2.1) Usando lo scitale esagonale scrivi il testo “Il nemico attaccherà stanotte le postazioni del fronte settentrionale” (*vedi in basso*)…

ILNEMICOATTACCHERASTANOTTELEPOSTAZIONIDELFRONTESETTENTRIONALE

… e trascrivi il testo “srotolato” _____

_____

Il metodo appena presentato ha un grado di segretezza estremamente basso, come dimostra la facilità di decodifica nei seguenti due problemi:

2.3) Decodifica il seguente messaggio creato con uno scitale a sezione <u>ottagonale</u>:

L	**L**	**E**	**A**	**A**	**E**	**G**	**R**	**C**	**D**	**A**		**A**	**E**	**L**	
P	**L**	**E**		**I**	**S**	**D**		**T**	**E**	**A**		**A**	**N**	**K**	

Testo in chiaro: _____

_____

2.4) Decodifica il seguente messaggio creato con uno scitale sconosciuto:

Q	**O**	**P**	**S**	**A**	**L**	**D**	**T**	**U**	**E**	**I**	**T**	**D**
E	**E**	**O**	**E**	**S**	**O**	**R**	**E**	**Z**	**L**	**D**	**S**	**E**
M	**A**	**B**	**Z**	**M**	**O**	**T**	**M**	**O**	**L**	**O**	**A**	**E**

Testo in chiaro: _____

_____

_____

Quasi tutti i sistemi di cifratura prevedono una “chiave”, cioè un’informazione che determina la codifica di un messaggio e senza la quale il testo resta (quasi) inviolabile, anche se si è a conoscenza del metodo crittografico

adottato. Certe volte la chiave è una parola, altre un numero, più spesso è un'intera sequenza numerica. Vale in ogni caso la regola generale che una buona chiave debba essere possibilmente lunga e apparentemente casuale (in modo da non poterla ricostruire conoscendone dei frammenti). Tenere a mente un numero o una sequenza numerica lunga, specialmente se "disordinata" è piuttosto difficile, mentre con parole/frasi come "nonceduesenzatre" è molto meno problematico. È quindi opportuno inventare un metodo che consenta di trasformare parole/frasi arbitrariamente lunghe in sequenza numeriche. Qui presenterò il metodo esposto sul *Sacco*, che permette di creare un rimescolamento della successione $1, 2, 3, \dots n$.

Metodo di *Sasso* di trasformazione da **Chiave letterale** a **sequenza numerica**

Passaggi necessari per ricavare una chiave di n numeri da una frase di N lettere.

1) Prima di tutto procuriamoci un alfabeto di 26 lettere. Possiamo poi iniziare con l'algoritmo:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
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

Procedimento	Esempio
2) Scrivete la vostra frase, senza spazi, punteggiatura, interpunzioni o accenti su una riga. Se $n \leq N$ basterà scrivere le prime n lettere della frase, altrimenti sarà necessario concatenare copie della frase fino a disporre di n lettere.	Utilizziamo la frase "VIA COL VENTO" per generare una sequenza di 8 numeri. Visto che `viacolvento` ha ben 11 lettere, ci accontenteremo di `viacolve` V I A C O L V E _ _ _ _ _ _ _ _
3) Sotto le lettere scrivete il numero d'ordine che la lettera andrebbe ad occupare se tutte le lettere fossero riordinate in ordine alfabetico (nel caso in cui una lettera si ripeta, basterà iniziare a considerarle nell'ordine, da sinistra a destra)	L'alfabeto ordinato sotto gli occhi, iniziamo a determinare i numeri d'ordine delle lettere: V I A C O L V E _ _ 1 _ _ _ _ _ V I A C O L V E _ _ 1 2 _ _ _ _ …e così via fino a… V I A C O L V E _ 4 1 2 6 5 _ 3 Le due lettere uguali si gestiscono semplicemente enumerandole da sinistra a destra. V I A C O L V E 7 4 1 2 6 5 8 3
4) Nella riga in basso si è così venuta a creare la sequenza numerica desiderata.	7 4 1 2 6 5 8 3

Osservazione: se la sequenza da generare fosse stata più lunga della frase (caso generalmente da evitare, quando le circostanze lo consentono) si sarebbe dovuta creare la "parola" `viacolventoviac` a generare la sequenza 13,6,1,3,10,8,14,5,9,12,11,15,7,2,4:

V	I	A	C	O	L	V	E	N	T	O	V	I	A	C
13	6	1	3	10	8	14	5	9	12	11	15	7	2	4

L'esempio da solo dimostra perché parole troppo brevi funzionano male: osservando la sequenza $13,6,1,3,10,8,14,5,9,12,11,15,7,2,4$ si notano frequenti balzi di 11 posizioni dal numero al successore (*vedi figura a fianco*).

Guarda caso 11 è proprio la lunghezza della chiave letterale: si tratta di un'informazione che a un crittoanalista potrebbe tornare utile per penetrare nel codice.

