



6.1) Considera l'esempio a fianco e immagina che i servizi segreti ti abbiano informato che il messaggio contiene una lista di città. Riesci a ricostruire il messaggio?

MESSAGGIO CIFRATO

(trasmesso in gruppi da 5)

RNBOA - EOLKE - YOGWR - TKOYD

Come si vede, per messaggi molto brevi, specialmente se contenuto, contesto o una lista di termini in esso contenuti sono noti, la trasposizione rischia di essere un sistema fragile. D'altro canto, se un messaggio lungo mette a riparo da una "de-anagrammizzazione" rapida, dall'altra espone il testo cifrato ad un'analisi più approfondita, la quale, in assenza di una chiave lunga quanto il testo, permette spesso di scovare ricorrenze e regolarità.

Nasce quindi l'esigenza di inventare un sistema nuovo. Abbiamo già visto un esempio del genere all'inizio del percorso.

6.2) Quale è il significato della seguente frase?

T	X	H	V	W	R	P	H	W	R	G	R	H	V	W	D	W	R	V	S	H	V	V	R
X	W	L	O	L	C	C	D	W	R	G	D	J	L	X	O	L	R	F	H	V	D	U	H

Per risolvere problemi del genere è sempre bene disporre di un alfabeto completo:

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

Ormai conoscete già il metodo usato e quindi la risposta. Le lettere usate nel codice sono le lettere dell'alfabeto italiano slittate di 3 unità, per cui le A sono state trasformate in D, le B in E e così via.

Avendo noi il compito di passare dal testo cifrato al testo in chiaro, ci conviene utilizzare una tabella come quella mostrata in basso, detta **tabella del decifratore** (le lettere messe in rilievo corrispondono alla prime lettere del messaggio cifrato e del messaggio in chiaro).

TABELLA DEL DECIFRATORE (o TABELLA DI DECIFRAZIONE)

Alfabeto CIFRATO	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
Alfabeto CHIARO	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W

Si trovano le lettere nella prima riga e si leggono le controparti della seconda. Si ottiene così il testo seguente:

CIFRATURA

T	X	H	V	W	R	P	H	W	R	G	R	H	V	W	D	W	R	V	S	H	V	V	R
----------	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

X	W	L	O	L	C	C	D	W	R	G	D	J	L	X	O	L	R	F	H	V	D	U	H
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

SOLUZIONE

Q	U	E	S	T	O	M	E	T	O	D	O	E	S	T	A	T	O	S	P	E	S	S	O
U	T	I	L	I	Z	Z	A	T	O	D	A	G	I	U	L	I	O	C	E	S	A	R	E

Volendo eseguire l'operazione di cifratura in modo analogo, trovando cioè le lettere “da tradurre” nella prima riga di una tabella e cercando le lettere cifrate nella seconda, dovremmo non solo invertire le righe ma, per maggiore chiarezza, fare in modo che la prima riga sia ordinato dalla A alla Z (come al solito è messa in rilievo la coppia $T \rightarrow Q$, che in questa tabella diventa $Q \rightarrow T$). Otteniamo così la **tabella del cifratore**.

TABELLA DEL CIFRATORE (o TABELLA DI CIFRATURA)	
Alfabeto CHIARO	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
Alfabeto CIFRANTE	D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

In questo caso, la sequenza di lettere che occupa la seconda riga è il cosiddetto **alfabeto cifrante**.

È evidente che il metodo usato per crittare il messaggio, detto *cifrario di Cesare*, può essere generalizzato a slittamenti qualsiasi: in pratica la misura dello slittamento costituisce la chiave della cifratura.

6.3) Compila una *tabella del cifratore* relativa ad un *cifrario di Cesare* slittato di 5 unità. Cifra poi il messaggio “ALEA IACTA EST”

TABELLA DEL CIFRATORE	
Alfabeto CHIARO	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
Alfabeto CIFRANTE	

Messaggio in chiaro	A L E A I A C T A E S T
Messaggio cifrato	

6.4) Il seguente messaggio è stato generato con un *cifrario di Cesare* slittato di 12 unità. Ricostruisci le tabelle del *cifratore* e del *decifratore* e poi riporta in chiaro il messaggio HIEIC – EISPF – IHSTW – ZWAW.

