalmente ricordarsi di usare le chiavi in senso inverso), applicare metodi diversi ad ogni iterazione (magari alternando lo ZigZag con altri percorsi) o, per maggiore semplicità (e minore sicurezza), si può decidere di usare sempre lo stesso metodo e con la stessa chiave.

Per maggiore chiarezza espositiva vedremo soltanto ripetizioni semplici con metodo e chiave invariati.

Vediamo un primo esempio con il metodo a colonna SENZA CHIAVE e poi un secondo con la chiave "Esempio". In entrambi i casi la frase da cifrare è "Questa trasposizione è ripetuta", cioè `QUESTATRASPOSIZIONEERIPETUTA`.

Esempio 1 – Doppia trasposizione a colonna senza chiave

Prima tabella

Q	U	E	S	T	A	T
R	A	S	P	O	S	I
Z	I	O	N	E	E	R
I	P	E	T	U	T	A

Prima codifica

```
QRZIU - AIPES - OESPN -
TTOEU - ASETT - IRA
```

Seconda tabella

Q	R	Z	I	U	A	I
P	E	S	O	E	S	P
N	T	T	O	E	U	A
S	E	T	T	I	R	A

Seconda codifica (FINALE)

```
QPNSR - ETEZS - TTIOO -
TUEEI - ASURI - PAA
```

Esempio 2 – Doppia trasposizione a colonna con chiave

Prima tabella

E	S	E	M	P	I	O
1	7	2	4	6	3	5
Q	U	E	S	T	A	T
R	A	S	P	O	S	I
Z	I	O	N	E	E	R
I	P	E	T	U	T	A

Prima codifica

QRZIE – SOEAS – ETSPN –
TTIRA – TOEUU – AIP

Seconda tabella

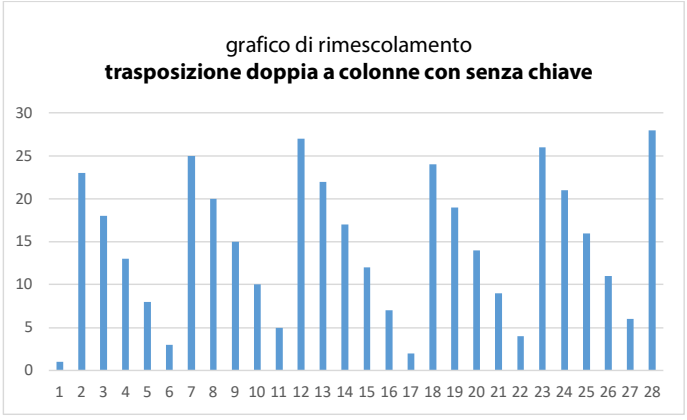
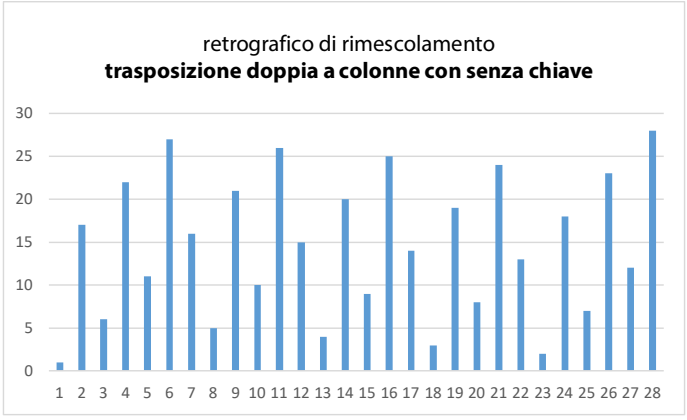
E	S	E	M	P	I	O
1	7	2	4	6	3	5
Q	R	Z	I	E	S	O
E	A	S	E	T	S	P
N	T	T	I	R	A	T
O	E	U	U	A	I	P

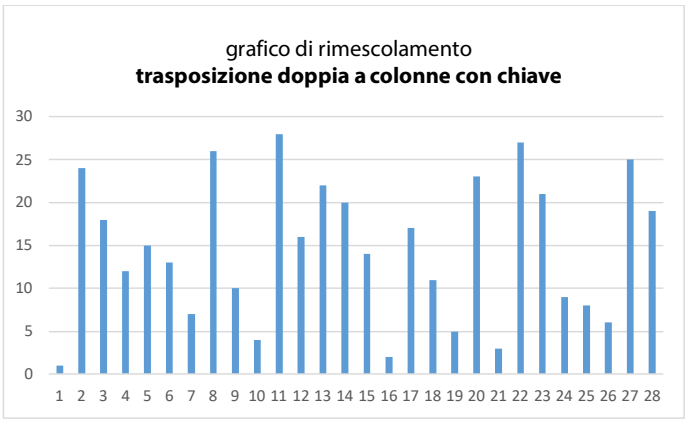
Seconda codifica (FINALE)

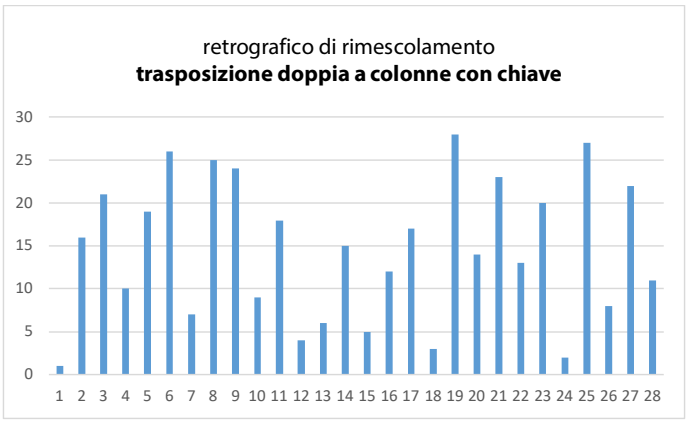
QENOZ – STUSS – AIIEI –
UOPTP – ETRAR – ATE

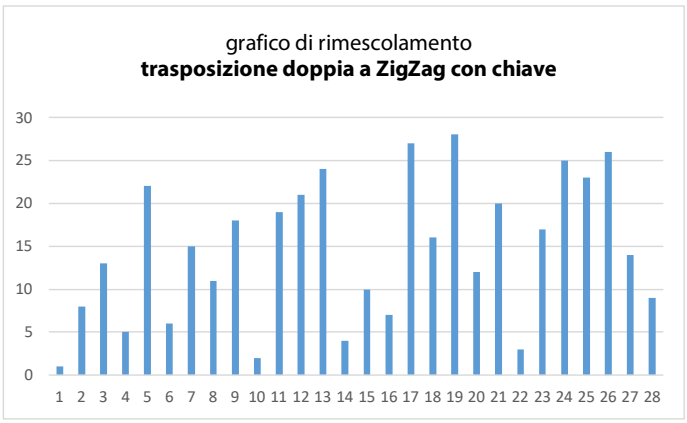
Per valutare la bontà di questa ripetizione, analizziamo i rispettivi grafici di rimescolamento, aggiungendo anche la doppia cifratura a *ZigZag* con la solita chiave “esempio”:

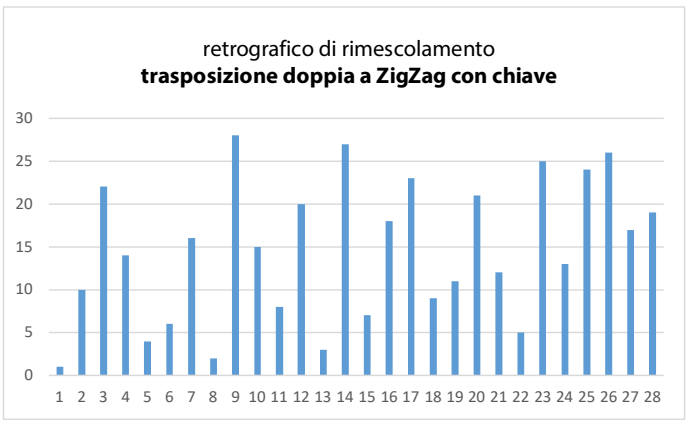
Come al solito il messaggio in chiaro è la sequenza $1,2,\dots,28$ rappresentata inizialmente con un istogramma “in salita” ($vedi\ a\ fianco \rightarrow$). Nel seguito, nei metodi a chiave, questa è sempre “esempio”.

