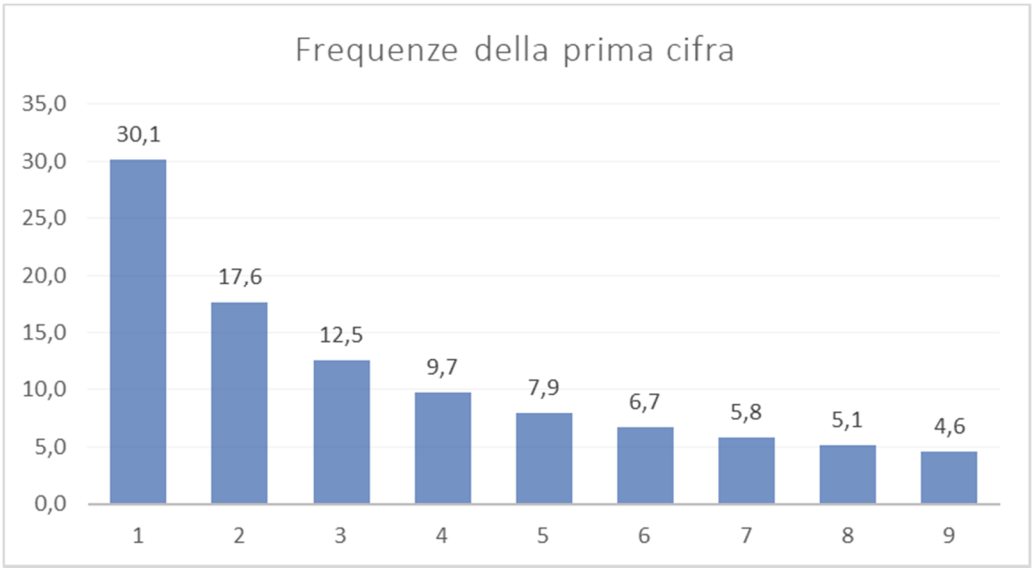
Riepiloghiamo l'ultimo esercizio del foglio di lavoro **7)**

1) Considera una qualche grandezza fisica o una matematica che misuri una quantità reale e che sia distribuita su diversi ordini di grandezza.
2) Dei dati a disposizione prendi nota soltanto della prima cifra, compilando la tabella in basso.

Prima cifra	Occorrenze	Percentuale %
1		
2		
3		
4		
5		
6		
7		
8		
9		

Iniziamo questa lezione con la risposta all'ultimo esercizio. Se avete scelto con oculatezza la grandezza da prendere in esame e il numero esiguo di dati non ha causato troppi guai, dovreste avere ottenuto una distribuzione di frequenze del genere:



8.1) Come spieghi il grafico sovrastante?

Il fenomeno della prima cifra è detto **legge di Benford** e prende il nome dal fisico Frank Benford, che nel 1938 pubblicò un articolo su questo argomento dal suggestivo titolo "*The Law of Anomalous Numbers*". Il primo lavoro pubblicato a riguardo è in verità antecedente (1881) ed è del matematico Simon Newcomb. In termini di *Storia della Matematica*, si tratta in ogni caso di una scoperta recente.

Torniamo ora al nostro filone principale, la crittografia per sostituzione monoalfabetica: abbiamo visto che essa ha delle fragilità tali da mettere in dubbio la sua applicabilità: dall'analisi di doppie, coppie, triple, di lettere amiche e nemiche e in generale di rapporti fra lettere vicine, ci si può difendere con una trasposizione in sovracifratura, cioè fatta in aggiunta alla sostituzione. Resta però la vulnerabilità rispetto all'analisi delle frequenze, dalla quale nessuna trasposizione mette al riparo.

Il primo stratagemma usato per rendere un messaggio inviolabile dall'analisi delle frequenze si basa su una tavola possibilmente ampia contenente simboli ripetuti. Per capire il senso di questa scelta consideriamo ancora una volta le frequenze letterali dei *Promessi Sposi*:

Frequenze letterali ne *I PROMESSI SPOSI*

A	11,51	G	1,71	L	5,56	Q	0,77	V	2,3
B	0,97	H	1,34	M	2,36	R	6,59	W	0,0
C	4,69	I	9,53	N	7,29	S	5,46	X	0,0
D	3,72	J	0,0	O	9,64	T	6,8	Y	0,0
E	12,4	K	0,0	P	2,96	U	3,56	Z	0,75
F	1,5								

La tabella sovrastante ci dice che in media, ogni 100 lettere, 11 o 12 saranno della A, una sarà una B e così via. Supponiamo ora di disporre non di una A ma di 11: A_1, A_2, … A_{11}. Usando prima l'una e poi l'altra per crittare un messaggio, avremo che, in media, ciascuna di esse avrà la stessa frequenza della B: l'analisi delle frequenze risulterà in questo modo inapplicabile. Consideriamo a questo proposito la seguente tavola:

Tavola 10x10 con *omofoni*

	0	1	2	3	4	5	6	7	8	9
0	A	A	A	A	A	A	A	A	A	A
1	A	B	C	C	C	C	D	D	D	E
2	E	E	E	E	E	E	E	E	E	E
3	E	F	G	H	I	I	I	I	I	I
4	I	I	I	J	K	L	L	L	L	L
5	M	M	N	N	N	N	N	N	N	O
6	O	O	O	O	O	O	O	O	P	P
7	P	Q	R	R	R	R	R	R	S	S
8	S	S	S	T	T	T	T	T	T	T
9	U	U	U	V	V	W	X	Y	Z	Z

La tavola è costituita da 100 simboli, ciascuno dei quali è ripetuto approssimativamente tante volte quanto è la sua percentuale (le lettere sotto l'uno per cento hanno naturalmente tutte un rappresentante).

Usando ora una tecnica traspositoria qualsiasi, possiamo rimescolare la tavola ed ottenerne una nuova. Le ripetizioni e l'ordine alfabetico delle lettere suggeriscono di iterare il procedimento più volte, al fine di ottenere un risultato possibilmente irregolare. Vediamo in basso a destra la tavola ottenuta mediante la trasposizione scalare iterata 5 volte con la chiave "MAJORANA":

Tavola di partenza (con omofone)

	0	1	2	3	4	5	6	7	8	9
0	A	A	A	A	A	A	A	A	A	A
1	A	B	C	C	C	C	D	D	D	E
2	E	E	E	E	E	E	E	E	E	E
3	E	F	G	H	I	I	I	I	I	I
4	I	I	I	J	K	L	L	L	L	L
5	M	M	N	N	N	N	N	N	N	O
6	O	O	O	O	O	O	O	O	P	P
7	P	Q	R	R	R	R	R	R	S	S
8	S	S	S	T	T	T	T	T	T	T
9	U	U	U	V	V	W	X	Y	Z	Z

→

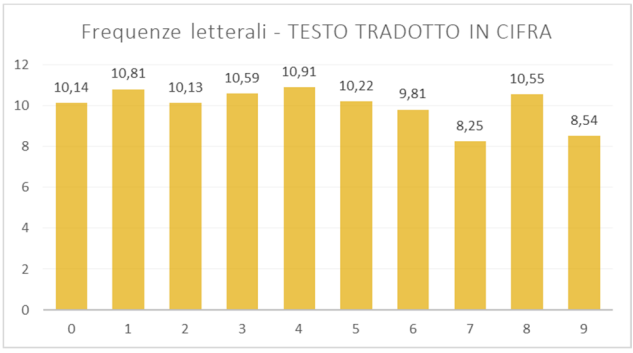
Tavola crittata

	0	1	2	3	4	5	6	7	8	9
0	L	E	S	E	N	T	I	R	O	G
1	N	T	V	X	D	L	A	H	V	I
2	E	L	A	O	N	O	E	E	R	E
3	O	Z	C	A	F	J	L	Q	D	A
4	N	M	T	N	C	S	A	S	K	C
5	T	A	N	E	L	T	O	O	P	R
6	U	T	U	E	U	T	P	O	D	I
7	Y	I	R	E	C	R	E	I	A	I
8	I	S	A	B	Z	M	I	W	E	A
9	A	E	P	I	O	R	A	O	S	N

Usando la tavola crittata per cifrare l'estratto dal "pendolo di Foucault" di Umberto Eco otteniamo….

TESTO IN CHIARO	CIFRA
FUALLORACHEVIDIILPENDOLOLASF	34629036159728904417531206688606215826243897
ERAMOBILEALLESTREMITADIUNLUN	00575422813453071641258379005333000029455595
GOFILOFISSATOALLAVOLTADELCOR	76850655161406624336645209973486153034794581
ODESCRIVEVALESUEAMPIEOSCILLA	46612596360046189436503338010032257230682947
ZIONICONISOCRONAMAESTASAPEVO	49288012881289542745645333416677299445497954
MACHIUNQUEAVREBBEDOVUTOAVVER	54398493670486495724774597740708523941390381
TIRENELLINCANTODIQUELPLACIDO	05464582662618574122491779624037602690127220
RESPIROCHEILPERIODOERAREGOLA	83832914561264112339121827595086282924291536
TODALRAPPORTOTRALARADICEQUAD	79994951240597688637629154923678326968942801
RATADELLALUNGHEZZADELFILOEQU	98587172943217917715582007199738230372467527
ELNUMERONCHEIRRAZIONALEALLEM	09300016652538221559336692577511946172461582
ENTISUBLUNARIPERDIVINARAGION	95826877745337648968592242963853005478216404
ELEGANECESSARIAMENTELACIRCON	09172684319014202134060057913764013610624163
…	…

