Ora che abbiamo visto una serie di trasposizioni a rettangolo, con e senza chiave, cerchiamo di tirare le fila e valutare la bontà dei vari metodi. I vantaggi dei sistemi a chiave sono evidenti: essi mantengono (chi più chi meno) la riservatezza del messaggio anche nel caso in cui la segretezza del meccanismo dovesse venire meno. Va inoltre tenuto presente che modificare una chiave è più semplice che modificare un metodo, il che rende possibile un frequente aggiornamento delle chiavi.

Un buon sistema crittografico "a mano", come quelli che stiamo trattando, dovrebbe avere le seguenti caratteristiche:

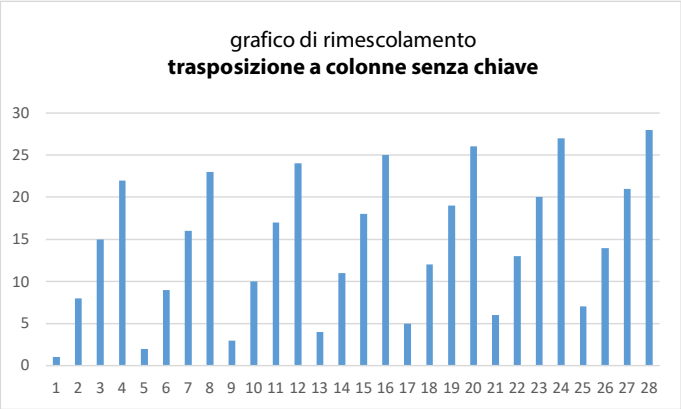
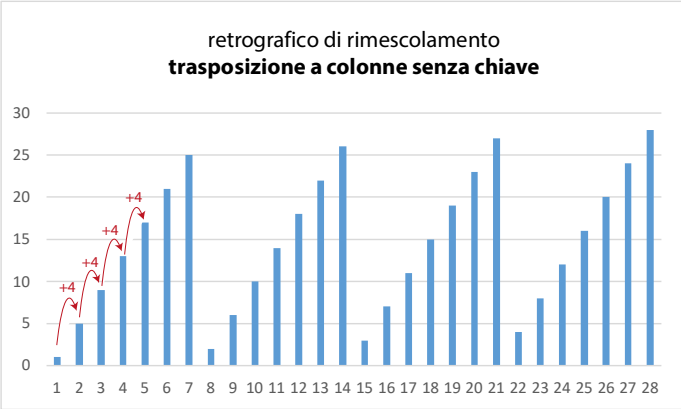
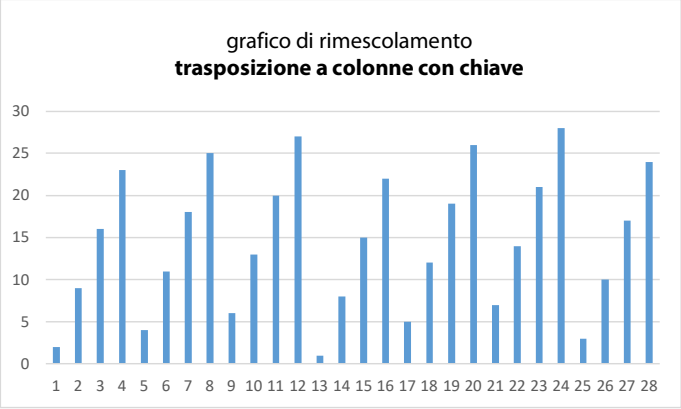
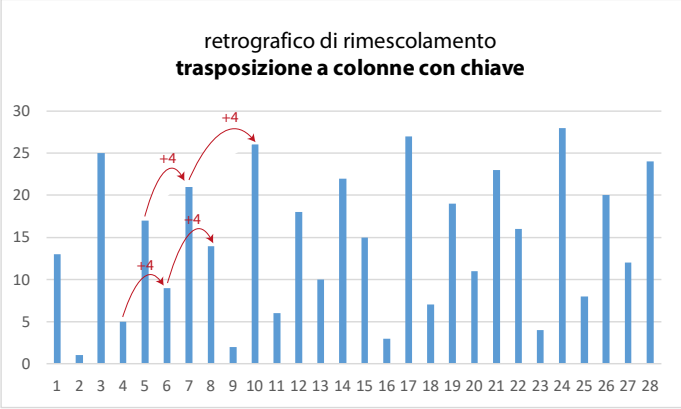
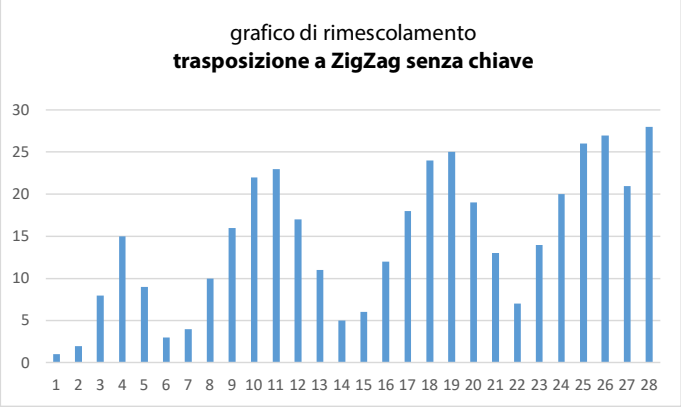
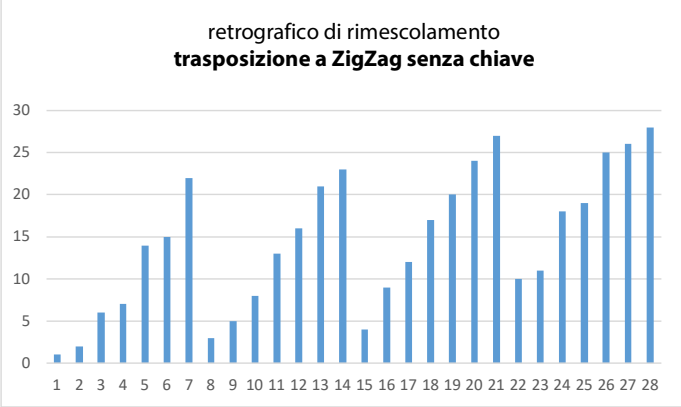
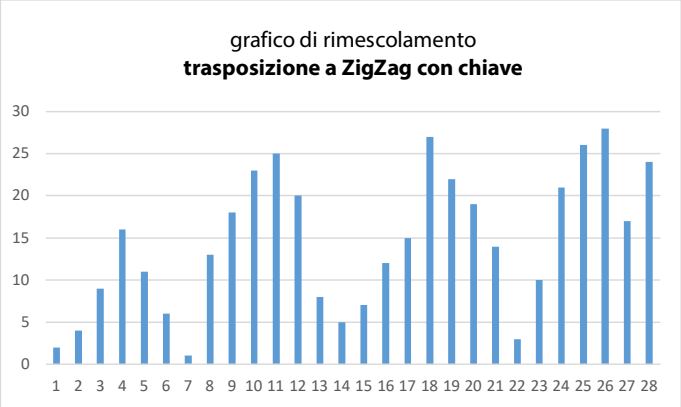
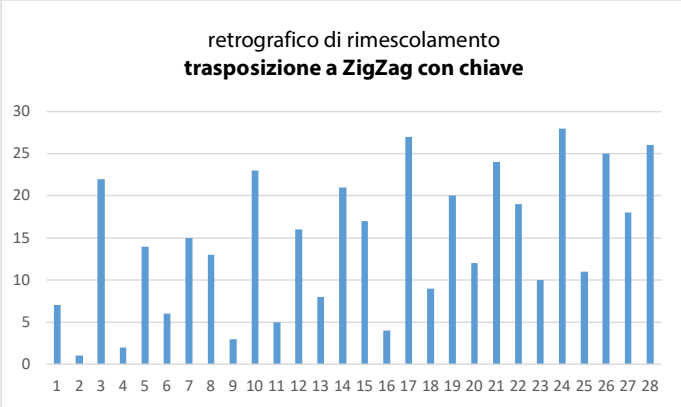
1. lentezza/impossibilità di decrittazione del messaggio da parte di un eventuale intercettatore
2. velocità in fase di cifratura
3. velocità in fase di decifratura (per il legittimo destinatario)
4. assenza di comunicazioni esterne al canale cifrato necessarie al suo funzionamento