Qui in basso il messaggio $1,2,\dots,28$ come appare dopo la cifratura.	Qui in basso la *retrocifra* dei messaggi cifrati, il grafico che rappresenta meglio la visuale dell’intercettatore (perché mostra come vengono “spezzate” le parole)
	









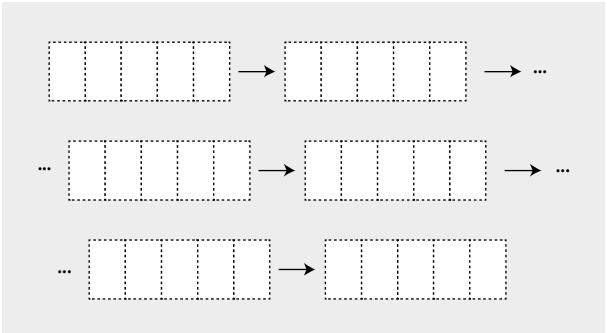
Come si evince dai grafici, la doppia cifratura rompe le regolarità in modo sorprendentemente efficace: anche la semplice trasposizione a colonne con chiave appare infatti piuttosto irregolare.

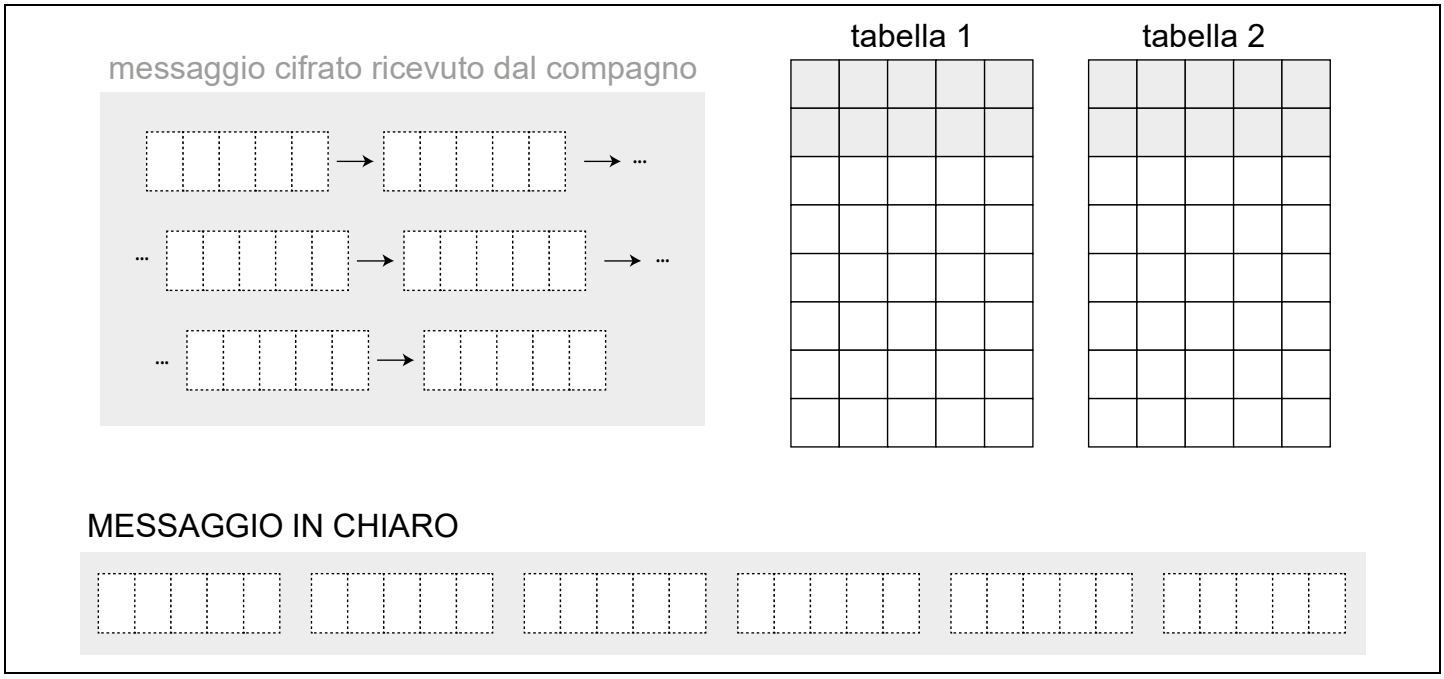
5.1) Inventa un messaggio di 30 lettere (aggiungendo eventualmente delle lettere riempitive finali) e cifralo con una doppia trasposizione a colonne con la chiave “CIELO”. Passa poi il tuo messaggio cifrato ad un compagno e fatti dare il suo. Cercate quindi entrambi di riportare in chiaro ciascuno il messaggio dell’altro (in basso una serie di tabelle che potrebbero esservi utili).

tabella 1

tabella 2

messaggio cifrato da dare al compagno



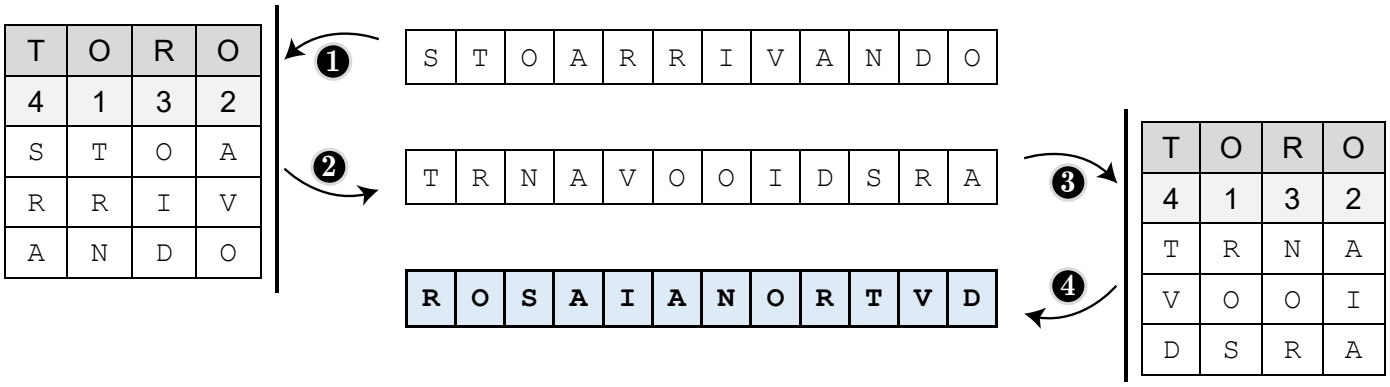


A questo punto di potrebbe pensare che la tripla cifratura sia più sicura della doppia, la quadrupla della tripla e così via. Questa è una conclusione generalmente falsa, come verrà chiarito in questa lezione. Per consentire un'esposizione più chiara è però bene introdurre dei metodi standard di rappresentazione delle trasposizioni.