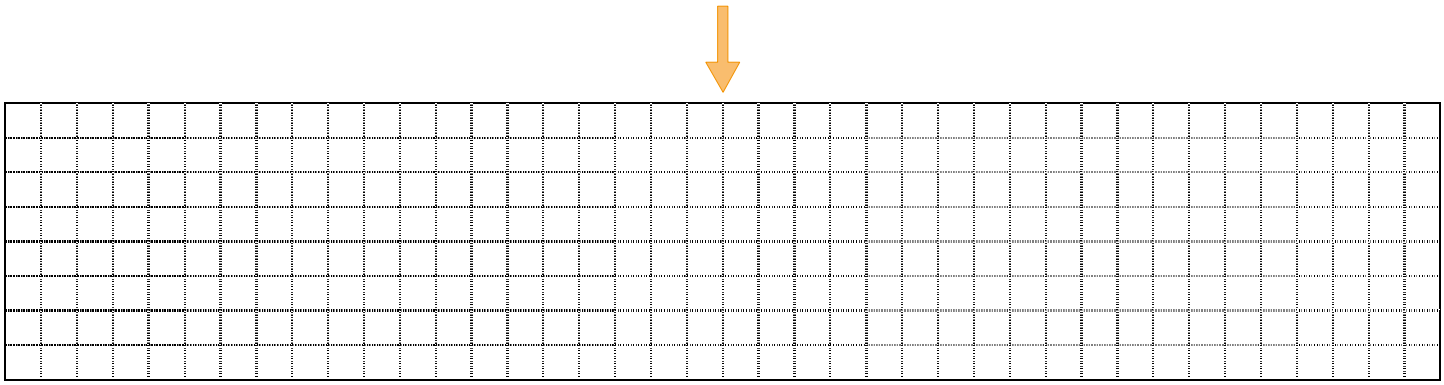
L'analisi delle frequenze delle cifre (da 0 a 9) fornisce il grafico accanto. Come si vede l'idea della tavola ha funzionato abbastanza bene:



Una tavola con più occorrenze di una specifica lettera si dice "tavole con omofoni" (da "omofono" → "stesso suono"). L'uso di una tavola con omofoni permette di tradurre la stesso messaggio in innumerevoli modi diversi e costituisce per il cifratore un lavoro difficile: la cifratura di ogni lettera deve infatti essere scelta in modo da evitare di incorrere in scelte ripetitive e prevedibili come l'usare sempre la stessa cifra per un simbolo o anche usare sempre cifre diverse, magari a rotazione. Questo elemento rende il crittatore parte del meccanismo di cifratura e costituisce in molti casi il punto debole del metodo stesso: prima o poi si ingenerano automatismi che possono essere riconosciuti in fase di analisi e i cifratori meno accorti potrebbero addirittura finire per lasciare una sorta di "firma" personale sulla cifra stessa.

8.2) Utilizzando la tavola 10×10 "con omofoni" presentata prima, cifra il messaggio "Tanto va la gatta al largo che ci lascia lo zampino", cioè …

TANTOVALAGATTAALLARGOCHECILASCIALOZAMPINO



Un altro stratagemma per rendere inoffensiva l'analisi della frequenze (e comunemente usato in combinazione con gli omofoni) è rappresentato dai *metasimboli*, coppie di cifre che non vanno tradotte ma lette come istruzioni. Per capire al meglio uso ed efficacia del metodo, consideriamo una Tavola 10×10 con omofoni (leggermente modificata rispetto alla precedente con tre omofoni in meno) e tre metasimboli: # (*nulla*), | (*sospensione*) e ! (*istruzione*) dal seguente significato:

Metasimbolo	Effetto
! (*istruzione*)	Se posto al di fuori di una sospensione (*vedi sotto*), va usato a coppie, come fossero delle parentesi. I caratteri posti tra due simboli di istruzione costituiscono una frase di senso compiuto che informa il decodificatore su un cambiamento di regole di decifratura
| (*sospensione*)	Se posto al di fuori di un'istruzione, va usato anch'esso a coppie. Tutti i simboli compresi fra due simboli di sospensione successivi non vanno letti
# (*nulla*)	Se posto al di fuori di un'istruzione o di una sospensione, non c'è alcun effetto, il simbolo semplicemente non viene letto.

Fase 1: preparazione del messaggio

```
TANTOVALAGATTAALLARGOCHECILASCIALOZAMPINO
```

↓

```
TANTOVALAGATTAAL#LARGOC#HECILASCIALOZAMP##INO
```

↓

```
TANT|Z#|OVAL||AGATTAAL#LARGOC#HECI|XWX|LASCIALOZAMP##INO|JYZJ|
```

↓

```
TANT|Z#|OVAL||AGAT!non leggere i prossimi quattro
simboli!XKWQTAAL#LARGOC#HECI|XWX|LASCIALOZAMP##INO|JYZJ|
```

Fase 2: Codifica della tavola dei simboli (chiave scalare OMBRELLO iterata 3 volte) e cifratura del messaggio:

Tavola di partenza (con omofone e metasimboli)

	0	1	2	3	4	5	6	7	8	9
0	A	A	A	A	A	A	A	A	A	A
1	A	B	C	C	C	C	D	D	D	E
2	E	E	E	E	E	E	E	E	E	E
3	E	F	G	H	I	I	I	I	I	I
4	I	I	I	J	K	L	L	L	L	L
5	M	M	N	N	N	N	N	N	N	O
6	O	O	O	O	O	O	O	O	P	P
7	P	Q	R	R	R	R	R	R	S	S
8	S	S	S	T	T	T	T	T	T	U
9	U	U	V	W	X	Y	Z	#	|	!

→

Tavola crittata

	0	1	2	3	4	5	6	7	8	9
0	O	N	N	O	O	E	W	U	T	I
1	L	A	P	R	E	E	A	C	U	S
2	I	A	B	C	Y	S	L	H	E	Q
3	!	N	P	R	K	T	L	E	A	T
4	O	J	I	R	I	T	Z	L	E	R
5	C	D	S	N	E	A	M	O	S	O
6	N	R	O	N	O	T	P	V	T	U
7	R	A	E	I	E	A	F	A	E	L
8	E	N	A	D	X	O	|	M	D	G
9	A	C	#	I	S	E	I	A	I	I

```
TANT|Z#|OVAL||AGAT!NONLEGGEREIPROSSIMIQUATTROSIMBOLI!XKWQTAAL#LAR
GOC#HECI|XWX|LASCIALOZAMP##INO|JYZJ|
```

```
68758145864692864067213686867189820830010381260589891470140912135
99494448798296938350813645220562259109830843406293577117992362170
89622392277417988684068486471694234282790346165612929273815986412
4464186
```

Fase 3: Valutazione a posteriori e "aggiustamento" finale

Per i nostri scopi è più utile rappresentare il codice in coppie di cifre:

```
68 75 81 45 86 46 92 86 40 67 21
36 86 86 71 89 82 08 30 01 03 81
26 05 89 89 14 70 14 09 12 13 59
94 94 44 87 98 29 69 38 35 08 13
64 52 20 56 22 59 10 98 30 84 34
06 29 35 77 11 79 92 36 21 70 89
62 23 92 27 74 17 98 86 84 06 84
86 47 16 94 23 42 82 79 03 46 16
56 12 92 92 73 81 59 86 41 24 46
41 86
```

CIFRA	OCCORRENZE	PERCENTUALE %
0	16	7,92
1	21	10,39
2	24	11,88
3	15	7,42
4	23	11,38
5	11	5,44
6	25	12,37
7	15	7,42
8	28	13,86
9	24	11,88

L'analisi delle occorrenze (riportate in valore assoluto prima delle percentuali) fornisce i valori mostrati in tabella. Possiamo equilibrare le frequenze inserendo nella cifra alcuni simboli interni ad una sospensione (codice `86`) e possiamo rompere alcune doppie con delle nulle (codice `92`):

```
68 75 81 45 86 46 92 86 40 67 21 36 86 86 71 89 82 08 30 01 03 81
26 05 89 92 89 14 70 86 55 75 38 07 57 53 37 75 86 14 09 12 13 59
94 94 44 87 98 29 69 38 35 08 13 64 52 20 56 22 59 10 98 30 84 34
06 29 35 77 11 79 92 36 21 70 89 62 23 92 27 74 17 98 86 84 06 84
86 47 16 94 23 42 82 79 03 46 16 56 12 92 92 73 81 59 86 41 24 46
41 86
```

Gli effetti dei *metasimboli* sono molto intriganti perché aprono la strada alla "crittografia perfetta". Supponiamo ad esempio di avere la seguente combinazione:

SIMBOLO1 `vai a destra` *SIMBOLO1* *SIMBOLO2* `vai a sinistra` *SIMBOLO2*

Supponiamo che un supercomputer abbia provato tutte le possibili chiavi associate a tutti le possibili cifrature, fino ad arrivare al risultato contenuto nel riquadro in alto: è plausibile che i due simboli ancora da interpretare siano dei *metasimboli*: non restano quindi che due possibilità.

Opzione A: $\begin{cases} SIMBOLO1 \rightarrow nulla \\ SIMBOLO2 \rightarrow sospensione \end{cases} \Rightarrow$ Il messaggio dice "`Vai a destra`"

Opzione B: $\begin{cases} SIMBOLO1 \rightarrow sospensione \\ SIMBOLO2 \rightarrow nulla \end{cases} \Rightarrow$ Il messaggio dice "`Vai a sinistra`"

Il fatto di "andare a sinistra" o "andare a destra" può essere il messaggio in sé o può essere collegato ad un'istruzione (introdotta altrove da un *metasimbolo*) e che, a seconda dei casi, cambia il senso o il contenuto dell'intero messaggio.

Questo piccolo gioco è incredibilmente importante: **dal momento che chiavi diverse possono creare messaggi perfettamente coerenti ma di contenuto diverso**, abbiamo dimostrato che attraverso i *metasimboli* si possono creare cifrature effettivamente **non decrittabili in assenza della chiave**. Ritorneremo su questo punto fra breve.

Concludiamo la parentesi sui *metasimboli* con i seguenti:

Metasimbolo	Effetto
$\boxed{<}$ (*cambio chiave*)	Da usare a coppie (come fossero delle parentesi). I caratteri posti tra due simboli di istruzione costituiscono la nuova chiave con la quale creare una nuova tavola dei simboli. Questa verrà usata per decrittare il resto del messaggio (a partire dalla chiusura delle parentesi virtuali).
$\boxed{+}$ (*itera chiave*)	Appena si incontra il simbolo di iterazione, la tavola dei simboli viene cifrata un'altra volta con la chiave originaria.