Tutti i sistemi visti finora hanno mostrato buone prestazioni per quanto riguarda i punti 2 e 3. Per il punto 4 bisogna ricordare che, al di là del messaggio, è necessario che il destinatario sia a conoscenza del metodo usato per cifrare ed eventualmente della chiave (questo passaggio di informazioni avviene normalmente in ambiente protetto). Nel caso estremo dello scitale spartano si aggiunge la necessità di costruire e poi fornire a tutti i membri della rete di comunicazione copia dello stesso attrezzo.
Valutare il punto 1 non è affatto semplice, dal momento che non conosciamo a priori le informazioni di cui dispone il nostro intercettatore. Dando per scontato che egli conosca perlomeno il tipo di cifratura usata, nel nostro caso **per trasposizione**, dobbiamo valutare il grado di rimescolamento del nostro anagramma e il numero di indizi che si possono estrarre da esso.

Notiamo innanzitutto che tutti i rimescolamenti visti finora si basavano su una o al massimo due operazioni: immaginando un mazziere che mischi le carte soltanto una o due volte ci rendiamo conto che la casualità dell'anagramma risultante è soltanto apparente.

Per valutare a colpo d'occhio la bontà dei rimescolamenti si è proceduto così: invece di cifrare un testo si è considerata una sequenza di numeri crescenti da 1 a 28 disposti in una griglia 4×7. Nel caso di cifrature con chiave si è scelto la parola "`Catalan`" cui corrisponde la sequenza $4,1,7,2,5,3,6$.

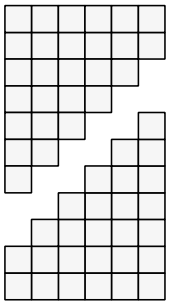
Qui in basso i messaggi cifrati come appaiono dopo la cifratura. Le prime colonne rappresentano i numeri $1,8,15,22$ perché questi sono i numeri che aprono il messaggio cifrato.	Qui in basso la *retrocifra* dei messaggi cifrati. Come si vede, le prime colonne rappresentano i numeri $1,5,9,13$: si tratta delle posizioni occupate dai primi quattro numeri del messaggio originario. Si tratta di

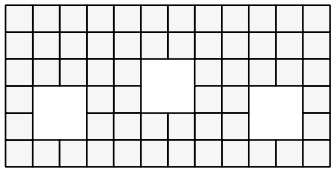
	un grafico più significativo del precedente, perché un eventuale intercettatore troverebbe le lettere delle parole “esca” proprio in questa forma.
	
	
	
	

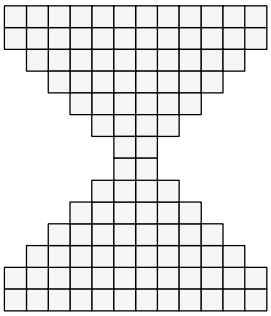
Come era lecito aspettarsi, la trasposizione a **ZigZag con chiave** presenta la situazione apparentemente meno regolare.

Fino ad ora abbiamo sempre considerato trasposizioni effettuate tramite un rettangolo: questa scelta facilita moltissimo il compito di un intercettatore che può stimare le dimensioni del rettangolo semplicemente contando le parole del testo: così un messaggio trasposto di 39 lettere è stato creato con un rettangolo 3×13 o 13×3, un messaggio di 49 lettere non sembra addirittura lasciare alcun dubbio (7×7).

In basso sono mostrate alcune figure che possono essere utilizzate a sostituzione del rettangolo. La principale caratteristica che devono possedere è la riproducibilità verso il basso (in modo da poter allungarsi via via che il messaggio cresce) secondo uno schema fisso e semplice.







La debolezza di questo sistema è la solita: bisogna comunicare la forma della griglia (o il destinatario deve essere a conoscenza della legge che la genera). Per ovviare al problema di comunicare questa informazione complessa e permettere anche un frequente aggiornamento della griglia stessa, sono stati ideati sistemi che variano la lunghezza delle colonne all'interno di un rettangolo classico tramite una chiave. In basso un esempio:

Cifratura per chiave scalare

Si tratta di un sistema di trasposizione a chiave che viene costruito mediante un rettangolo che in parte resta vuoto. L'esempio seguente chiarirà il meccanismo:

Trasposizione a cifratura scalare

Procedimento (cifratura)	Esempio

1) Di nuovo la chiave determina il numero di colonne. Scriviamo quindi nella prima riga `SALAME` (6 colonne) e calcoliamo la sequenza di *Sacco* associata.

S	A	L	A	M	E
6	1	4	2	5	3

2) Iniziamo a scrivere il nostro messaggio "Queste esempio mostra come usare una chiave scalare", cioè `QUESTOESEMPIOMOSTACOMEUNAUSAREUNACHIAVE-SCALARE` utilizzando la prima riga della tabella (messa in rilievo a fianco). Invece di iniziare dalla prima cella bisogna posizionarsi in corrispondenza della colonna contrassegnata dal numero 1 della chiave e partire da lì.

S	A	L	A	M	E
6	1	4	2	5	3

S	A	L	A	M	E
6	1	4	2	5	3
	Q	U	E	S	T

3) Arrivati in fondo alla riga continuiamo a scrivere il messaggio nella successiva, mettendoci in corrispondenza del "2" della chiave.

S	A	L	A	M	E
6	1	4	2	5	3
	Q	U	E	S	T
			O	E	S

4) Continuiamo in questo modo fino ad esaurire il messaggio o eventualmente la chiave. In quest'ultimo caso (che è quello descritto a fianco) basterà riprendere dalla colonna 1 e proseguire sempre allo stesso modo.