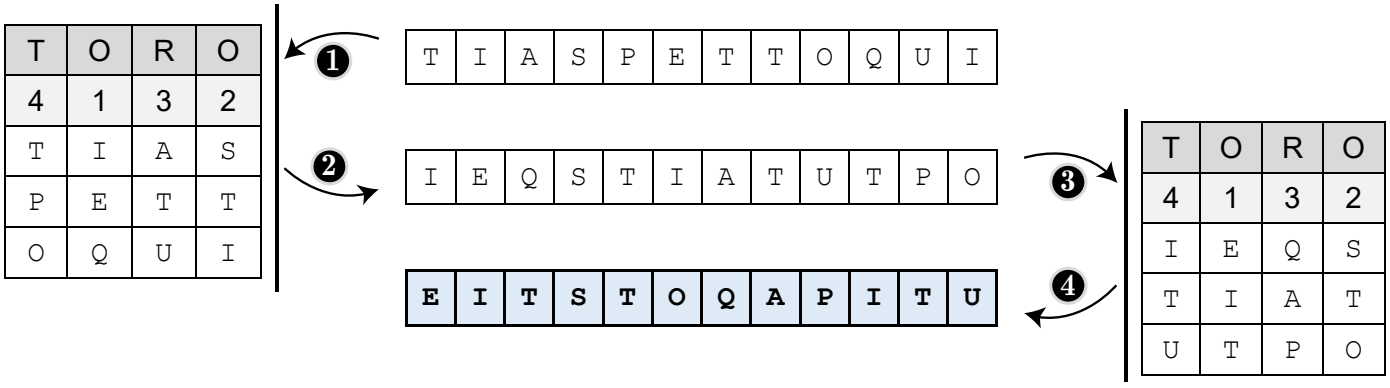
Rappresentazione di una trasposizione

Supponiamo di avere due messaggi entrambi composti da n lettere e sottoposti alla stessa trasposizione. In basso è mostrato un caso del genere, nel quale vengono trasposti due messaggi (entrambi di 12 lettere) mediante una **doppia cifratura** a colonne con la chiave TORO.

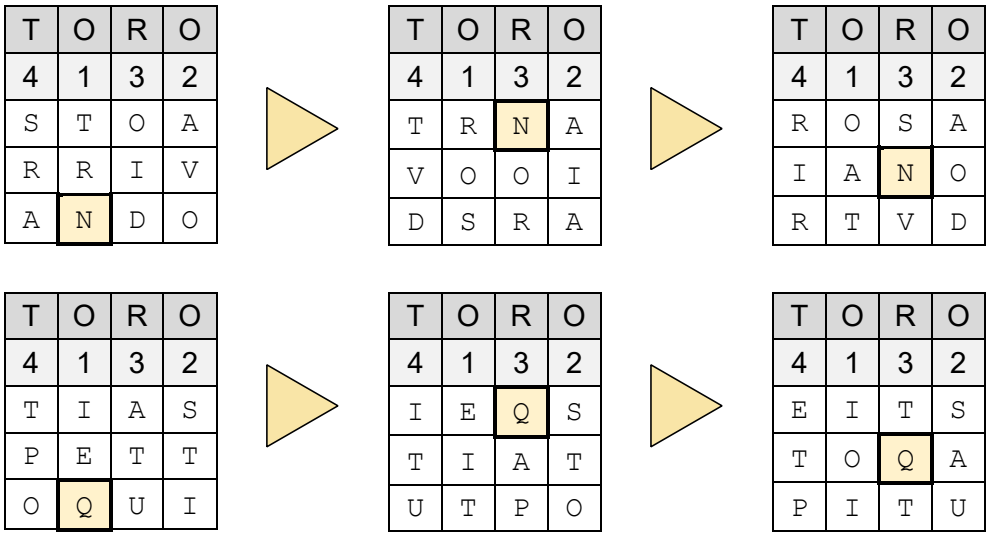
Trasposizione del **messaggio 1**: "Sto arrivando"



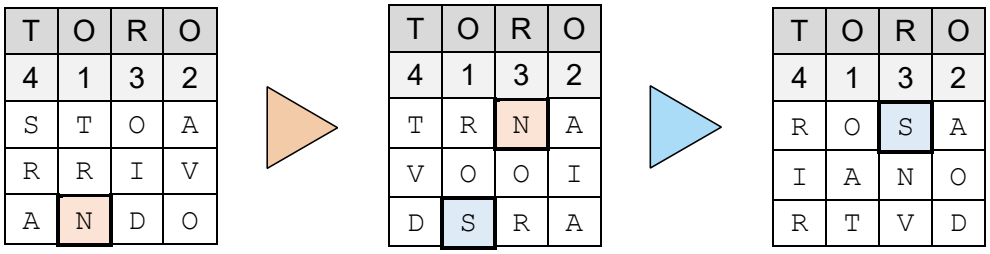
Trasposizione del **messaggio 2**: "Ti aspetto qui"



Le due frasi cifrate sono evidentemente diverse, ma entrambi i messaggi sono stati sottoposti alla stessa identica trasformazione, determinata univocamente dalla lunghezza del messaggio e dalla chiave (che fissa anche il numero di colonne del rettangolo di trasposizione). Per capire appieno quanto affermato, conviene fissare una cella posta in una certa posizione ed osservare il suo "tragitto" durante la cifratura nei due casi presentati sopra:

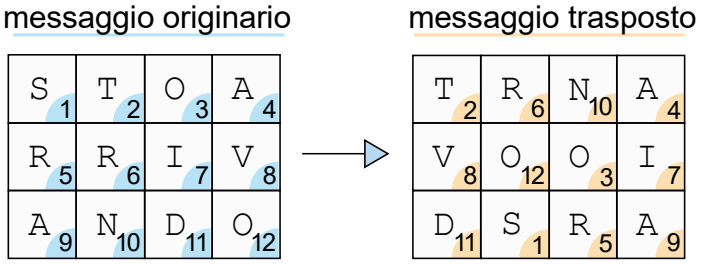


Come si vede in entrambi i casi la cella "si muove" allo stesso modo, segno evidente che la trasposizione usata per le due cifrature è la stessa. Notiamo inoltre che la trasposizione si basa su una cifratura ripetuta, circostanza che può essere osservata dal seguente schema: si vede infatti che il secondo elemento della terza riga viene spostato nella prima riga in terza posizione, indipendentemente dal suo contenuto.



Aver cifrato i due messaggi iniziali (di lunghezza uguale) con una doppia cifratura a chiave costante, si può quindi non solo riassumere con "abbiamo fatto due volte la stessa cosa" ma addirittura "abbiamo fatto quattro volte la stessa cosa" (la singola trasposizione con chiave `TORO`)

Questa premessa ha lo scopo di convincervi della necessità di rappresentare una trasposizione in modo **indipendente** dal contenuto del messaggio oggetto della trasformazione. Questo ci consentirà di rappresentare tutte le trasposizioni viste finora allo stesso modo e di farne oggetto di "algebra", come accenneremo alla fine. Torniamo alla prima trasformazione del messaggio 1, da `STOARRIVANDO` a `TRNAVOOIDSRA` (si tratta della prima delle due trasposizioni della doppia cifratura)



Nel primo rettangolo, le celle sono tutte numerate nell'ordine canonico, ogni riga è percorsa da sinistra a destra e le righe sono compilate dall'alto verso il basso. Tale numerazione rispecchia l'ordine di scrittura e rappresenta la posizione delle lettere nel messaggio originario. Immaginando tutte le celle come tessere di un mosaico, il messaggio trasposto rappresenta semplicemente una loro ricomposizione. I numeri scritti in ciascuna cella della tabella di destra non rappresentano più l'ordine di lettura, ma la posizione che le celle occupavano prima di essere trasposte. Confrontando le due griglie, si vede che la "vecchia prima posizione" (occupata dalla S) è finita in "decima posizione" (basta cercare il numero 1 nella tabella di destra e utilizzare i numeri in azzurro della tabella di sinistra per determinarne il numero d'ordine), la "vecchia posizione 2" (occupata dalla T) è finita nella "nuova posizione 1" e così via. Tutto ciò permette di costruire la seguente tabella:

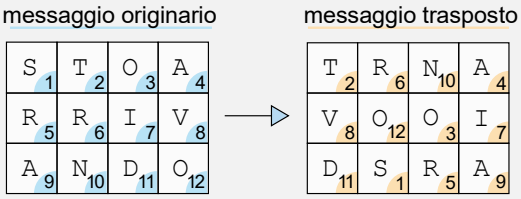
Posizione di partenza	↓	1	2	3	4	5	6	7	8	9	10	11	12
Posizione di arrivo		10	1	7	4	11	2	8	5	12	3	9	6

La griglia così costruita, detta **tabella di permutazione**, descrive la trasposizione in modo completo. Possiamo identificare la trasposizione con la tabella stessa o eventualmente con la sua ultima riga (visto che la prima è sempre 1,2,3, ...). Tale sequenza numerica viene normalmente scritta tra parentesi quadre (nel caso precedente avrà quindi [10 1 7 4 11 2 8 5 12 3 9 6]) ed è detta **traccia della permutazione**

Il metodo usato normalmente per determinare la tabella di permutazione è il seguente:

1) Si trascrivono in ordine i numeri della griglia trasposta su una riga
2) Sulla seconda riga si inserisce la sequenza 1,2,3,…
3) Si riordinano le colonne in base ai numeri delle prima riga

Esempio



Passaggio 1

2	6	10	4	8	12	3	7	11	1	5	9

Passaggio2

2	6	10	4	8	12	3	7	11	1	5	9
1	2	3	4	5	6	7	8	9	10	11	12

Passaggio 3

1	2	3	4	5	6	7	8	9	10	11	12
10	1	7	4	11	2	8	5	12	3	9	6

Esercizio 5.2) Componi le tabelle di permutazione associate alle seguenti cifrature per trasposizione:

	Metodo	Chiave	Lunghezza del messaggio
a)	Trasposizione a colonna	MIR	9

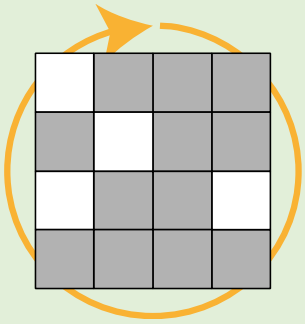
SOLUZIONE **a)** →

	1	2	3	4	5	6	7	8	9
traccia									

	Metodo	Chiave	Lunghezza del messaggio
b)	Trasposizione a chiave scalare	MILANO	10

SOLUZIONE **b)** →

	1	2	3	4	5	6	7	8	9	10
traccia										

	Metodo	Chiave	Lunghezza del messaggio
c)	Griglia quadrata 4×4		16

SOLUZIONE **c)** →

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

Usare la **tabella di permutazione** per crittare un messaggio è molto semplice:

1) Si predispone una tabella di quattro righe e tante colonne quante sono le lettere del messaggio

- Le prime righe sono dedicate alla **tabella di permutazione** (la traccia va nella seconda riga)
- Nella terza riga va scritto il messaggio in chiaro
- L'ultima riga va lasciata libera per inserirvi il messaggio cifrato

(nell'esempio si parte dal solito messaggio "Sto arrivando")

	1	2	3	4	5	6	7	8	9	10	11	12
TABELLA DI PERMUTAZIONE	10	1	7	4	11	2	8	5	12	3	9	6
MESSAGGIO IN CHIARO	S	T	O	A	R	R	I	V	A	N	D	O
MESSAGGIO CIFRATO												

2) Predisposta la tabella, si scorrono le lettere del messaggio in chiaro assieme ai numeri della traccia di permutazione (la seconda riga): essi ci diranno dove andrà a finire ciascuna lettera. La `S` ad esempio va inserita nella posizione (colonna) 10, la `T` nella posizione 1, la `O` della posizione 7, la `A` resterà dov'è, e così via…

TABELLA DI PERMUTAZIONE	1	2	3	4	5	6	7	8	9	10	11	12
	10	1	7	4	11	2	8	5	12	3	9	6
MESSAGGIO IN CHIARO	S	T	O	A	R	R	I	V	A	N	D	O
MESSAGGIO CIFRATO (una volta)	T	R	N	A	V	O	O	I	D	S	R	A

Per trovare la "doppia trasposizione" del messaggio (così come visto all'inizio), basterà applicare la stessa tecnica al codice appena ottenuto:

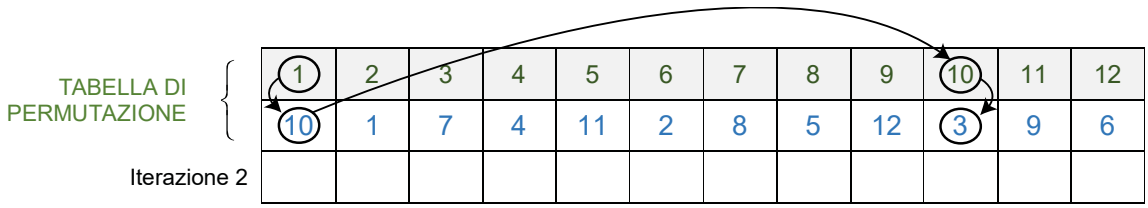
TABELLA DI PERMUTAZIONE	1	2	3	4	5	6	7	8	9	10	11	12
	10	1	7	4	11	2	8	5	12	3	9	6
MESSAGGIO CIFRATO (una volta)	T	R	N	A	V	O	O	I	D	S	R	A
MESSAGGIO CIFRATO (due volte)	R	O	S	A	I	A	N	O	R	T	V	D

Da notare che la stessa identica tabella di permutazione genererà anche la doppia cifratura `TIASPETTOQUI→EITSTOQAPITU` (il secondo messaggio visto prima).

Per sviluppare il discorso nella direzione più feconda, è opportuno vedere un altro modo per giungere allo stesso risultato: determiniamo la tabella di permutazione della "doppia trasposizione", applicando la tabella di permutazione alla sua traccia:

TABELLA DI PERMUTAZIONE	1	2	3	4	5	6	7	8	9	10	11	12
	10	1	7	4	11	2	8	5	12	3	9	6
Iterazione 2												

Avremo che l'1 finisce in 10 e il 10 finisce in 3. (vedi sotto)



Possiamo quindi scrivere…

TABELLA DI PERMUTAZIONE	1	2	3	4	5	6	7	8	9	10	11	12
	10	1	7	4	11	2	8	5	12	3	9	6
Iterazione 2	**3**											

Applicando lo stesso procedimento a tutte le posizioni della traccia, si arriva a…

TABELLA DI PERMUTAZIONE	1	2	3	4	5	6	7	8	9	10	11	12
	10	1	7	4	11	2	8	5	12	3	9	6
Iterazione 2	**3**	**10**	**8**	**4**	**9**	**1**	**5**	**11**	**6**	**7**	**12**	**2**

Va da sé che applicando la traccia relativa alla seconda iterazione, si ottiene di nuovo…

TABELLA DI PERMUTAZIONE	1	2	3	4	5	6	7	8	9	10	11	12
	3	10	8	4	9	1	5	11	6	7	12	2
MESSAGGIO IN CHIARO	S	T	O	A	R	R	I	V	A	N	D	O
MESSAGGIO CIFRATO (una volta)	R	O	S	A	I	A	N	O	R	T	V	D

Quello che abbiamo appena visto accelera decisamente la tecnica della cifratura iterata: una volta stabilita la tabella di permutazione, è infatti un gioco da ragazzi trovare le cifratura doppia, tripla, quadrupla e così via. Bisogna però prestare attenzione ad agire in modo consapevole sui numeri in tabella. Il seguente esempio chiarirà il problema:

TABELLA DI PERMUTAZIONE	1	2	3	4	5	6	7	8	9	10	11	12
	10	1	7	4	11	2	8	5	12	3	9	6
Iterazione 2	**3**	**10**	**8**	**4**	**9**	**1**	**5**	**11**	**6**	**7**	**12**	**2**
Iterazione 3	**?**											
Iterazione 4												

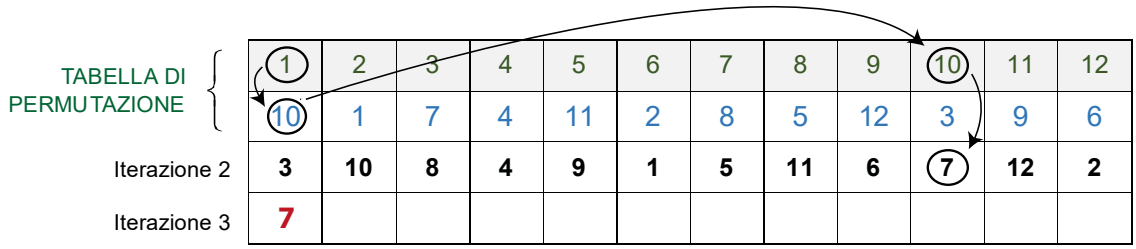
Volendo stabilire il numero che va posto nella cella con il punto interrogativo bisogna avere bene presente cosa si sta facendo: al momento, dopo la doppia cifratura, il primo elemento del messaggio in chiaro sta in terza posizione. Dove finirà alla prossima cifratura?

5.4) Secondo voi, quale o quali dei quattro schemi in basso descrive la **tripla cifratura a colonna** e risponde alla questione posta?

a) ☐

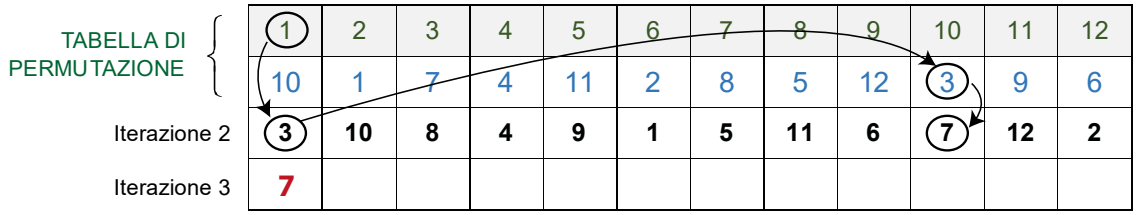
TABELLA DI PERMUTAZIONE	(1)	2	(3)	4	5	6	7	8	9	10	11	12
	10	1	(7)	4	11	2	8	5	12	3	9	6
Iterazione 2	(3)	**10**	**8**	**4**	**9**	**1**	**5**	**11**	**6**	**7**	**12**	**2**
Iterazione 3	**7**											

b) ☐



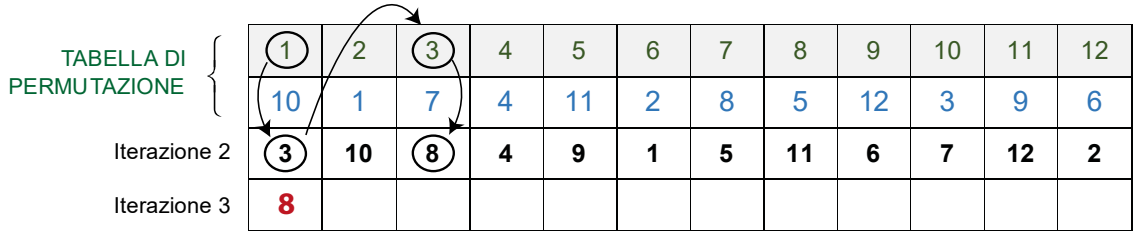
	1	2	3	4	5	6	7	8	9	10	11	12
TABELLA DI PERMUTAZIONE	10	1	7	4	11	2	8	5	12	3	9	6
Iterazione 2	**3**	**10**	**8**	**4**	**9**	**1**	**5**	**11**	**6**	**7**	**12**	**2**
Iterazione 3	**7**											

c) ☐



	1	2	3	4	5	6	7	8	9	10	11	12
TABELLA DI PERMUTAZIONE	10	1	7	4	11	2	8	5	12	3	9	6
Iterazione 2	**3**	**10**	**8**	**4**	**9**	**1**	**5**	**11**	**6**	**7**	**12**	**2**
Iterazione 3	**7**											

d) ☐



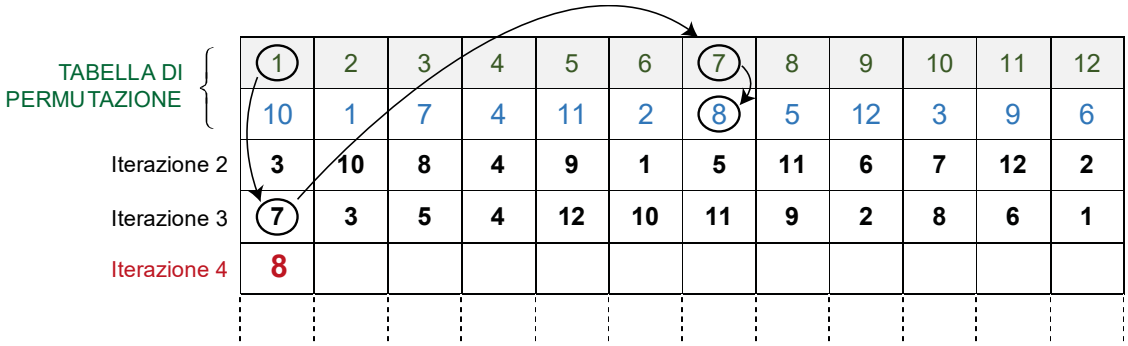
	1	2	3	4	5	6	7	8	9	10	11	12
TABELLA DI PERMUTAZIONE	10	1	7	4	11	2	8	5	12	3	9	6
Iterazione 2	**3**	**10**	**8**	**4**	**9**	**1**	**5**	**11**	**6**	**7**	**12**	**2**
Iterazione 3	**8**											

(la soluzione a seguire, non sbirciare!)

Soluzione 5.4)

Sono giusti i tre schemi **a,b,c**, la coincidenza dei valori non è infatti affatto accidentale. Lo schema proposto in **a)** è il più classico: per ottenere la cifratura tripla si applica alla cifratura doppia (seconda riga) una cifratura singola (prima riga). Nel caso **b)** si applica prima una cifratura singola e ad essa una cifratura doppia. Lo schema **c)** ripropone in chiave diversa e un po' cervellotica quanto fatto in **a)**.

È interessante soffermarsi sullo schema **d)**: esso non rappresenta una cifratura tripla, bensì una cifratura quadrupla, ottenuta applicando due volte una cifratura doppia. Il seguente schema mostra in modo alternativo che il primo elemento di un messaggio in chiaro finirà dopo 4 trasposizioni proprio nella posizione 8:



Abbiamo incidentalmente scoperto un modo estremamente efficiente per iterare trasposizioni. Utilizzando infatti sempre lo schema $prima\ riga \rightarrow ultima\ riga \rightarrow prima\ riga \rightarrow ultima\ \ riga$ possiamo ogni volta raddoppiare il numero di iterazioni.

Nell'esempio seguente, si vede un calcolo brevissimo con il quale si ottiene una cifratura di ordine 16! Per capire quanto sia efficiente questo metodo, considera un computer in grado di calcolare ogni secondo una nuova trasposizione iterata; dovendo calcolare una cifratura che sia miliardesima (o più), il computer impiegherebbe circa 34 anni per calcolarla con il metodo classico (un miliardo di secondi fanno circa 34 anni) e soltanto 30 secondi con il metodo appena introdotto (infatti $2^{30} > 10^9$).