Vediamo un esempio e consideriamo il messaggio: "Di iterazione in iterazione" cioè "`DIITERAZIONEINITERAZIONE`" e aggiungiamo i *metasimboli* "`DII+TERAZIONEI+NITERAZIONE`". Le prime tre lettere "`DII`" e il simbolo stesso di iterazione "`+`" verranno crittati con una certa tavola cifrata, le seguenti "`TERAZIONEI+`" con la tavola "ricifrata" e gli ultimi "`NITERAZIONE`" con la tavola cifrata un'ultima volta.

Predisponiamo una serie di tavole: la $tavola\ 1$ è stata creata per cifratura sulla tavola base ($tavola\ 0$) iterando la chiave scalare "`AEROPLANO`" per 3 volte, le restanti tavole semplicemente iterando il procedimento (quindi applicando la chiave scalare prima 6 volte e poi 9)

Tavola di partenza con omofoni e metasimboli ($TAVOLA\ 0$)

	0	1	2	3	4	5	6	7	8	9
0	A	A	A	A	A	A	A	A	A	A
1	A	B	C	C	C	C	D	D	D	E
2	E	E	E	E	E	E	E	E	E	E
3	E	F	G	H	I	I	I	I	I	I
4	I	I	I	J	K	L	L	L	L	L
5	M	N	N	N	N	N	N	O	O	O
6	O	O	O	O	O	O	P	P	P	Q
7	R	R	R	R	R	R	S	S	S	S
8	S	T	T	T	T	T	T	U	U	U
9	V	W	X	Y	Z	#	|	!	<	+

Tavola crittata 1 volta ($TAVOLA\ 1$)

	0	1	2	3	4	5	6	7	8	9
0	A	U	I	S	P	F	|	N	N	E
1	I	S	D	L	A	L	O	H	Z	O
2	O	O	Y	E	O	A	T	E	M	C
3	!	E	A	C	I	T	X	R	I	R
4	D	E	G	I	N	I	R	Q	O	T
5	E	J	A	L	U	R	O	S	I	+
6	T	S	R	U	N	E	I	E	C	S
7	C	A	L	E	<	T	O	E	A	E
8	B	V	#	A	P	A	N	T	O	N
9	A	I	W	A	D	E	P	L	R	K

Tavola crittata 2 volte ($TAVOLA\ 2$)

	0	1	2	3	4	5	6	7	8	9
0	A	O	T	E	I	E	P	U	L	O
1	D	O	Z	O	N	I	N	C	D	S
2	U	E	A	O	I	U	A	A	E	L
3	L	C	N	L	X	N	W	<	E	C
4	H	T	A	I	J	R	L	S	R	A
5	E	I	E	R	T	A	S	E	R	K
6	#	A	T	N	O	M	I	E	D	B
7	A	I	T	O	R	P	T	Y	I	O
8	S	A	E	|	C	S	A	V	+	R
9	F	G	I	P	O	!	E	Q	E	N

Tavola crittata 3 volte ($TAVOLA\ 3$)

	0	1	2	3	4	5	6	7	8	9
0	A	+	N	O	I	C	E	T	R	S
1	H	T	D	R	U	R	O	L	O	E
2	N	M	P	I	R	O	S	U	E	O
3	Q	L	L	I	W	A	I	R	T	A
4	C	A	N	E	I	<	T	B	T	|
5	A	I	O	L	V	I	A	Y	C	N
6	E	I	P	R	S	E	X	O	Z	S
7	N	D	A	E	E	C	#	A	T	U
8	O	F	!	P	D	E	E	A	K	A
9	E	A	G	I	N	L	E	S	O	J

Otteniamo così…

DII+	$TAVOLA\ 1$ →	12 66 91 95
TERAZIONEI+	$TAVOLA\ 2$ →	76 28 53 70 12 66 64 16 98 51 88
NITERAZIONE	$TAVOLA\ 3$ →	59 33 48 73 63 00 68 23 52 42 85

…e quindi, riassumendo…

DIITERAZIONEINITERAZIONE

↓

DII+TERAZIONEI+NITERAZIONE

↓

12 66 91 95 76 28 53 70 12 66 64 16 98 51 88 59 33 48 73 63 00 68 23 52 42 85

Prima di utilizzare questa tecnica bisognerebbe naturalmente accertarsi del periodo della trasposizione usata per cifrare la tavola. Nel caso specifico abbiamo un trasposizione che concatena 4 cicli rispettivamente di $1, 34, 55, 10$ elementi. Il periodo della trasposizione è quindi $mcm(1{,}34{,}55{,}10) = 3740$, al riparo da accidentali "rimesse in ordine" per iterazioni ripetute.

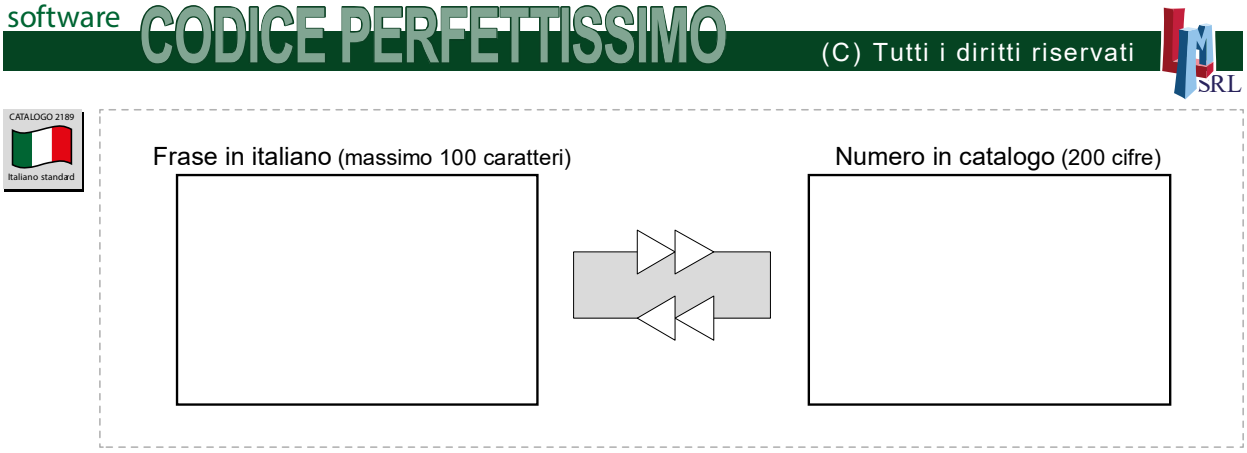
La tecnica appena vista è estremamente potente dal momento che la continua sostituzione di tavole rende l'analisi delle frequenze inefficace, perlomeno se effettuata sul messaggio intero. Vedremo nella prossima lezione una tecnica incentrata interamente sul continuo e automatico slittamento della tavola, senza necessità di frapporre *metasimboli* tra i caratteri del messaggio originale.

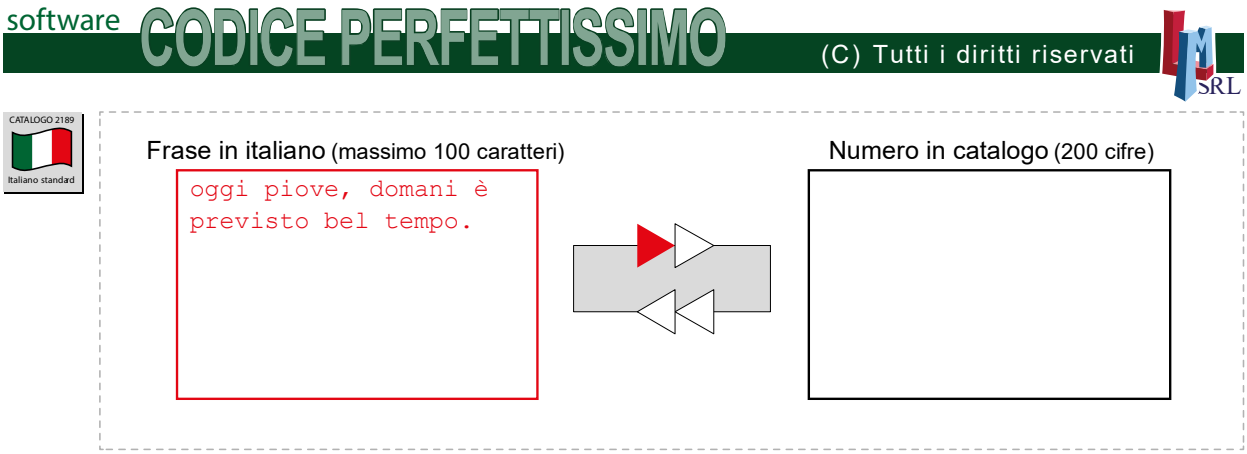
Ritorniamo per un attimo al *codice perfetto* introdotto in precedenza. Esso funziona per un motivo molto semplice: due decodifiche differenti portano a due messaggi in chiaro dal significato diverso ma entrambi plausibili. Questo rende la decifrazione senza chiave vana, dal momento che è impossibile optare per un contenuto rispetto all'altro. La natura "binaria" (due messaggi tra i quali scegliere) di questo sistema non è che l'antipasto per la cifratura *perfettissima*: una codifica che trasformi ogni possibile decodifica in un messaggio plausibile (perlomeno in un messaggio scritto correttamente in italiano). Per giungere a tanto bisogna introdurre un concetto tipico della crittografia moderna, la cosiddetta **chiave pubblica**.