S	A	L	A	M	E
6	1	4	2	5	3
	Q	U	E	S	T
			O	E	S
					E
		M	P	I	O
				M	O
S	T	R	A	C	O

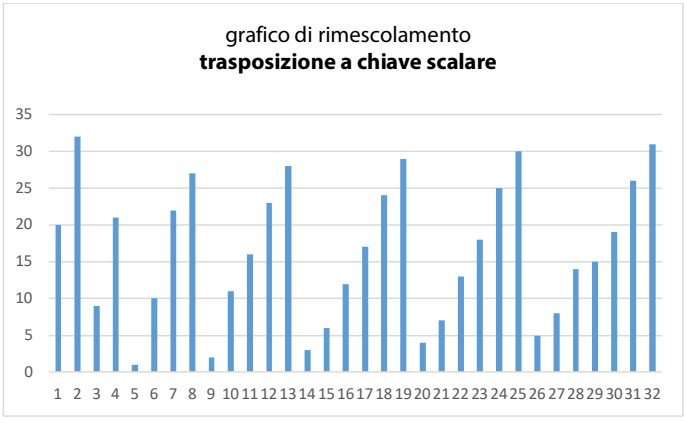
5) La cifratura vera e propria si effettua per colonne, da sinistra a destra (la chiave non svolge più alcun ruolo in questa fase). Otteniamo così

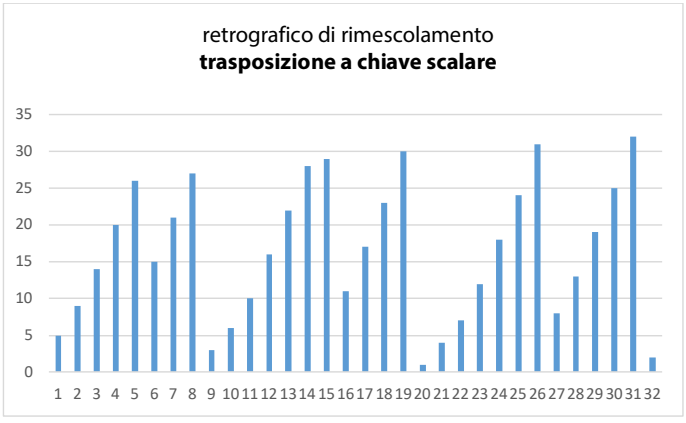
MESSAGGIO CIFRATO
(trasmesso in gruppi da 5)

```
SEQTM - SRUMR - EACEE -
OPAUR - CASEI - MCSEH -
ALTSE - OOOAU - NIVA
```

S	A	L	A	M	E
6	1	4	2	5	3
	Q	U	E	S	T
			O	E	S
					E
		M	P	I	O
				M	O
S	T	R	A	C	O
	M	E	U	S	A
			R	E	U
					N
		A	C	H	I
				A	V
E	S	C	A	L	A
	R	E			

Come si vede dai grafici di rimescolamento, il sistema della *chiave scalare* genera sequenze piuttosto regolari (il che non va bene) occasionalmente perturbate.





Vediamo in ogni caso come decrittare un messaggio codificato con questo sistema, supponendo naturalmente di avere a disposizione la chiave e il messaggio (e quindi anche la sua lunghezza).

4.1) Poniamo di ricevere il seguente messaggio con la chiave "TRIESTE" e codificato con una trasposizione a chiave scalare:

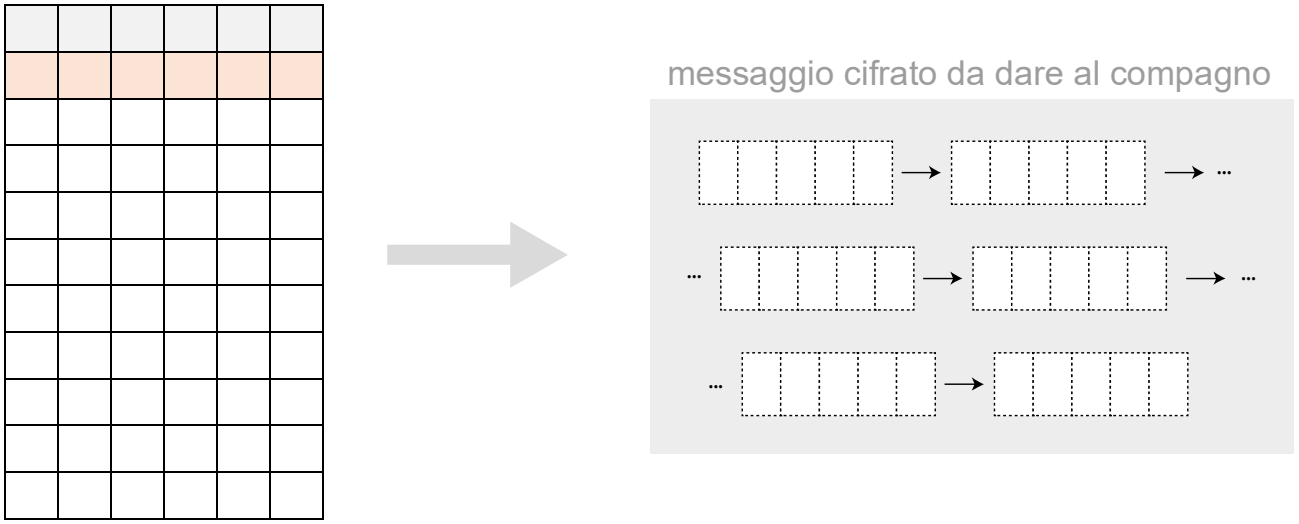
TATOS – OIRCI – OLOOO – LBTES – SSSLE – SNTOA - SU