TABELLA DEL CIFRATORE	
Alfabeto CHIARO	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
Alfabeto CIFRANTE	

TABELLA DEL DECIFRATORE	
Alfabeto CIFRATO	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
Alfabeto CHIARO	

DECRITTAZIONE DEL MESSAGGIO:

H	I	E	I	C	E	I	S	P	F	I	H	S	T	W	Z	W	A	W

6.5) Il testo incorniciato in basso è stato cifrato con il metodo di Cesare. Trova e scrivi l'alfabeto cifrante (completando così la *tabella del cifratore*), compila poi la *tabella del decifratore*, decifra il testo e scopri di che cosa si tratta:

TABELLA DEL CIFRATORE																										
Alfabeto CHIARO	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
Alfabeto CIFRANTE																										

TABELLA DEL DECIFRATORE																										
Alfabeto Cifrato	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
Alfabeto Chiaro																										

PBKDOVVSNSDKVSKVSDKVSKCONOCDKNOVVOVWYNSCMSZSYCOMSXDKVKDOCDKNYF
 OVKFSDDDYBSKVOZYBQKVKMRSYWKMRORCMRSKFKNSBYWKSNNNSYVKMBOYCDBSXQSKW
 MSKMYBDOCSKWZBYXDSKVVKWYBDOVSDKVSKMRKWKYXYSKSKWYNKCOMYVSMKVZO
 CDSNOBSCSZOBMROXYXCSKWZYZYVYZOBMROCSKWNSFSCSBKMMYVQKMSEXEXSMKL
 KXNSOBKEXKCZOWONSPYXNOBMSSXCSOWOQSKVYBKCEYXYCDBSXQSKWMSKMYBDO
 CSKWZBYXDSKVVKWYBDOVSDKVSKMRKWKYEXSKWYMSKWSKWMYMSVEXSYXOOVKWYBO
 BSFOVKXYKSZYZYVSVOFSONOVCSQXYBOQSEBSKWYPKBVSLOBYSVCEYVYXKDSYEX
 SDSZOBNSYMRSFSXMOBMSZEYCDBSXQSKWMSKMYBDOCSKWZBYXDSKVVKWYBDOVS
 DKVSKMRKWKYNKVVKVZOKCSMSVSKNYFEXAEOOVOQXKXYQXEYWNSSPOBBEMMSYRK
 SVMYBOOVKWKXYSLSWLSNSDKVSKCSMRKWKXLKVSVKSVCEYXNYQXSCAESVVKSF
 OCZBSCEYXYCDBSXQSKWMSKMYBDOCSKWZBYXDSKVVKWYBDOVSDKVSKMRKWKYCY
 XQSEXMRSMROZSOQKXYVOCZKNOFOXNEDOQSKVKAESVKNKECDBSKVOZOXORKZOB
 NEDOSVCKXQEONSDKVSKOSVCKXQEOZYVKMMYLOFOMYVMYCKMMYWKSVMYBVOLBEM
 SYCDBSXQSKWMSKMYBDOCSKWZBYXDSKVVKWYBDOVSDKVSKMRKWKY

Il *cifrario di Cesare* è molto semplice da rompere, è però un ottimo esempio introduttivo perché contiene in sé alcune caratteristiche comuni a tutti i sistemi di sostituzione **monoalfabetica** (in basso è chiarito il significato di questo aggettivo).

Un metodo di sostituzione **monoalfabetica** si basa essenzialmente su uno scambio biunivoco di simboli, in modo che ad ogni lettera “in chiaro” ne corrisponda esattamente una “in cifra” e viceversa. La grande differenza con i metodi di traslazione visti fino ad ora può essere riassunta dal seguente schema:

- nelle cifrature a traslazione i simboli si mantengono ma cambia la loro posizione
- nelle cifrature a sostituzione cambiano i simboli che però mantengono la loro posizione

Un modo ovvio per migliorare il *cifrario di Cesare* è quello di permettere sostituzioni meno rigide, in modo che ad ogni lettera ne corrisponda un'altra “a caso” (senza che l'intero alfabeto slitti allo stesso modo). Vediamo un esempio:

Alfabeto CHIARO	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
Alfabeto CIFRANTE	W	R	K	L	Y	C	B	T	E	J	I	H	V	Z	D	X	S	A	N	F	U	Q	M	G	P	O

6.6) Utilizzano l'alfabeto cifrante sovrastante, codifica il messaggio “La notte sta arrivando”:

Messaggio in chiaro	L	A	N	O	T	T	E	S	T	A	A	R	R	I	V	A	N	D	O
Messaggio cifrato																			

6.7) È da decodificare il messaggio RUDZY – QWKWZ – OYWFU – FF riportato in basso e creato con l'alfabeto cifrante definito sopra (A→W, B→R, C→K, ecc.). Prima di tutto determina la tabella del decifratore e poi decodifica il messaggio:

TABELLA DEL DECIFRATORE																										
Alfabeto CIFRATO	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
Alfabeto CHIARO																										

Messaggio cifrato	R	U	D	Z	Y	Q	W	K	W	Z	O	Y	W	F	U	F	F
Messaggio in chiaro																	

Sistemi del genere sono naturalmente afflitti dal solito problema: come tenere a mente l'intero alfabeto cifrante, come cambiarlo di frequente fornendo il nuovo alfabeto a tutti i membri della rete di comunicazione e come effettuare una comunicazione estemporanea con una persona esterna alla rete?

Nei sistemi a trasposizione avevamo affrontato tutti questi problemi introducendo i sistemi “a chiave”, in modo che non fosse il sistema a dover essere cambiato e/o comunicato ad un estraneo, ma soltanto una parola che ne determinasse il comportamento. Si tratta ora di introdurre anche la chiave per i sistemi a sostituzione:

I sistemi di sostituzione monoalfabetica a chiave

L'alfabeto cifrante non è che un anagramma dell'alfabeto in chiaro e ciò vuol dire che tutti i sistemi a trasposizione visti finora possono essere usati per creare alfabeti cifranti. Vediamo subito un esempio:

Crea un alfabeto cifrante utilizzando la trasposizione la chiave scalare “AMERICA”

Cifratura dell'alfabeto in chiaro

A	M	E	R	I	C	A
1	6	4	7	5	3	2
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		

Alfabeto cifrante

ABSCK - TDLUY - EMPVZ -
FINQW - GHJOR - X

Trattandosi di un alfabeto cifrante, è conveniente d'ora in poi inserire la cifratura direttamente sotto l'alfabeto in chiaro:

Alfabeto CHIARO	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
Alfabeto CIFRANTE	A	B	S	C	K	T	D	L	U	Y	E	M	P	V	Z	F	I	N	Q	W	G	H	J	O	R	X

Volendo ora cifrare il messaggio "Riunione segreta domani alle ventidue al solito posto", cioè

RIUNIONESEGRETTADOMANIALLEVENTIDUEALSOLITOPOSTO

si ottiene

NUGVUZVKQKDNKWACZPAVUAMMKHKVWUCGKAMQZMUWZ FZQWZ

Come già visto in un esercizio precedente, per effettuare una decifrazione veloce e possibilmente priva di errori, è opportuno creare la *tabella del decifratore*, conviene cioè scambiare fra loro le righe della tabella sovrastante e riordinare le colonne in modo da portare la prima riga nell'ordine consueto (in pratica stiamo scrivendo la retrochiave dell'alfabeto cifrante).

Alfabeto CIFRANTE	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto CHIARO	A	B	D	G	K	P	U	V	Q	W	E	H	L	R	X	M	S	Y	C	F	I	N	T	Z	J	O