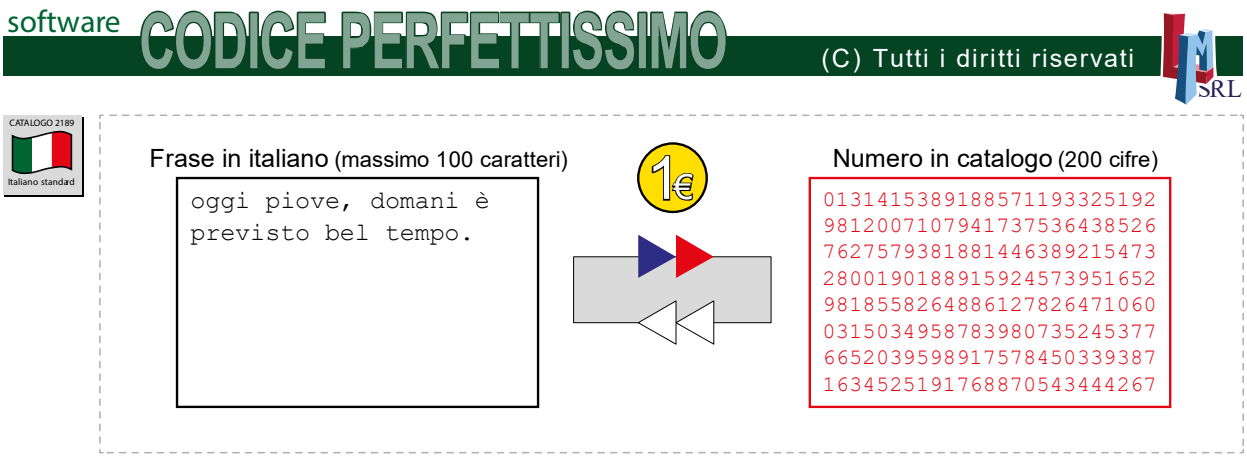
Sistemi a chiave pubblica

Ritorniamo al nostro progetto di codice *perfettissimo* e consideriamo un programma capace di selezionare le frasi di senso compiuto (o perlomeno le stringhe corrette da un punto di vista ortografico, sintattico e grammaticale) pescate dall'elenco di tutte le possibili concatenazioni alfanumeriche di una certa lunghezza. Chiamiamo queste stringhe "frasi sensate". Immaginiamo ora la seguente situazione: grazie al programma, una certa azienda, la *Liceo Matematico SRL*, crea un'enorme banca dati, accessibile online a chiunque (magari a pagamento), contenente tutte le "frasi sensate" scritte in italiano e composte da un massimo di 100 caratteri appartenenti ad una tavola di simboli 10×10 (semplice, senza omofoni o metasimboli). Le "frasi sensate" sarebbero registrate secondo una qualche logica che non ci interessa e a ciascuna di queste frasi verrebbe associato univocamente un numero d'ordine di 200 cifre. È di fondamentale importanza che ad ogni "frase sensata" sia associato un solo numero e ad ogni numero di 200 cifre sia associata una "frase sensata".

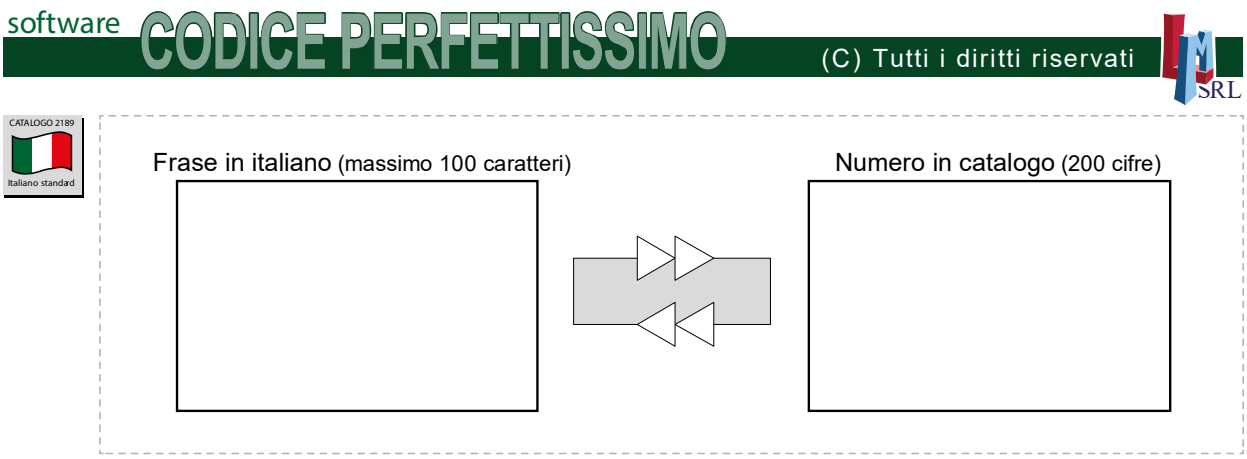
In basso è mostrato un ipotetico utilizzo del software per trasformare un messaggio in un numero:

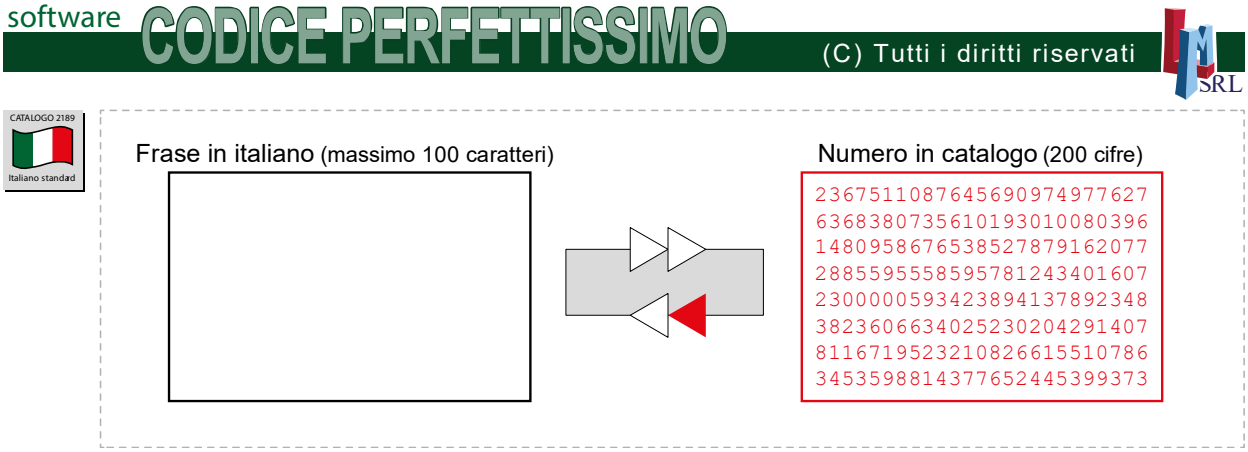


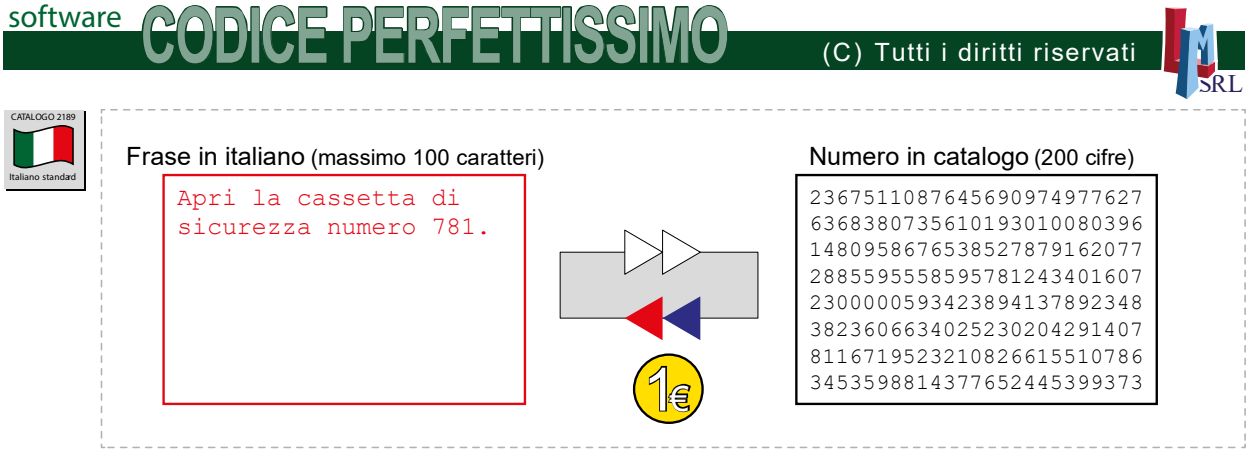




A seguire, l'ipotetico utilizzo del software in senso inverso, da numero a frase:







Crittando il numero in catalogo con una qualche chiave ed avvertendo l'interlocutore che si sta utilizzando la banca dati della *Liceo Matematico SRL* relativa all'*italiano standard*, si otterrebbe effettivamente un *codice perfettissimo*: in questo sistema ogni chiave diversa genererebbe un messaggio scritto in italiano perfettamente coerente e non sarebbe quindi possibile in alcun modo decrittare il messaggio senza disporre della chiave.