2.5) Con il metodo di *Sasso* ricava una sequenza numerica di elementi dalla parola `CARCIOFO`.

2.6) Con il metodo di *Sasso* ricava una sequenza numerica di dodici elementi a partire dal tuo NOME+COGNOME.

La trasposizione semplice

Questo metodo è quasi identico alla scitale ma permette una maggiore flessibilità. Si tratta di predisporre una griglia formata da n colonne (il numero di righe sarà determinato dal testo stesso) dentro la quale andrà scritto il testo da decifrare, una lettera per volta e nell'ordine canonico: da sinistra a destra, dalla riga in alto a scendere, in modo da riempire tutto lo schema (in caso di necessità aggiungendo lettere senza significato). La codifica si otterrà leggendo la sequenza di lettere ottenuta scorrendo la griglia in un modo convenuto tra le parti.

Esempio

Predisponiamo una griglia composta da 7 lettere e scriviamo il testo "`Alla fiera dell'est, per due soldi, un topolino mio padre comprò`". Se alcune celle dell'ultima riga dovessero risultare scoperte, dovranno essere riempite con lettere a caso o con parole che non modifichino il senso del testo (nell'esempio a fianco si è aggiunto BZGBP

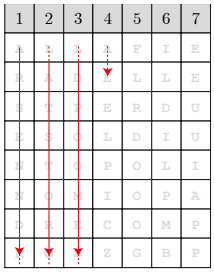
1	2	3	4	5	6	7
A	L	L	A	F	I	E
R	A	D	E	L	L	E
S	T	P	E	R	D	U
E	S	O	L	D	I	U
N	T	O	P	O	L	I
N	O	M	I	O	P	A
D	R	E	C	O	M	P
R	O	B	Z	G	B	P

A questo punto disponiamo di un "tappeto" di lettere che possono essere riarrangiate in svariati modi.

Vediamo tre scelte semplici:

Riarrangiamento *per colonne*

Si leggono le lettere scorrendo le colonne da sinistra a destra e le lettere dall'alto in basso (l'effetto è quello dello scitale)

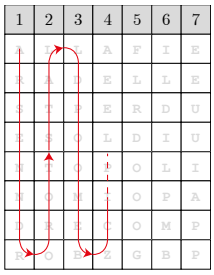


MESSAGGIO CIFRATO
(trasmesso in gruppi da 5)

```
ARSEN - NDRLA - TSTOR
OLDPO - OMEBA - EELPI
CZFLR - DOOOG - ILDIL
PMBEE - UUIAP - P----
```

Riarrangiamento *a serpentina*

Si leggono le lettere scorrendo le colonne da sinistra a destra e le lettere delle colonne prima dall'alto in basso, poi dal basso in alto e così via, in modo alternato.

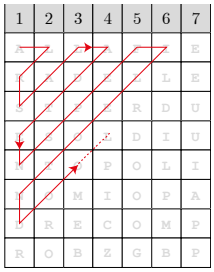


MESSAGGIO CIFRATO
(trasmesso in gruppi da 5)

```
ARSEN - NDROR - OTSTA
LLDPO - OMEBZ - CIPLE
EAFLR - DOOOG - BMPLI
DLIEE - UUIAP - P----
```

Riarrangiamento *a zig zag*

Si leggono le lettere scorrendo le celle come mostrato a fianco.

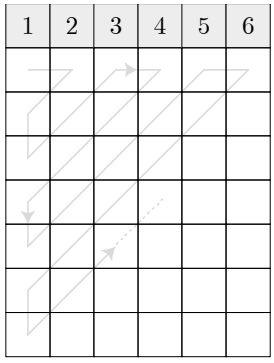


MESSAGGIO CIFRATO
(trasmesso in gruppi da 5)

```
ALRSA - LADTE - NSPEF
ILEOT - NDOOL - RLEED
DPMRR - OEIOI - UULOC
BZOPI - AMGBP - P----
```

Il lavoro di decodifica segue un procedimento speculare: una volta predisposta la griglia, si inseriranno le lettere del codice secondo l'ordine prestabilito (per colonne, a serpentino, a zigzag, e così via). Una volta fatto questo, il messaggio in chiaro apparirà sulle righe:

2.6) Il messaggio cifrato in basso è stato ottenuto con una griglia composta da 6 colonne percorsa “a zig zag” *(vedi a fianco*). Ricostruisci il messaggio in chiaro.



MESSAGGIO CIFRATO
(trasmesso in gruppi da 5)

```
ASCTE – PITRL – MLOON
ASVIA – TGITC – AIIEE
CLIOM – OAMOR – IE---
```

2.7) Codifica il messaggio “`Attenzione: domani verifica di Matematica`” per trasposizione semplice con una griglia a 9 colonne percorsa *per colonne*.

MESSAGGIO CIFRATO
(trasmesso in gruppi da 5)