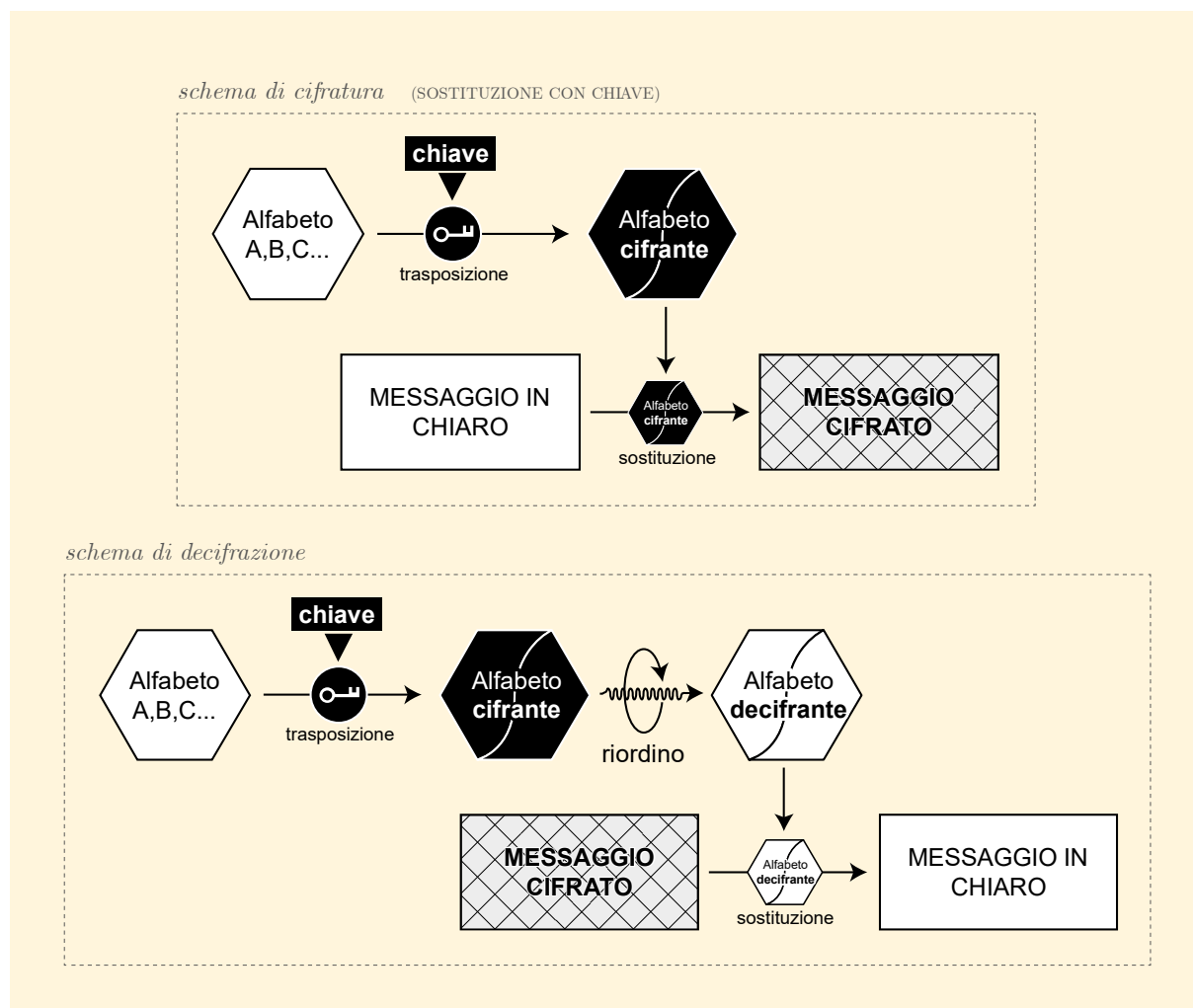
Iniziamo ora la decifrazione (non è necessario arrivare fino alla fine):

Messaggio cifrato

Messaggio in chiaro

N	U	G	V	U
R	I	U	N	I

Possiamo riassumere quanto visto finora sui metodi di sostituzione con i seguenti schemi di cifratura/decifratura:



È interessante notare che la trasposizione che crea l'alfabeto cifrante non viene mai decifrata per inversione del meccanismo: il “riordino” che lega le tabelle del cifratore e del decifratore è infatti assimilabile alla tecnica della tabella di permutazione della *trasformazione inversa*. Il fatto che il meccanismo di trasposizione venga invertito in questo modo consente di utilizzare tecniche generalmente considerate “scomode” in fase di decifrazione come la **trasposizione a chiave scalare** e le **trasposizioni a rettangolo incompleto**.