TABELLA DI PERMUTAZIONE	1	2	3	4	5	6	7	8	9	10	11	12
	10	1	7	4	11	2	8	5	12	3	9	6
Iterazione 2	**3**	**10**	**8**	**4**	**9**	**1**	**5**	**11**	**6**	**7**	**12**	**2**
Iterazione 2^2 (cioè 4)	**8**	**7**	**11**	**4**	**6**	**3**	**9**	**12**	**1**	**5**	**2**	**10**
Iterazione 2^3 (cioè 8)	**12**	**9**	**2**	**4**	**3**	**11**	**1**	**10**	**8**	**6**	**7**	**5**
Iterazione 2^4 (cioè 16)	**5**	**8**	**9**	**4**	**2**	**7**	**12**	**6**	**10**	**11**	**1**	**3**

5.5a) Calcola la <u>cifratura ottava</u> ottenuta iterando la trasposizione di traccia $[3\ 4\ 2\ 5\ 9\ 1\ 8\ 6\ 7]$ (*ti conviene utilizzare la griglia a fianco*)

5.5b) Calcola la cifratura quinta ottenuta iterando la trasposizione di traccia $[3\ 7\ 2\ 5\ 1\ 4\ 6]$ (*ti conviene utilizzare la griglia a fianco*)

In generale è sempre possibile ricondurre un intero N ad una somma di potenze di due, basterà riscrivere N in codice binario (questo però è un filone enl quale non ci addentreremo).

Consideriamo la seguente questione: i grafici di rimescolamento hanno mostrano che applicare più volte uno stesso metodo di trasposizione, anche se fragile, ne aumenta notevolmente la robustezza. Contestualmente, le ultime tecniche apprese ci permettono di iterare qualsiasi metodo un numero quasi illimitato di volte in tempi ragionevoli. Sembrerebbe quindi che la nostra capacità di crittare sia cresciuta esponenzialmente e che sia scesa quasi a zero la nostra speranza di intercettare/decrittare comunicazioni destinate ad altri.

Il seguente esempio mostrerà che le cose non stanno esattamente così:

Esempio
Determiniamo la cifratura quarta della trasposizione di traccia $[9\ 3\ 8\ 1\ 4\ 11\ 2\ 7\ 5\ 10\ 6]$.

Svolgimento

0	1	2	3	4	5	6	7	8	9	10	11
1	9	3	8	1	4	11	2	7	5	10	6
2	**5**	**8**	**7**	**9**	**1**	**6**	**3**	**2**	**4**	**10**	**11**
4	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**

Pare che il mazziere abbia mescolato le carte talmente spesso da averle riportate in fila! L'esempio appena visto mostra che non ha senso cifrare uno stesso messaggio più volte se c'è il rischio che l'ordine si ricrei spontaneamente. Vediamo un altro esempio:

5.6) Calcola la cifratura sesta della trasposizione di traccia $[4\ 6\ 8\ 5\ 1\ 9\ 2\ 7\ 3]$. (come al solito ti conviene utilizzare la griglia sottostante)

La rappresentazione per cicli disgiunti

Per fortuna è facile prevedere a monte quale sarà la ciclicità di questo tipo di meccanismo. Per mettere in luce questo aspetto, è però necessario introdurre una notazione diversa dalla tabella delle permutazioni: la rappresentazione **per cicli**. Per capire di che cosa di tratta, consideriamo la trasposizione di traccia $[4\ 6\ 9\ 5\ 1\ 10\ 2\ 7\ 8\ 3\ 12\ 11]$. Conviene scrivere in modo ordinato la tabella di permutazione:

TABELLA DI PERMUTAZIONE

1	2	3	4	5	6	7	8	9	10	11	12
4	6	9	5	1	10	7	2	8	3	12	11

Consideriamo il numero $\boxed{1}$ e seguiamo tutto il suo percorso (detto orbita) fino al suo ritorno al valore iniziale. Costruiamo le orbite soltanto per gli elementi di cui non conosciamo il tragitto (se cioè un numero è già presente nell'orbita di un altro non perderemo tempo a ricalcolarne tutto il percorso)

elemento di partenza	orbita
1	$(1 \to 4 \to 5)$
2	$(2 \to 6 \to 10 \to 3 \to 9 \to 8)$
$3,6,7,8,9,10$	…
$4,5$	…
7	(7)
11	$(11 \to 12)$

La tabella delle orbite permette di introdurre la seguente importantissima notazione, detta rappresentazione **per cicli disgiunti**:

$$[4\ 6\ 9\ 5\ 1\ 10\ 2\ 7\ 8\ 3\ 12\ 11] \quad = \quad (1\ 4\ 5)\,(2\ 6\ 10\ 3\ 9\ 8)\,(7)\,(11\ 12)$$

(traccia della permutazione)

(concatenazione di cicli disgiunti)

Definizioni
Data una regola matematica T, si chiama **orbita** di un elemento E, la sequenza ordinata che parte da E ed elenca, senza ripetizioni, tutti i valori che si ottengono applicando ripetutamente la regola T. Se T è una trasposizione, T^n indica l'n-esima iterazione di T.
Se l'orbita di un elemento E è una sequenza finita, essa si dice **ciclo**. Due o più cicli si dicono **disgiunti** se non hanno elementi in comune. L'insieme di più cicli applicati contemporaneamente si dice **concatenazione**. La concatenazione $(1)(2)(3)$ ... si chiama **identità** (si tratta della trasposizione che non cambia posizione a nessun elemento). Il più piccolo intero positivo P per il quale vale che T^P è un'identità si dice **periodo** di T.

Questi nuovi oggetti matematici possono essere scritti in molti modi diversi, per cui è bene fissare un'ortografia:

Un ciclo è scritto in **forma normale** se inizia con il suo elemento minore.
Una concatenazione di cicli disgiunti è scritta in **forma ordinata** se i cicli sono scritti in forma normale e disposti in ordine crescente rispetto al loro primo elemento.

Come il buonsenso suggerisce, vale il seguente risultato:

Teorema
Ogni *traccia di permutazione* può essere rappresentata in un unico modo mediante una *concatenazione ordinata di cicli disgiunti*.

Tocca ora fare un po' di pratica.

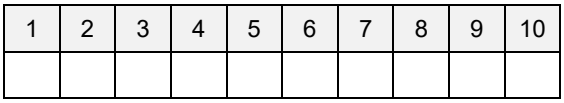
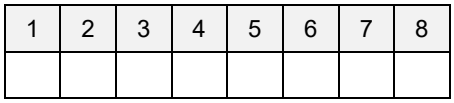
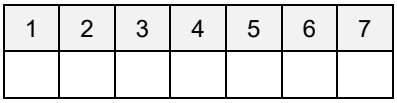
5.7) Riscrivi le tabelle di permutazione elencate in forma di cicli disgiunti (se possibile scritti in forma normale)

	Tabelle di permutazione	Rappresentazione per cicli disgiunti
a)	1 2 3 4 5 6 7 8 9 10 11 **5 3 1 11 2 4 7 9 8 6 10**	
b)	1 2 3 4 5 6 7 8 9 **3 5 7 6 2 9 1 4 8**	
c)	1 2 3 4 5 6 7 8 9 10 **10 7 2 8 6 1 9 5 4 3**	
d)	1 2 3 4 5 6 7 8 **1 3 5 7 2 4 6 8**	
e)	1 2 3 4 5 6 7 **7 6 3 4 5 2 1**	

Vediamo ora di fare la mano anche con l'operazione inversa:

5.8) Riscrivi le tabelle di permutazione elencate in forma di cicli disgiunti (se possibile scritti in forma normale)