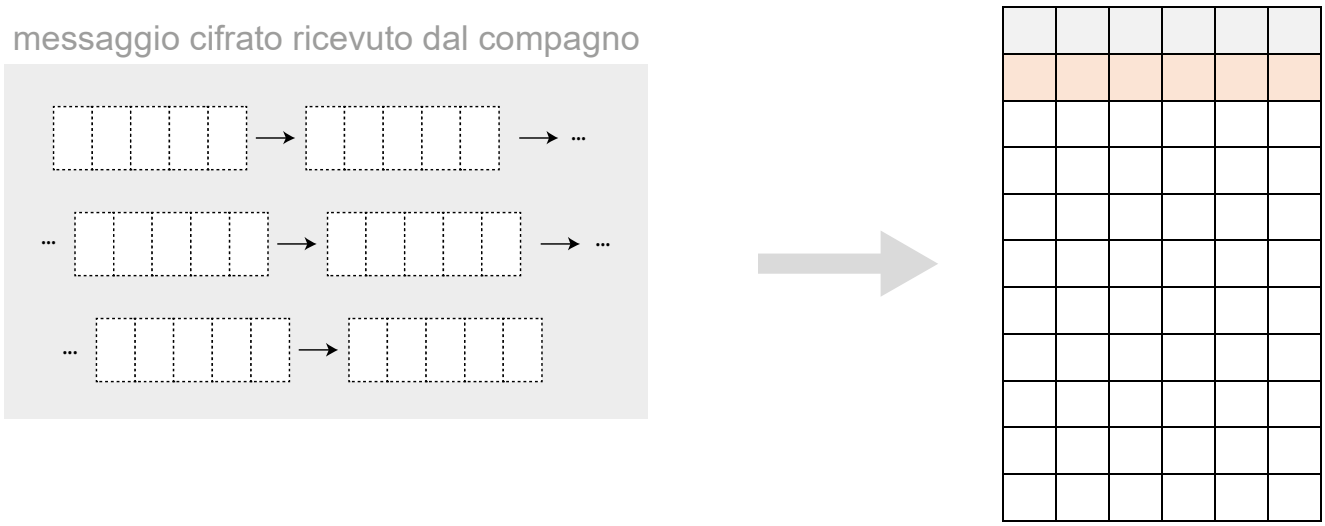
Possiamo presumere che la fase di decrittazione inizi predisponendo la seguente tabella:

T	R	I	E	S	T	E
6	4	3	1	5	7	2

La domanda è … dove va scritta la prima lettera (la T)? Riesci a trovare un metodo per portare in chiaro il messaggio (e in generale per portare in chiaro messaggi cifrati con la chiave scalare)?

4.2) Inventa un messaggio di 30 e cifralo con una *trasposizione a chiave scalare* con la chiave "TORINO". Passa poi il tuo messaggio cifrato ad un compagno e fatti dare il suo. Cercate quindi di riportare in chiaro ciascuno il messaggio dell'altro (in basso una serie di tabelle che potrebbero essere utilizzate allo scopo). *Nota bene: nelle tabelle riportate in basso, il numero di righe potrebbe essere eccessivo.*



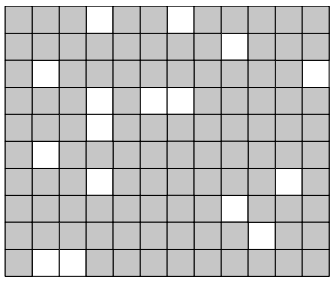


Le griglie bucate

Concludiamo questa sezione con due esempi di *griglie bucate*. La prima griglia bucata che mostrerò permette di realizzare uno steganogramma e quindi non rientra strettamente nel tema di questo foglio di lavoro.

Si tratta di una sagoma bucata che permette di nascondere messaggi dentro altri testi, come mostrato in basso. La bravura consiste nello scrivere frasi in un italiano sensato e che non destino allarme: le lettere importanti devono stare tutte al posto giusto, il che non è sempre facile da realizzare.