Vediamo ora una serie di esercizi di cifratura / decifratura:

6.8) Cifra i seguenti messaggi con i metodi indicati

MESSAGGIO		ALFABETO CIFRANTE DA USARE
a)	I soldati si stanno avvicinando	Per trasposizione a chiave scalare con chiave PANORAMA
	ISOLDATISISTANNOAVVICINANDO	
b)	Oggi festa a sorpresa a casa di Laura	Per trasposizione a chiave scalare con chiave LAURA
	OGGIFESTAASORPRESAACASADILAURA	

L'ambasciata deve essere abbandonata immediatamente
da tutto il personale

c)

LAMBASCIATADEVEESSEREABBANDONATA
IMMEDIATAMENTEDATUTTOILPERSONALE

Per **doppia** trasposizione a colonna
con chiave **INDIA** (*rettangolo
incompleto*)

L'ingrediente segreto è il rabarbaro

d)

LINGREDIENTESEGRETOEILRABARBARO

Per trasposizione a colonna con
chiave **TRAMUTEVOLMENTE**

Usa la chiave numero 2

e)

USALACHIAVENUMERODUE

Per **ottava** trasposizione a
colonne con chiave **CANOA**
(*rettangolo incompleto*)

6.9) Decifra i seguenti messaggi (vedi l'esercizio guida svolto in basso)

Alfabeto cifrato per **doppia trasposizione** a colonne con chiave **OCCHIO** (*rettangolo incompleto*)

Esercizio guida

Y	X	U	Q	S	J	M	S	E	X	I	H	B	X
---	---	---	---	---	---	---	---	---	---	---	---	---	---

Alfabeto cifrato per trasposizione a colonne con chiave **CASTELLO** (*rettangolo incompleto*)

a)

F	B	O	B	H	G	F	B	Z	G	H	Z	E	V	A	A	R	B	H	B	N	A	F	F	B
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

Alfabeto cifrato per trasposizione a chiave scalare con chiave **LETTO**

b)

P	N	W	P	M	K	D	I	E	N	K	L	B	B	K	E	T	E	I	I	P	H	I	P
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

Alfabeto cifrato per trasposizione a chiave scalare con chiave **PINGUINO**

c)

G	F	G	G	Y	S	F	V	F	J	H	S	Y	S	H	T	R	T	V	H	G	F	G	G	Y
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

SVOLGIMENTO DELL'ESERCIZIO GUIDA

Prima cifratura
dell'alfabeto

O	C	C	H	I	O
5	1	2	3	4	6
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				

Seconda cifratura
dell'alfabeto

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

Alfabeto cifrante

HOEMX - NUKST -
DQYZJ - WFBIV -
GRCPA - L

TABELLA DEL

CIFRATORE

Alfabeto CHIARO	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
Alfabeto CIFRANTE	H	O	E	M	X	N	U	K	S	T	D	Q	Y	Z	J	W	F	B	I	V	G	R	C	P	A	L

TABELLA DEL DECIFRATORE

Alfabeto Cifrato	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
Alfabeto Chiaro	Y	R	W	K	C	Q	U	A	S	O	H	Z	D	F	B	X	L	V	I	J	G	T	P	E	M	N

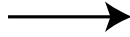
Messaggio cifrato	Y	X	U	Q	S	J	M	S	E	X	I	H	B	X
Lettere in chiaro	M	E	G	L	I	O	D	I	C	E	S	A	R	E

MESSAGGIO: MEGLIO DI CESARE

SVOLGIMENTO DELL'ESERCIZIO a)

Cifratura dell'alfabeto in chiaro

C	A	S	T	E	L	L	O
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						



Alfabeto cifrante



TABELLA DEL CIFRATORE

[illegible]

TABELLA DEL DECIFRATORE

[illegible][illegible]

SVOLGIMENTO DELL'ESERCIZIO b)

Cifratura dell'alfabeto in chiaro

[illegible]

Alfabeto cifrante



TABELLA DEL CIFRATORE

[illegible]

TABELLA DEL DECIFRATORE

[illegible]

Messaggio
cifrato

Lettere in chiaro

[illegible]

SVOLGIMENTO DELL'ESERCIZIO c)

Cifratura dell'alfabeto in chiaro

P	I	N	G	U	I	N	O

Alfabeto cifrante



TABELLA DEL CIFRATORE

Alfabeto CHIARO	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
Alfabeto CIFRANTE																										