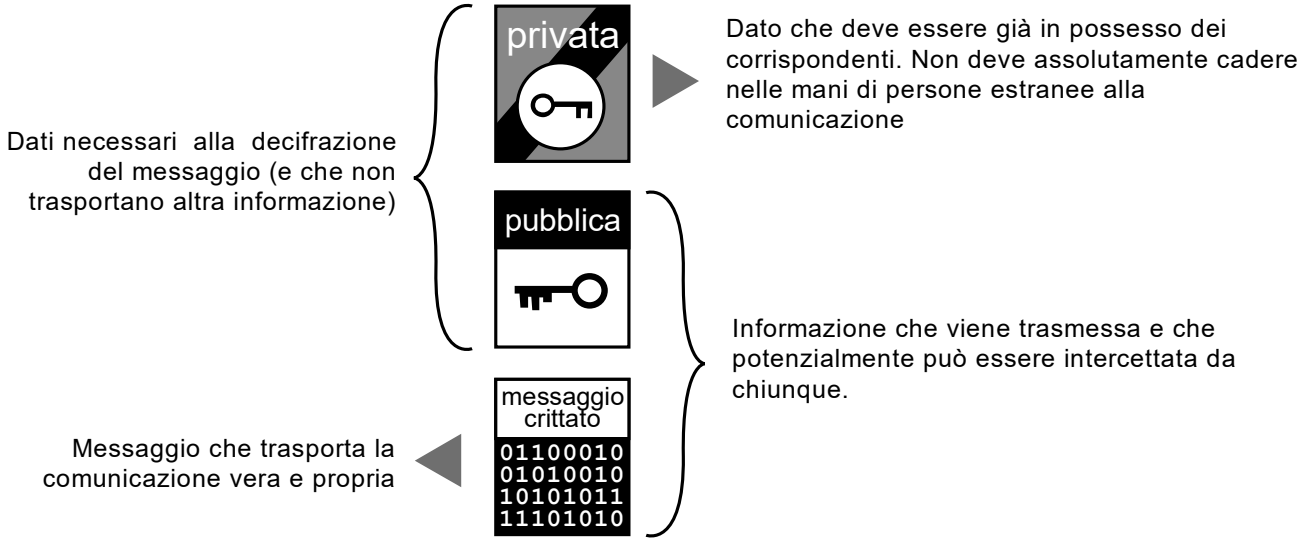
Per garantire l'effettiva "perfezione" del metodo, è fondamentale che ad ogni numero in catalogo corrisponda una "frase sensata" della lingua di comunicazione. L'ipotetica azienda *Liceo Matematico SRL* dovrebbe quindi preoccuparsi di creare banche dati per ogni lingua e, auspicabilmente, per ogni lingua predisporre cataloghi dedicati a specifici settori: dovendo spedire un testo scritto in italiano ma afferente all'Economia, sarebbe fondamentale che l'algoritmo non abbia eliminato dall'elenco delle "frasi sensate" le stringhe contenenti termini

come “spread”, “BOT”, “A++” e così via. Possiamo quindi immaginare che il mittente debba comunicare al suo interlocutore non solo il testo crittato ma anche il codice del catalogo usato: senza di esso nessuna messa in chiaro sarà possibile.

Riassumendo, nel *codice perfettissimo*, il mittente dovrà trasmettere al destinatario le tre informazioni incorniciate a fianco.

- LA CHIAVE
- IL CODICE DEL CATALOGO
- IL MESSAGGIO CRITTATO

Si suppone come al solito che la chiave usata per cifrare il messaggio sia già in possesso del destinatario o che possa essere trasmessa attraverso un canale alternativo, eventualmente lento ma sicuro. È importante notare che anche il codice del catalogo è indispensabile alla decodifica del messaggio e che esso non trasporta altra informazione che questa: esso è quindi a tutti gli effetti un’altra chiave, anche se di pubblico dominio, che dovrà essere trasmessa, in chiaro, insieme al messaggio. Il concetto di “chiave” deve quindi essere scisso in due: nella *Crittografia moderna* si distingue infatti tra **chiave privata** (la “classica” chiave che deve rimanere segreta ed è necessaria alla decodifica) e la **chiave pubblica** (informazione anch’essa necessaria per decodificare il messaggio ma accessibile a tutti o perlomeno suscettibile di intercettazione).



Le difficoltà tecnologiche e teoriche di disporre di un’intelligenza artificiale capace di selezionare da un paniere di stringhe create a caso, non solo “frasi formalmente corrette”, ma addirittura “frasi sensate” (è solo in questo caso che il sistema si merita l’appellativo di *perfettissimo*), non permettono al momento di implementare il metodo che abbiamo appena visto. Si tratta in ogni caso di una possibile direzione di sviluppo della *Crittografia* e che promette, almeno in linea teorica, la morte della Crittoanalisi. La distinzione fra chiave privata e pubblica al contrario è largamente diffusa e caratterizza molti dei sistemi crittografici contemporanei.

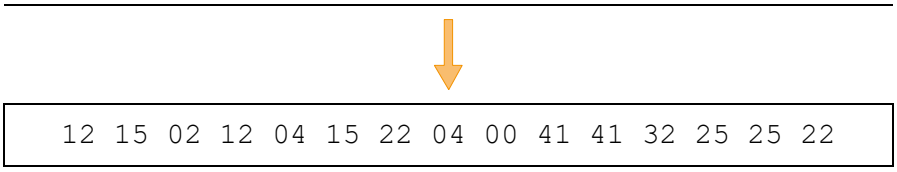
Vediamo ora un altro importante metodo per migliorare la sicurezza dei messaggi e che riguarda, almeno all’apparenza, un metodo di sostituzione.

Le parasostituzioni

Consideriamo la classica tavola 6×6 e traduciamo il messaggio “Il cielo è azzurro”. Otteniamo…

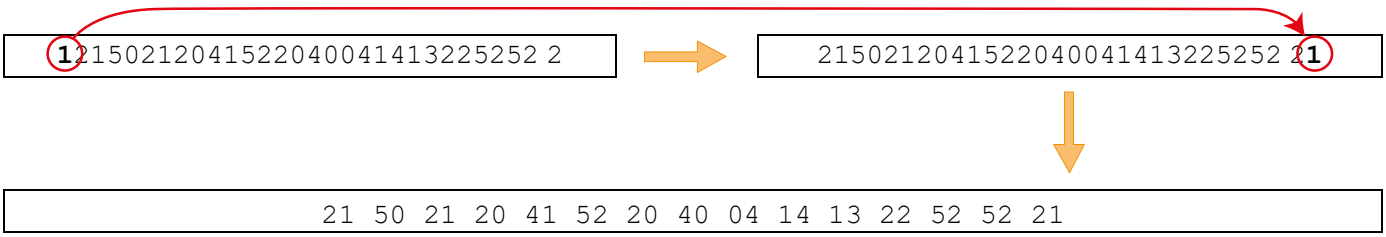
ILCIELOEAZZURRO

	0	1	2	3	4	5
0	A	B	C	D	E	F
1	G	H	I	J	K	L

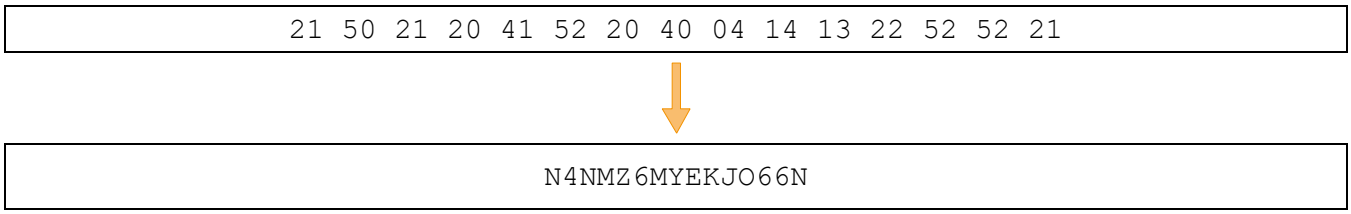


2	M	N	O	P	Q	R
3	S	T	U	V	W	X
4	Y	Z	0	1	2	3
5	4	5	6	7	8	9

Operiamo ora uno slittamento delle cifre riassemblando le coppie in modo sfalsato: basterà spostare la prima cifra in ultima posizione e poi considerare le coppie della nuova sequenza.

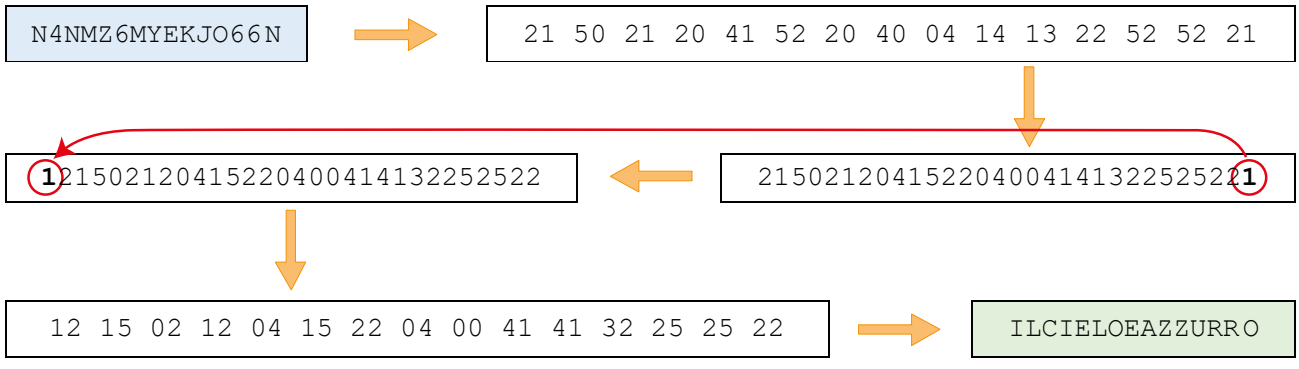


L'ultimo passaggio consiste nel "retrotradurre" le coppie utilizzando la tavola 6×6 in senso decifrante. Il risultato è mostrato in basso



Riassumendo abbiamo ottenuto…

Volendo decifrare il messaggio `N4NMZ6MYEKJO66N` basterà agire in senso contrario:



8.3) La codifica `ILCIELOEAZZURRO` → `N4NMZ6MYEKJO66N` si distingue dalle sostituzioni viste finora per una caratteristica inedita. Di che si tratta?

Il caso appena visto è un primo esempio di **parasostituzione**, una tecnica che usa la sostituzione per camuffare un altro metodo di cifratura. Prima di approfondire questo aspetto, familiarizziamo con lo "slittamento".