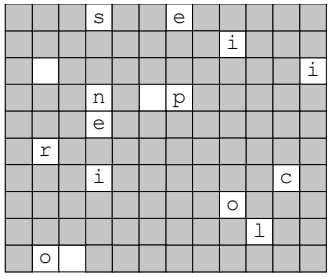
Sagoma fissa



Testo apparentemente innocente

l	a		s	e	r	e	n	i	t	à	
d	e	l	l	o		s	p	i	r	i	t
o		è		l	a		c	o	n	d	i
z	i	o	n	e		p	r	i	n	c	i
p	a	l	e		p	e	r		p	o	t
e	r		p	r	e	n	d	e	r	e	
d	e	c	i	s	i	o	n	i		c	h
e		a	b	b	i	a	n	o		u	n
	r	e	s	p	i	r	o		l	u	n
g	o		e		s	a	p	p	i	a	n

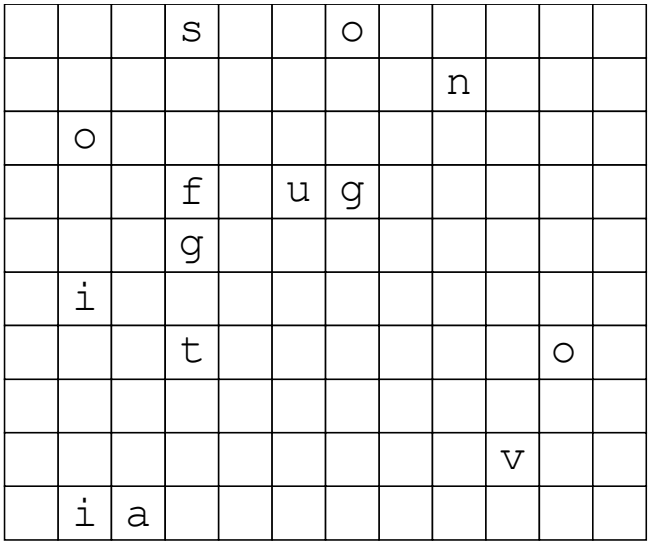
Messaggio nascosto



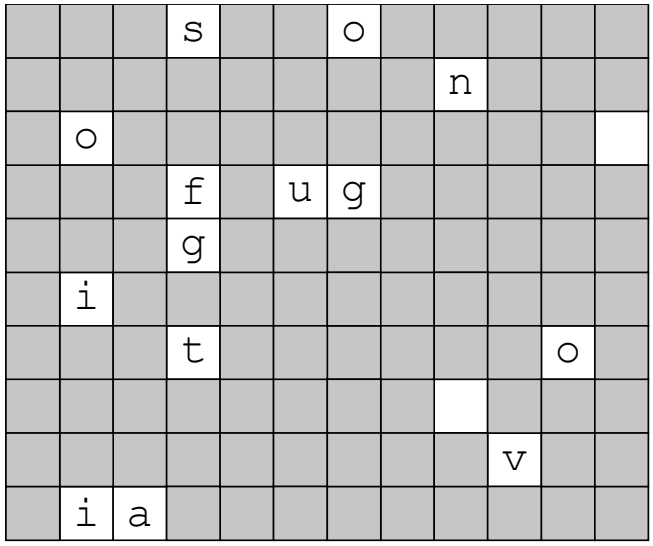
Per capire la difficoltà dell'operazione cimentati nel seguente compito:

4.3) Utilizzando la sagoma dell'esempio precedente, scrivi un testo "innocente" in un italiano scorrevole (una lettere per casella, spazi compresi) che contenga il messaggio di 16 lettere (di nuovo comprensivo di spazi) "SONO FUGGITO VIA" o "SONO FUGGITA VIA".

Testo apparentemente innocente



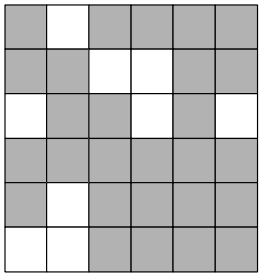
Messaggio nascosto



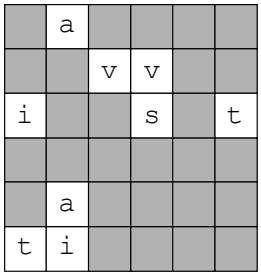
La griglia quadrata a rotazione

La prossima griglia quadrata bucata è detta **a rotazione** ed è propriamente un sistema di trasposizione.

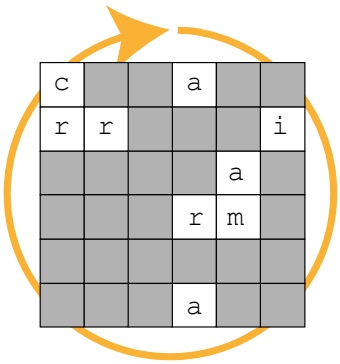
Uso della griglia a rotazione

Procedimento (cifratura)	Esempio
1) Lo strumento che si utilizza per questa trasposizione è una griglia quadrata $n \times n$ con $n^2/4$ buchi se n è pari e $(n^2-1)/4$ se n è dispari. I fori devono essere disposti in maniera ragionata (come vedremo fra breve). A fianco è mostrata una sagome quadrata di 36 quadratini e 9 fori.	