	Rappresentazione per cicli disgiunti	Tabelle di permutazione
a)	$(1\ 7\ 8)\,(2\ 11)\,(3\ 4\ 5\ 10)\,(6\ 9)$	1 2 3 4 5 6 7 8 9 10 11 _ _ _ _ _ _ _ _ _ _ _
b)	$(1\ 5\ 3\ 7\ 8\ 4\ 2\ 9\ 6)$	1 2 3 4 5 6 7 8 9 _ _ _ _ _ _ _ _ _

c)	$(1\ 10)\,(2\ 9)\,(3\ 8)\,(4\ 7)\,(5\ 6)$	
d)	$(1\ 2\ 3\ 4\ 5\ 6\ 7\ 8)$	
e)	$(1\ 7)\ (2)\ (3)\ (4\ 6\ 5)$	

La *rappresentazione per cicli disgiunti* è sicuramente uno dei modi più potenti per rappresentare una trasposizione. Il seguente esercizio mette in luce alcuni vantaggi della notazione introdotta:

5.9) Considera la trasposizione $T = (1\ 7\ 8)\,(2\ 11)\,(3\ 4\ 5\ 10)\,(6\ 9)$ (ripresa da un esercizio precedente). Indichiamo poi con T^2 la cifratura doppia, con T^3 la cifratura tripla e così via. Rispondi alle seguenti domande:

- **a)** Rappresenta in forma di concatenazione di cicli disgiunti T^2
- **b)** Rappresenta in forma di concatenazione di cicli disgiunti T^3.
- **c)** Rappresenta in forma di concatenazione di cicli disgiunti T^4.
- **d)** Quale è il periodo di T, cioè per quale n vale $T^n = (1)(2)(3)(4)(5)(6)(7)(8)(9)(10)(11)(12)$?
- **e)** Quale è il più piccolo n intero positivo per il quale $T^n = T$?
- **f)** Rappresenta in forma di concatenazione di cicli disgiunti T^{123}.
- **g)** Quale è la rappresentazione per cicli disgiunti di un cifrario di Cesare generico (con uno slittamento di k unità e una lunghezza non indicata)?

Abbiamo visto che con il simbolo T^n si intende l'n-esima iterazione della trasposizione T. L'utilizzo della stessa notazione delle potenze è giustificato dalle numerose analogie che intercorrono fra la concatenazione di cicli e l'operazione di moltiplicazione. Bisogna però prestare attenzione ad una differenza sostanziale: se (A) e (B) sono due trasposizioni diverse e non disgiunte allora le due concatenazioni $(A)(B)$ e $(B)(A)$ (composte dalle stesse trasposizioni ordinate in modo differente) sono generalmente due trasformazioni diverse. In altre parole l'operazione di concatenazione non è commutativa.

Non resta ora che chiarire il nesso fra ciclicità dell'iterazione (il fenomeno per il quale dopo un certo numero di iterazioni si ritorna ad una sequenza ordinata) e cicli che compongono la trasposizione.

5.10) Secondo te che legame sussiste fra la ciclicità dell'iterazione e cicli che compongono la trasposizione?

(la soluzione a seguire, non sbirciare!)

Vale il teorema seguente:

Teorema
Siano $L_1, L_2, \dots$ le lunghezze dei cicli disgiunti concatenati che rappresentano una trasposizione T. Il periodo P_T di T è uguale a $P_T = mcm(L_1, L_2, \dots)$, vale cioè che:

- $T^P = (1)(2)(3) \dots$
- $T^{P+k} = T^k$

Siamo ora finalmente in grado di valutare quante iterazioni di una certa trasposizione fragile possano effettivamente complicare il quadro generare e quante invece rischiano di riportare il messaggio spontaneamente in chiaro (o comunque di riordinarlo). In generale non è una buona idea ripetere lo stesso tipo di trasformazione per un numero di volte maggiore della metà del suo periodo.

Vediamo ora un esercizio che riassume molte delle tecniche viste finora:

Sia T la trasposizione a chiave scalare di chiave `LEGAME` applicata ad un messaggio di 12 simboli.
- **(A)** Costruisci la tabella delle permutazioni di T.
- **(B)** Rappresenta T in forma di cicli concatenati disgiunti e determina il periodo di T
- Verifica il periodo di T con due tecniche diverse:
  - **(C)** la tabella (veloce) delle iterazioni
  - **(D)** applicando T P volte ad un messaggio qualsiasi composto da 12 lettere

L	E	G	A	M	E
5	2	4	1	6	3
			1	**2**	**3**
	4	**5**	**6**	**7**	**8**
					9
		10	**11**	**12**	

4	5	10	1	6	11	2	7	12	3	8	9
1	2	3	4	5	6	7	8	9	10	11	12

1	2	3	4	5	6	7	8	9	10	11	12
4	7	10	1	2	5	8	11	12	3	6	9

Tabella di permutazione

1	2	3	4	5	6	7	8	9	10	11	12
4	7	10	1	2	5	8	11	12	3	6	9

Cicli disgiunti: $(1\ 4)\ (2\ 7\ 8\ 11\ 6\ 5)\ (3\ 10)\ (9\ 12)$

$mcm(2,6,2,2) = 6$

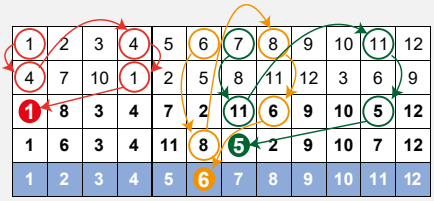
periodo $P_T = 6$

Verifica del periodo con la tabella (veloce) delle iterazioni

0	1	2	3	4	5	6	7	8	9	10	11	12
(traccia) $2^0 = 1$	4	7	10	1	2	5	8	11	12	3	6	9
$2^1 = 2$	**1**	**8**	**3**	**4**	**7**	**2**	**11**	**6**	**9**	**10**	**5**	**12**
$2^2 = 4$	**1**	**6**	**3**	**4**	**11**	**8**	**5**	**2**	**9**	**10**	**7**	**12**
$4 + 2 = 6$	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**

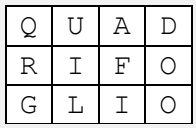
Schema delle operazioni svolte:

- le prime due righe sono la tabella della permutazioni
- la costruzione terza riga è mostrata dalle frecce rosse
- la costruzione quarta riga è mostrata dalle frecce verdi
- la costruzione dell'ultima riga è mostrata dalle frecce arancioni