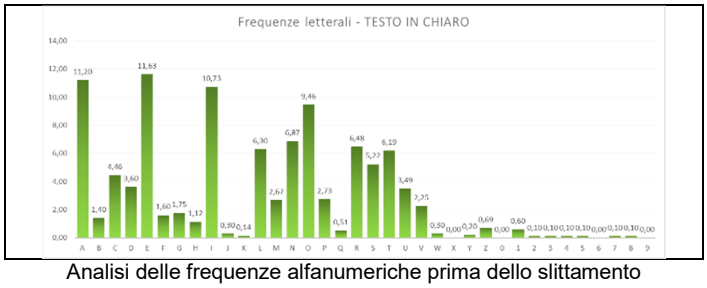
8.4) Usando la tavola 6×6 e la tecnica di “slittamento” vista sopra, codifica i seguenti messaggi:

a) Il mattino ha l’ora in bocca **b)** Non c’è 2 senza 3 **c)** Chi trova un amico trova un tesoro

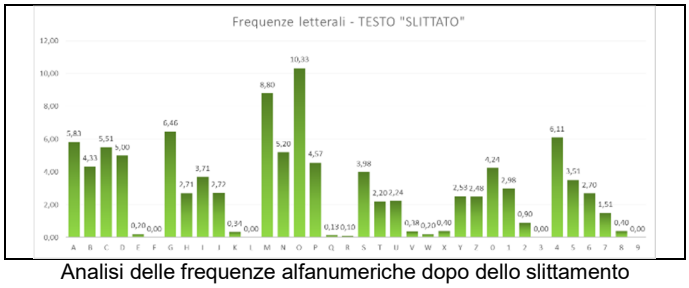
8.5) Decifra i seguenti messaggi cifrati “per slittamento” usando una tavola 6×6.

a) `N7I5MCHCN6MTPGC7GBB5MB` **b)** `UO40BM4DCN54DBM` **c)** `O6HPIO5OGOO`

Come abbiamo visto, la tecnica di slittamento scombina in modo apparentemente imprevedibile le lettere fra loro. Per valutare questo aspetto, osserviamo la comparazione proposta in basso relativa a due analisi effettuate prima e dopo uno slittamento: da un lato si nota un effettivo “snaturamento” delle caratteristiche statistiche del testo in chiaro, dall’altro risulta evidente che la cifratura non riesce a nascondere la presenza di una struttura sottostante.

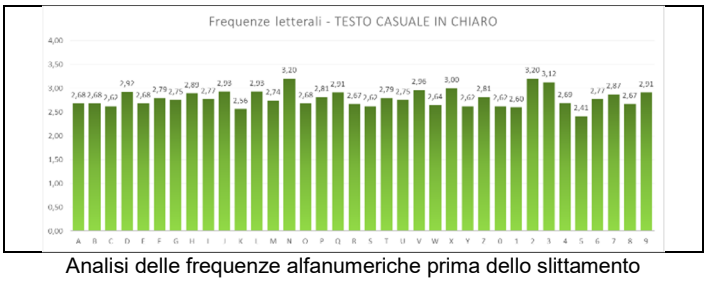


Analisi delle frequenze alfanumeriche prima dello slittamento

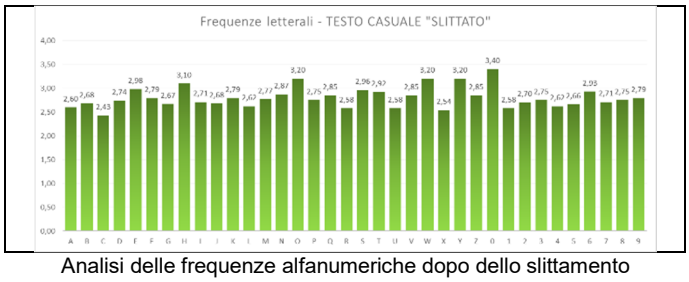


Analisi delle frequenze alfanumeriche dopo dello slittamento

Considerando lo stesso tipo di comparazione effettuato su un testo composto da caratteri alfanumerici casuali, si vede che l’assenza di struttura dell’origine si riflette sulla cifratura.



Analisi delle frequenze alfanumeriche prima dello slittamento



Analisi delle frequenze alfanumeriche dopo dello slittamento

Purtroppo lo slittamento simula un disordine che in verità è molto superficiale, come si intuisce riflettendo sul seguente aspetto:

8.6) Considera una frase qualunque come “Meglio una gallina oggi che un uovo domani”, cioè “`MEGLIOUNAGALLINAOGGICHEUNUOVODOMANI`” ed itera due volte lo slittamento (adottando una tavola qualsiasi). Cosa otterrai?

La tecnica appena introdotta non costituisce una vera e propria cifratura dal momento che non prevede alcuna chiave. Essa è però il primo esempio di un insieme di tecniche che ricadono sotto il nome di **parasostituzioni** e che sfruttano una caratteristica delle tavole viste finora: l’insieme dei simboli di “arrivo” (a seconda della tavola usata, le cifre da 0 a 5, da 0 a 7 o da 0 a 9 o anche solo $0,1$ in binario) è più compatto dell’insieme dei simboli di partenza (come l’alfabeto anglosassone o l’insieme dei simboli alfanumerici). La contrazione del paniere simbolico ha per effetto l’allungamento del messaggio stesso: si dice per questo motivo che il nuovo alfabeto è “di espansione”, sebbene sia composto da meno simboli.

	0	1	2	3	4	5	6	7
0	A	B	C	D	E	F	G	H
1	I	J	K	L	M	N	O	P
2	Q	R	S	T	U	V	W	X
3	Y	Z	0	1	2	3	4	5
4	6	7	8	9	À	È	Ì	Ò
5	Ù	'		,	.	!	?	:

Vediamo subito un esempio di *alfabeto di espansione* indotto prima dalla tavola 8×8 mostrata a fianco (prima espansione del messaggio) e poi dalla riscrittura in binario (seconda espansione).

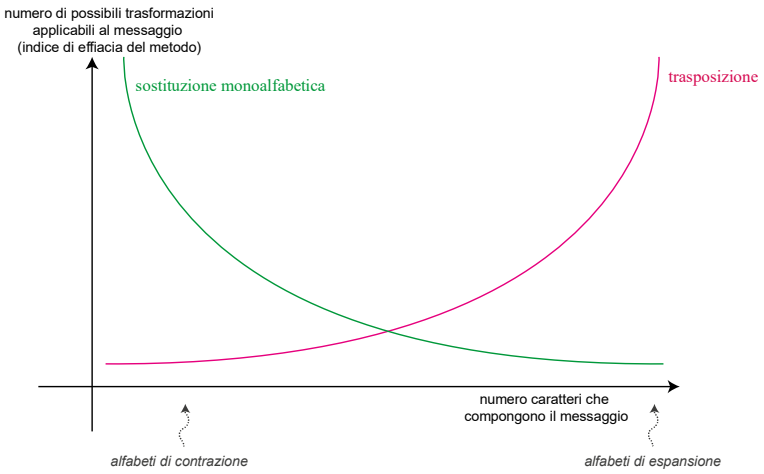
6	(	)	+	-	*	/	=	^
7	\	@	"	€	$	&	%	_

8.7) Compila le caselle vuote sottostanti:

MESSAGGIO ORIGINALE	MESSAGGIO TRADOTTO CON LA TAVOLA 8×8	MESSAGGIO IN BINARIO
Simboli a disposizione: 64	Simboli a disposizione: 8	Simboli a disposizione: 2
`Ciao`	`02100016`	`000010001000000000001110`
Lunghezza messaggio: 4	Lunghezza messaggio: 8	Lunghezza messaggio: 24
	espansione 1	espansione 2
NUMERO DI POSSIBILI SOSTITUZIONI (NELL'ALFABETO DI RIFERIMENTO)	NUMERO DI POSSIBILI SOSTITUZIONI (NELL'ALFABETO DI RIFERIMENTO)	NUMERO DI POSSIBILI SOSTITUZIONI (NELL'ALFABETO DI RIFERIMENTO)
NUMERO DI POSSIBILI TRASPOSIZIONI	NUMERO DI POSSIBILI TRASPOSIZIONI	NUMERO DI POSSIBILI TRASPOSIZIONI

Notiamo che se il messaggio originale fosse composto non da quattro, ma da un migliaio di caratteri, il numero di sostituzioni non cambierebbe (esso dipende soltanto dall'alfabeto) mentre quello delle trasposizioni crescerebbe esponenzialmente. Questa considerazione giustifica il diagramma mostrato in basso:

Nota bene: i grafici accanto non sono stati creati inserendo dati reali ma cercando di dare un'idea dei rispettivi andamenti.



Lo schema a fianco suggerisce una strategia tanto semplice quanto efficace: dato un certo messaggio, si può adottare un alfabeto specifico in modo da "spostarsi" nella zona matematicamente più favorevole (per esempio in una zona ad alto numero di trasposizioni), e poi, effettuata la trasformazione, tornare all'alfabeto iniziale: in questo modo la lunghezza del messaggio tornerà quella iniziale e, auspicabilmente, verrà nascosto il processo di crittazione.