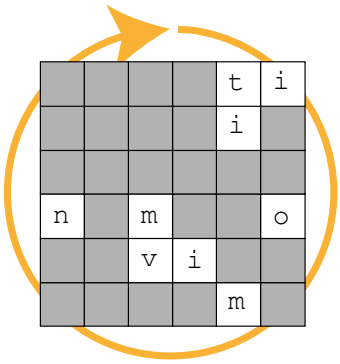
2) Dobbiamo ora scrivere un messaggio di lunghezza pari al numero di celle (nel nostro esempio 36).
Supponiamo che il testo reciti “AVVISTATI CARRI ARMATI IN MOVIMENTO DA SUD” che diventa
“AVVISTATICARRIARMATIINMOVIMENTODASUD”
Teniamo la sagoma su una griglia di carta delle stesse dimensioni e iniziamo a scrivere il testo

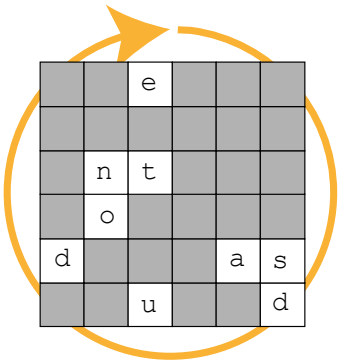


3) A questo punto ruotiamo la griglia di 90 gradi in senso orario. Se tutto è andato bene, i 9 fori sono posti in corrispondenza di celle vuote. Possiamo quindi continuare a scrivere.



4) Continuiamo come sopra fino a completare il messaggio:



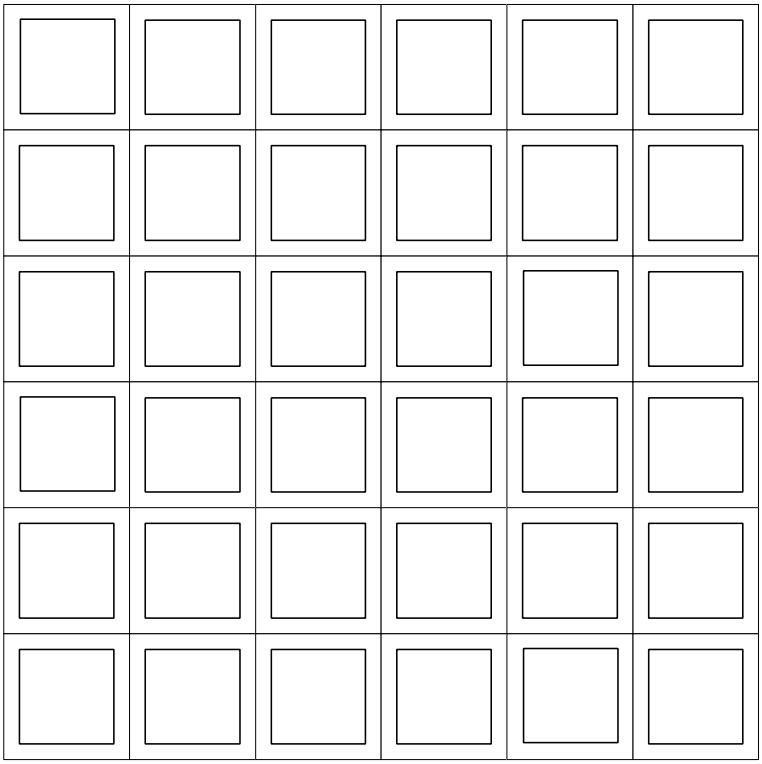


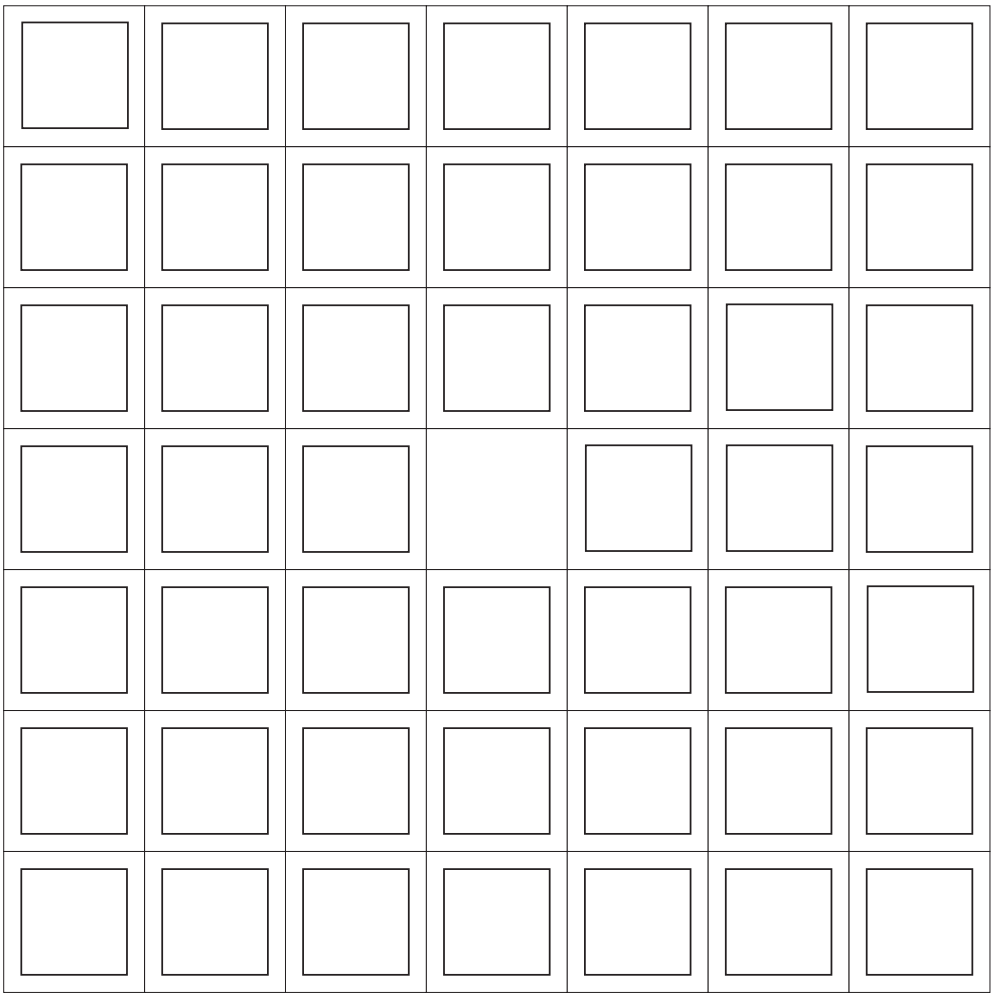
5) Alzando la sagoma abbiamo ora la trasposizione completa:

c	a	e	a	t	i
r	r	v	v	i	i
i	n	t	s	a	t
n	o	m	r	m	o
d	a	v	i	a	s
t	i	u	a	m	d

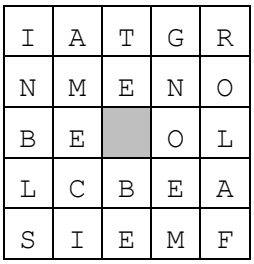
La decrittazione si realizza in modo semplicissimo: basterà appoggiare nuovamente la griglia sul foglio, leggere le lettere visibili e ruotare la sagoma fino a completamento del messaggio.

4.4) Cerca di costruire da solo una griglia quadrata a rotazione 6×6 (diversa da quella rappresentata sopra) e poi una griglia 7×7 indicando dove applicare i fori (si tratta di 9 buchi da fare nella prima griglia ($9 = 36/4$) e 12 nella seconda ($12 = (49 - 1)/2$)). Se vuoi costruire realmente la tua griglia di rotazione (conviene naturalmente farne due se lo scopo è quello di comunicare segretamente con qualcuno), puoi fotocopiare la prossima pagina e incollare il foglio su un cartone da ritagliare).





4.5) Passiamo brevemente dalla parte dei decrittatori, anche per renderci conto della difficoltà che si incontrano nel rompere un codice. Cerca quindi di riportare i seguenti messaggi in chiaro (si tratta in molti casi di problemi al limite dell'impossibile, nei quali anche gioca un ruolo importante anche la fortuna):

Testo (in gruppi da 5)	Metodo utilizzato	Parola presente nel testo in chiaro (e indicazioni)
VAIIZ – CVZAA – IFLNF – AAETD – Q	Trasposizione per colonna semplice	TAZZINA
ILGOI – FUTSO – CVIIG – VTAIT – IRNTA	Trasposizione a ZigZag semplice	FUGGITIVO
NSDPA – CZNEI – EIIEN – MTEAE – SALRT – COO	Trasposizione per colonna con chiave	ZAMPIRONE (chiave da 7 lettere)
EANRL – LYUAI – OOEEL – XLTRO – SEBAT – IOCPL	Trasposizione a ZigZag con chiave	XYLELLA (chiave da 6 lettere)
SEERN – MVOTE – ORRID – NINII – TOFIM – MAI	Trasposizione a chiave scalare	RIFORNIMENTI (chiave da 7 lettere)
	Trasposizione a griglia quadrata bucata	GOBBE