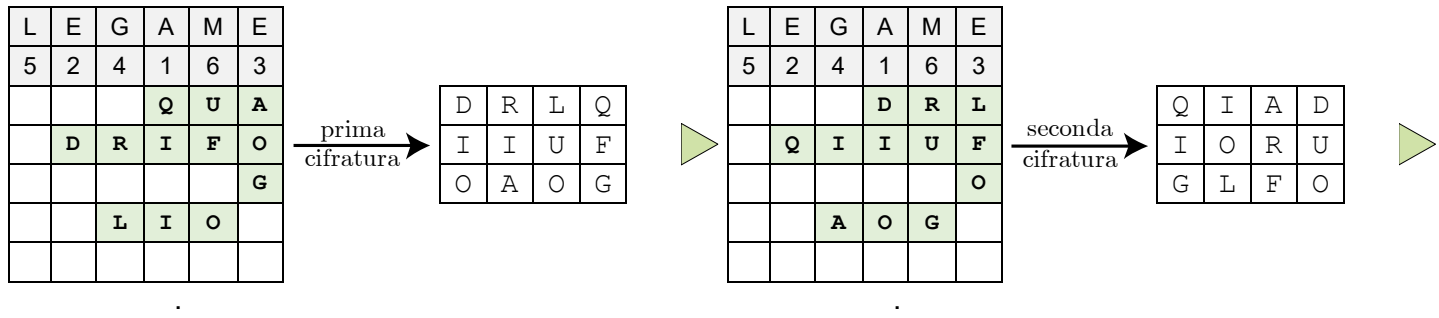


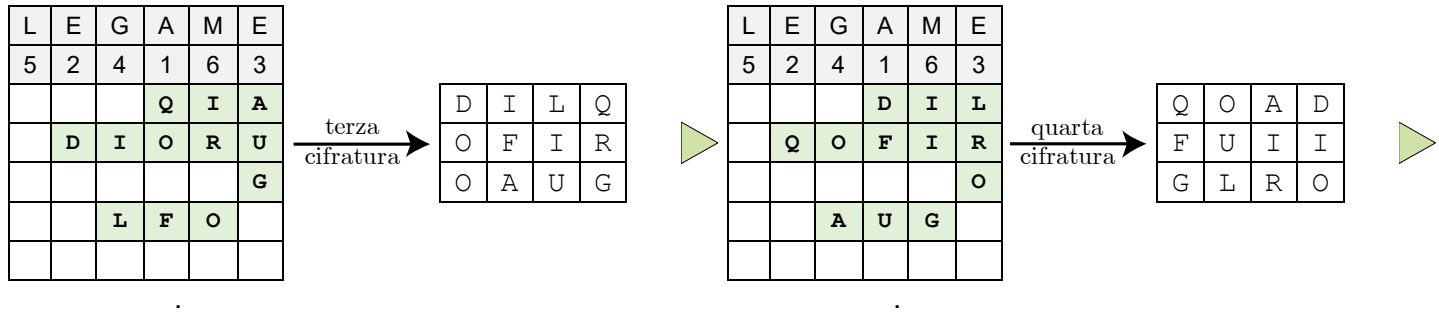
Verifica tramite cifratura iterata del messaggio (di 12 lettere) "QUADRIFOGLIO"

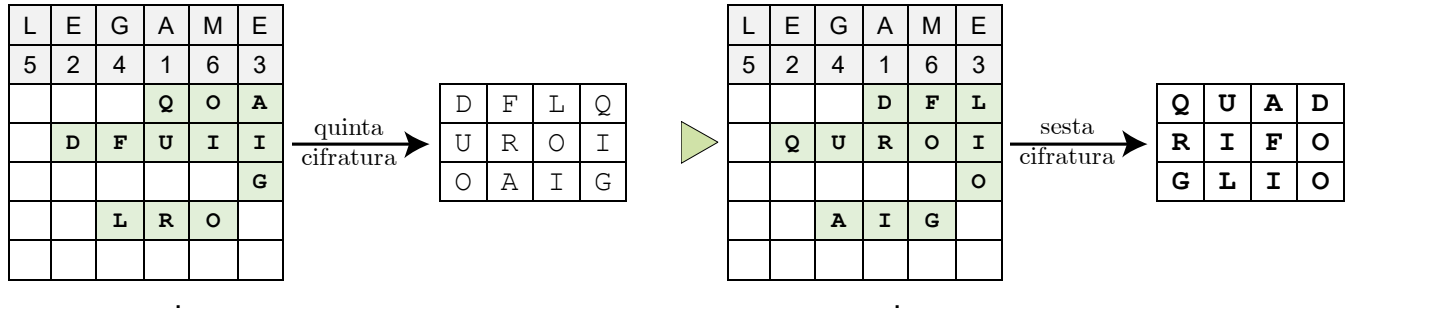
Q	U	A	D	R	I	F	O	G	L	I	O



Q	U	A	D
R	I	F	O
G	L	I	O







5.11) Svolgi tutti i punti elencati in basso (verifica **iv** solo per periodi P_T brevi) per le cifrature proposte in seguito

Le trasposizioni sono tutte idealmente applicate ad un messaggio composto di 12 simboli (come "QUADRIFOGLIO")

- **(i)** Costruisci la tabella delle permutazioni di T.
- **(ii)** Rappresenta T in forma di cicli concatenati disgiunti e determina il periodo di T
- Verifica il periodo di T con due tecniche diverse:
  - **(iii)** la tabella (veloce) delle iterazioni
  - **(iv)** applicando $T\ P$ volte ad un messaggio qualsiasi composto da 12 lettere

a) Cifratura a chiave scalare con chiave GIONA

b) Cifratura a colonne con chiave ARIA

c) Cifratura a chiave scalare con chiave GIUSTO

d) Cifratura a colonne con chiave SCUOLA

e) Cifratura a chiave scalare con chiave LUCE

f) Cifratura a ZigZag con chiave RISO

g) Cifratura a chiave scalare con chiave FAME

h) Cifratura a ZigZag con chiave SOS

i) Cifratura a colonne con chiave LEGAME

5.12) Quale è il periodo massimo di una trasposizione di un messaggio di 15 lettere?

5.13) Trova una tabella delle permutazioni relativa ad un messaggio di 10 lettere di periodo 14.

Trasposizioni inverse

Abbiamo ridotto tutte le trasposizioni di un messaggio di n simboli a una sequenza di n numeri: nel caso della *traccia della permutazione* i numeri sono scritti tra parentesi quadre, nel caso della *rappresentazione per cicli*

disgiunti tra parentesi tonde (variamente distribuite). Possiamo ora affrontare in termini generali il caso della trasposizione inversa, cioè di quella trasformazione che annulla gli effetti di una cifratura.

Data una trasformazione T, chiamiamo **trasformazione inversa** $\boldsymbol{T^{-1}}$ (o *retrotrasformazione*) la trasformazione che concatenata a T restituisci l'identità.

Evidentemente la trasformazione inversa è la trasformazione che interessa il decifratore. Vediamo subito un esempio:

5.14) Considera la trasformazione T rappresentata nei due modi canonici:

Tabella di permutazione di T

1	2	3	4	5	6	7	8	9	10	11	12
7	1	12	3	5	4	2	10	9	8	6	11

Rappresentazione di T per cicli disgiunti

$$(1\ 7\ 2)\ (3\ 12\ 11\ 6\ 4)\ (5)\ (8\ 10)\ (9)$$

Trova le due rappresentazioni della trasformazione inversa T^{-1}

(la soluzione a seguire, non sbirciare!)

Data la tabella di permutazione di una trasformazione T, la tabella della **trasformazione inversa T^{-1}** si ottiene invertendo le righe e riordinando le colonne rispetto alla nuova prima riga.

Data la rappresentazione per cicli disgiunti di una trasformazione T, la **trasformazione inversa T^{-1}** è rappresentata dai cicli invertiti di T (ed eventualmente riordinati in forma normale)

Riprendiamo la cifratura di un messaggio di 12 lettere per chiave scalare `LEGAME` vista in precedenza. La sua tabella di permutazione è la seguente

1	2	3	4	5	6	7	8	9	10	11	12
4	7	10	1	2	5	8	11	12	3	6	9

La tabella di permutazione dell'inversa è quindi la quella riportata in basso a destra:

4	7	10	1	2	5	8	11	12	3	6	9
1	2	3	4	5	6	7	8	9	10	11	12

$\rightarrow$

1	2	3	4	5	6	7	8	9	10	11	12
4	5	10	1	6	11	2	7	12	3	8	9

Per provare l'efficacia della trasformazione inversa in fase di decodifica, consideriamo il messaggio crittato `DRLQI – IUFOA – OG` e applichiamo d'inversa.

$\rightarrow$

1	2	3	4	5	6	7	8	9	10	11	12
4	5	10	1	6	11	2	7	12	3	8	9
D	R	L	Q	I	I	U	F	O	A	O	G
Q	**U**	**A**	**D**	**R**	**I**	**F**	**O**	**G**	**L**	**I**	**O**

Concludiamo questa lezione con alcune considerazioni sull'inversa:

- Per quanto abbiamo visto, se P è il periodo di T allora deve essere $T^{-1} = T^{P-1}$
- Visto che la lunghezza e il numero di cicli restano immutati passando da una trasformazione alla sua inversa, i due periodi devono coincidere, cioè $P_T = P_{T^{-1}}$

L'ultima osservazione mostra che trasformazione e inversa