Vediamo due strategia in atto crittando il primo capitolo dei promessi sposi nel seguente modo:

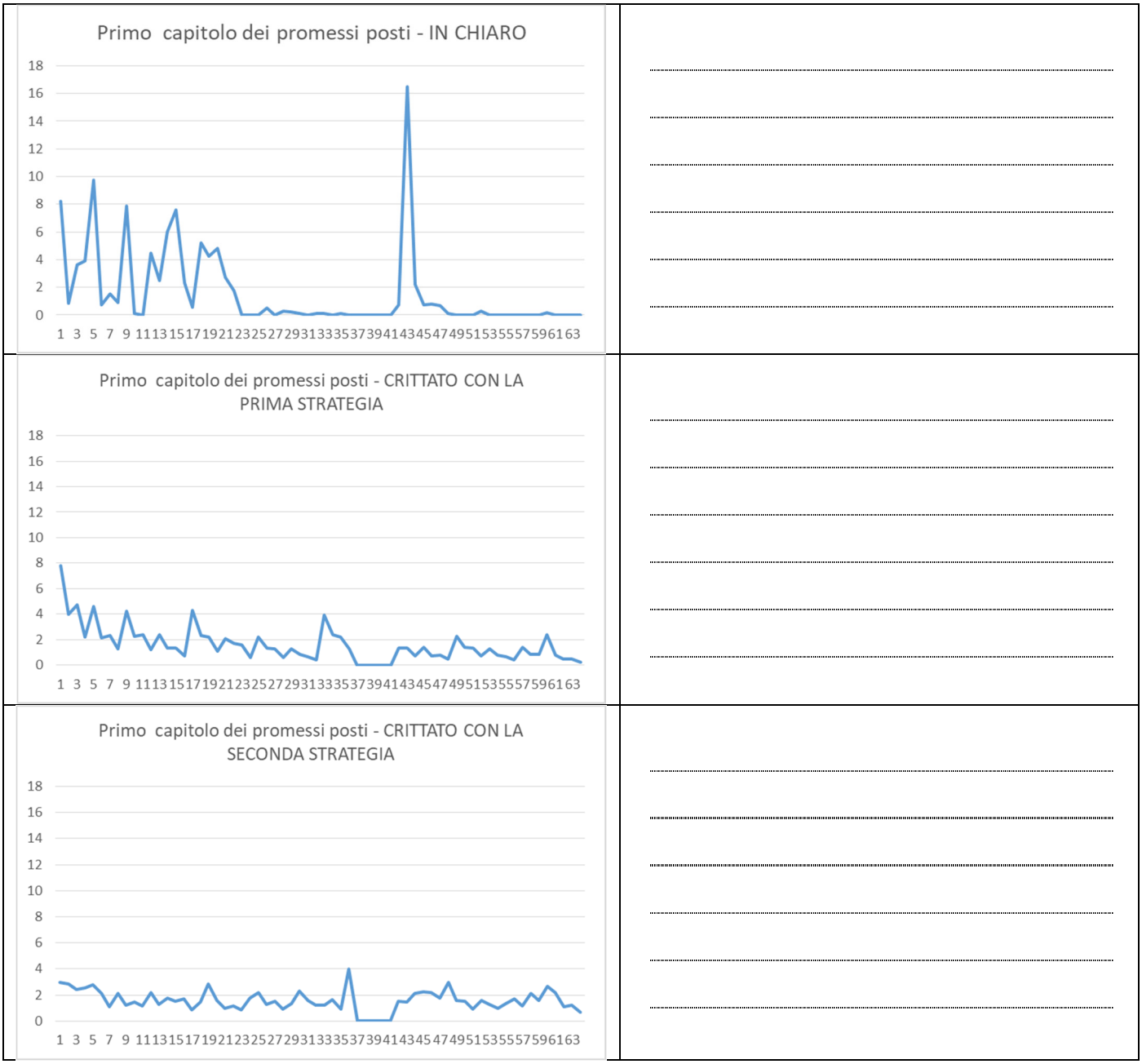
Nel primo caso si procederà così:	
1	Si userà la tavola 8×8 per tradurre il messaggio in cifre e poi si passerà al binario (l'alfabeto di espansione massima). Ciò ci porterà ad una zona ad alto numero di trasposizioni.

Nel secondo caso si procederà così:	
1	Si trasporrà la tavola 8x8 con la chiave scalare "DIALESSANDROMANZONI"

2	Si effettuerà una traslazione sul testo in binario con la chiave scalare “DIALESSANDROMANZONI”	2,3,4	Come 1,2,3 del primo caso (naturalmente al punto 3 si userà la tavola 8×8 trasposta precedentemente)
3	Si tornerà all’alfabeto originale (di contrazione) passando per la tavola 8×8.		

Per vedere valutare la bontà del metodo, consideriamo come al solito l’analisi delle frequenze. Avendo a che fare con la tavola 8×8 si hanno teoricamente 64 colonne: per maggiore chiarezza si è preferito un grafico continuo piuttosto che un istogramma.

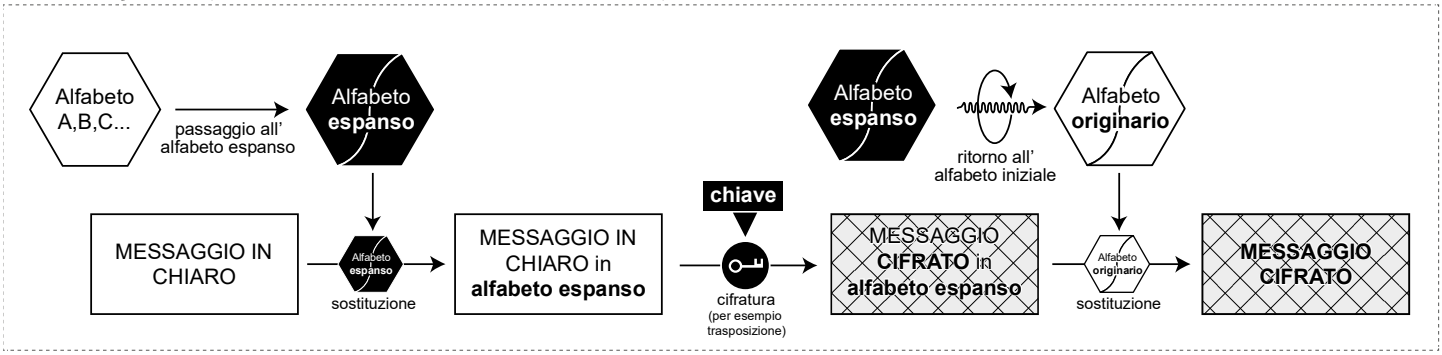
8.7) Cerca di spiegare la forma dei diagrammi rappresentati in basso:



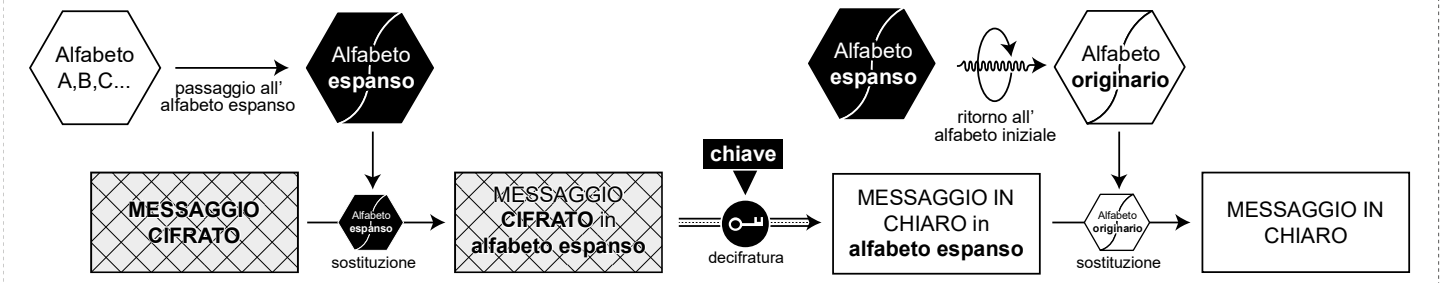
La tecnica appena vista, che consiste in una traduzione finalizzata ad uno “aggiustamento combinatorio” dell’alfabeto, che viene infine annullato tornando alla tavola simbolica di partenza, di chiama **parasostituzione** (perché la prima e l’ultima sostituzione non sono necessariamente finalizzate alla cifratura) o anche **guscio di sostituzione**.

Gli schemi in basso mostrano il funzionamento del guscio di sostituzione e illustrano tre diversi “interventi” della chiave.

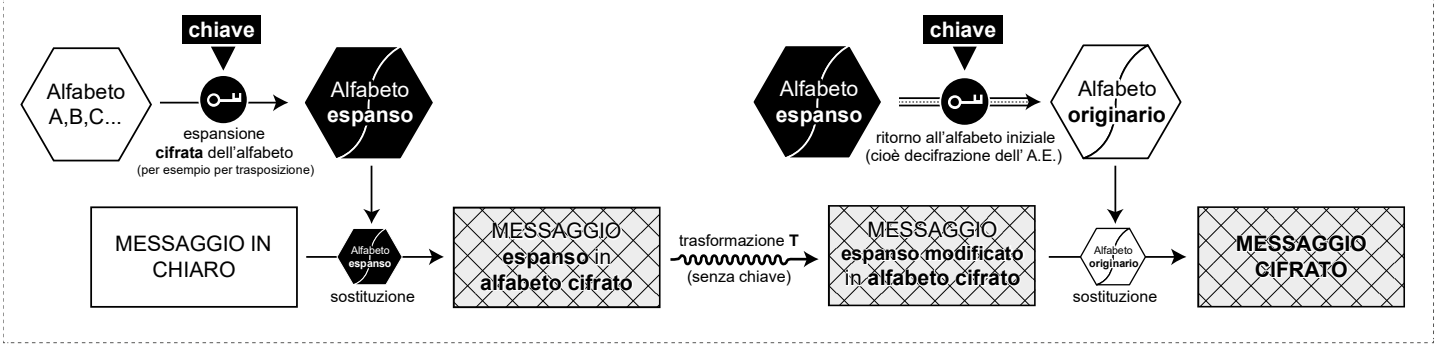
schema di cifratura (GUSCIO DI SOSTITUZIONE SEMPLICE CON NUCLEO A CHIAVE)



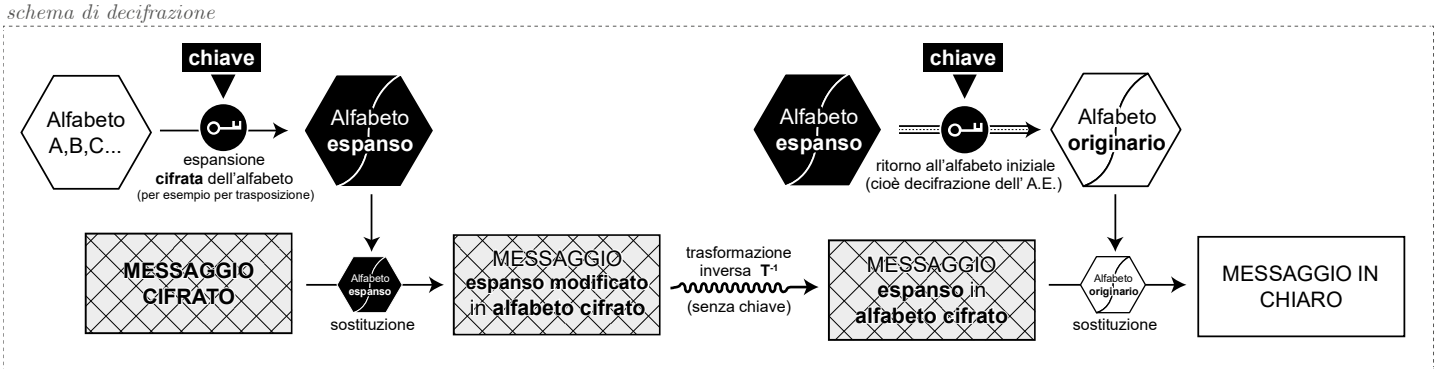
schema di decifrazione



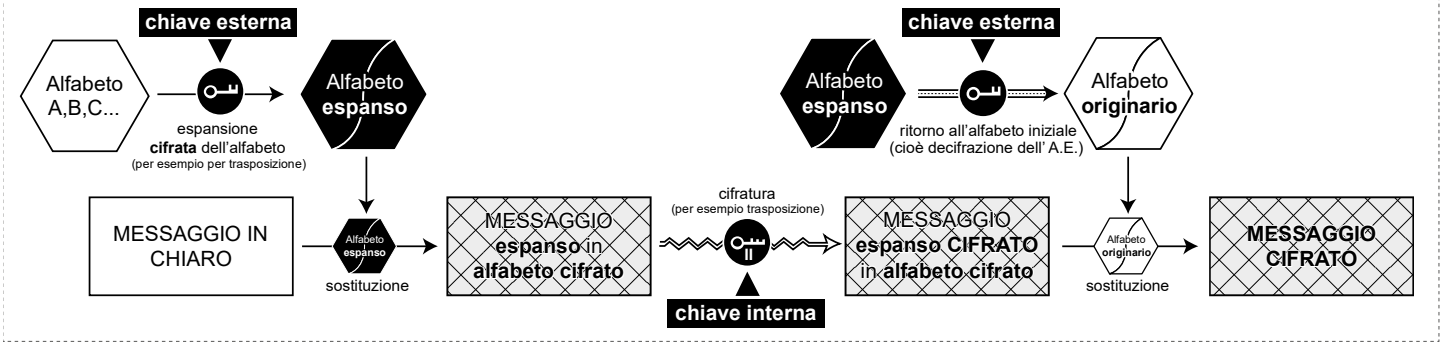
schema di cifratura (GUSCIO DI SOSTITUZIONE A CHIAVE CON NUCLEO SEMPLICE)



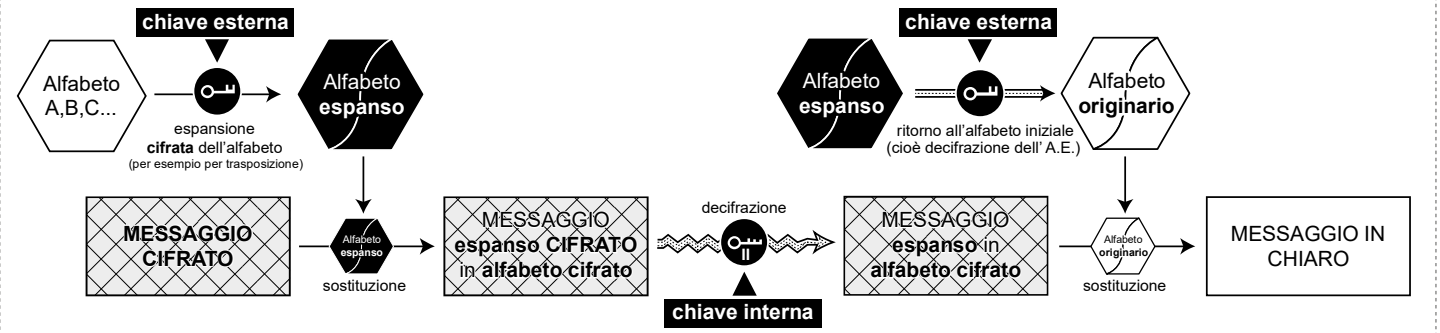
schema di decifrazione



schema di cifratura (GUSCIO DI SOSTITUZIONE A CHIAVE CON NUCLEO A CHIAVE)



schema di decifrazione



8.9) Vediamo ora come ve la cavate con una decifrazione complessa. Il seguente messaggio è stato cifrato con la seguente metodologia:

Cifratura effettuata	
1	Il messaggio è stato tradotto con una tavola 8×8 e poi trasformato in binario a 3 cifre fisse.
2	Si è usata la trasposizione per colonna con chiave “GENOVA” per cifrare il testo in binario
3	Si è tornati all’alfabeto originario (tavola 8×8).

Alla fine la cifra è la seguente:
(c’è un solo spazio e sta fra le due N)

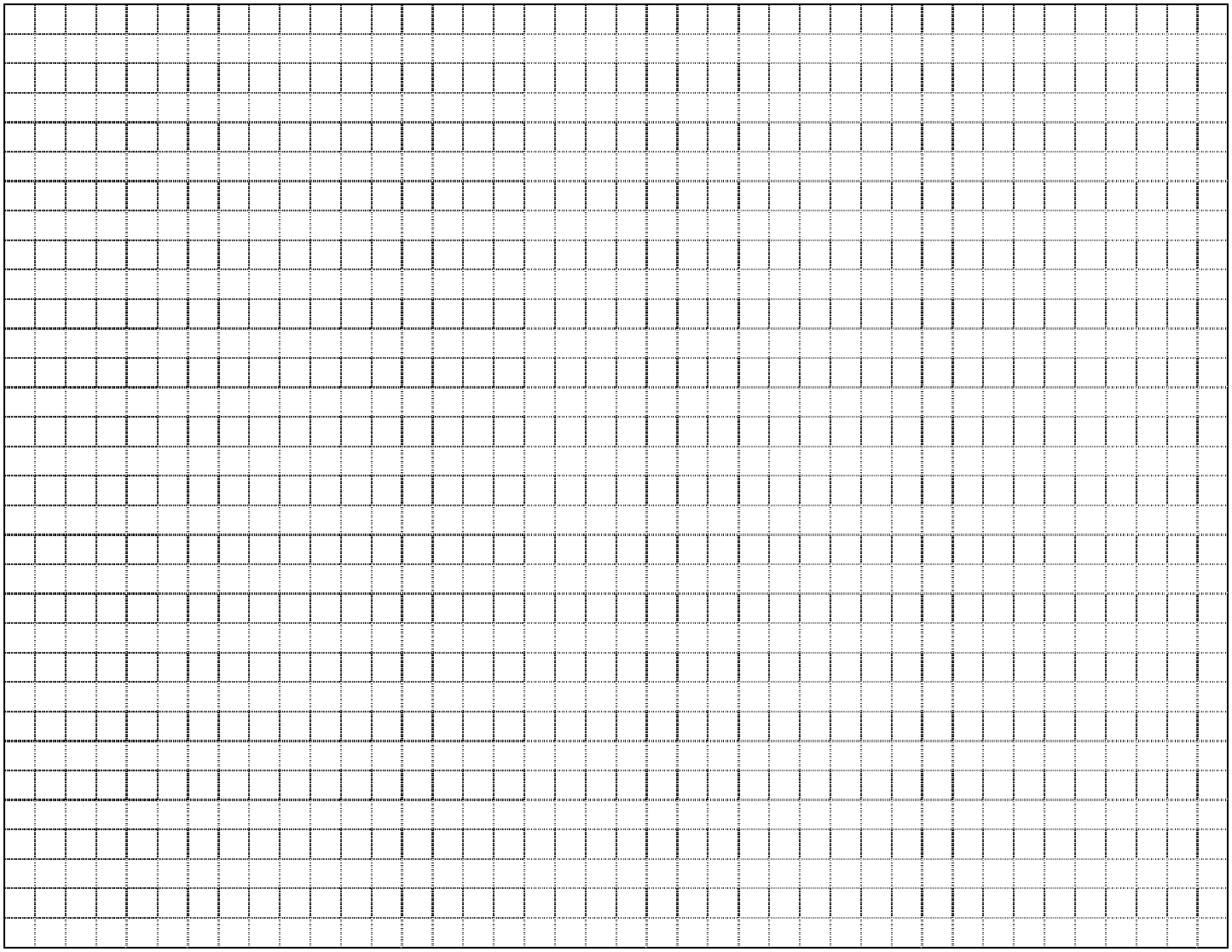
→ `QSCR)HNRLNB9CN NSÌNÈA+H(HNRÒH(BH?`

TAVOLA 8×8

	0	1	2	3	4	5	6	7
0	A	B	C	D	E	F	G	H
1	I	J	K	L	M	N	O	P
2	Q	R	S	T	U	V	W	X
3	Y	Z	0	1	2	3	4	5
4	6	7	8	9	À	È	Ì	Ò
5	Ù	'		,	.	!	?	:
6	(	)	+	-	*	/	=	^
7	\	@	"	€	$	&	%	_

CONVERSIONE BINARIO - DECIMALE

Numeri in binario uniformati a 3 cifre

decimale	*binario*		
0	0	0	0
1	0	0	1
2	0	1	0
3	0	1	1

decimale	*binario*		
4	1	0	0
5	1	0	1
6	1	1	0
7	1	1	1