TABELLA DEL DECIFRATORE

Alfabeto CIFRATO	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
Alfabeto CHIARO																										

Messaggio
cifrato

Lettere
in chiaro

G	F	G	G	Y	S	F	V	F	J	H	S	Y	S	H	T	R	T	V	H

Rappresentazioni del metodo di sostituzione e periodo della trasformazione

È facile convincersi che le due rappresentazioni sintetiche che abbiamo adottato per descrivere le cifrature per trasposizione, cioè la **tabella delle permutazioni** (o la traccia di permutazione) e la **concatenazione di cicli disgiunti**, possono essere usate per descrivere anche i metodi di sostituzione. Per come abbiamo introdotto l'argomento, la tabella di permutazione (che informa su dove finiscono le lettere originariamente poste in 1,2,3..) ha il suo corrispettivo nella **tabella del cifratore** (che informa su come vengono cambiati i simboli originariamente scritti come *A, B, C, ...*): la traccia di permutazione è quindi associata all'alfabeto cifrante. Costruire i cicli di una sostituzione è un lavoro banale, come mostrato nel seguente esempio:

TABELLA DEL CIFRATORE																										
Alfabeto CHIARO	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
Alfabeto CIFRANTE	F	G	P	A	H	Q	B	I	R	X	C	J	M	S	Y	D	K	N	T	V	Z	E	L	O	U	W

Rappresentazione per cicli disgiunti della sostituzione

$(A\ F\ Q\ K\ C\ P\ D)\ (B\ G)\ (E\ H\ I\ R\ N\ S\ T\ V)\ (J\ X\ O\ Y\ U\ Z\ W\ L)\ (M)$

Possiamo concludere che il calcolo del **periodo** P_S di una sostituzione obbedisce alle stesse regole già viste nella trasposizione a anzi, può essere direttamente calcolato dalla legge di trasposizione usata per creare l'alfabeto cifrante.

Tabelle di sostituzione intervertite

Usando per l'alfabeto una trasposizione T di periodo $P_T = 2$ si può costruire una tabella con una doppia funzione cifrante-decifrante, molto fragile da un punto di vista crittografico ma comoda e rapida (e importante da un punto di vista storico). Per chiarire il meccanismo consideriamo la seguente *tabella del cifratore*:

TABELLA DEL			CIFRATORE						ALFABETO INTERVERTITO																			
Alfabeto CHIARO	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		
Alfabeto CIFRANTE	K	S	F	Z	R	C	H	G	P	O	A	U	Y	V	J	I	X	E	B	T	L	N	W	Q	M	D		

Si riconosce subito che ogni ciclo ha lunghezza 1 (vedi ad esempio la (T)) oppure 2 (vedi (A, K)). Non c'è quindi alcuna perdita di informazione lasciando per ogni ciclo di lunghezza 2 una coppia soltanto ed eventualmente cancellando le coppie di ciclo unitario (infatti volendo si potrebbe ricostruire la tabella originaria senza difficoltà):

ALFABETO INTERVERTITO (ridotto)																										
Alfabeto CHIARO	A	B	C	D	E		G		I	J		L	M	N			Q			T			W			
Alfabeto CIFRANTE	K	S	F	Z	R		H		P	O		U	Y	V			X			T			W			

Togliendo spazi vuoti coppie eliminate, si ottiene uno schema come quello mostrato in basso, detto **alfabeto intervertito** o **tabella intervertita**. Negli schemi di questo tipo ciascuna lettera o non è presente oppure occorre una volta soltanto. Non è quindi possibile parlare di alfabeto in chiaro o di alfabeto cifrante: sia per cifrare che per decifrare si opera allo stesso modo, cercando in tabella la lettera da modificare e, se presente, usando la compagna per effettuare la sostituzione.

Nella tabella a fianco si è scelto di non cancellare le lettere relative ai due cicli unitari (T) e (W) per maggiore chiarezza.

TABELLA INTERVERTITA														
Alfabeto CHIARO	A	B	C	D	E	G	I	J	L	M	N	Q	T	W
Alfabeto CIFRANTE	K	S	F	Z	R	H	P	O	U	Y	V	X	T	W

Vediamo subito un esempio:

6.10) Usando la tabella intervertita sovrastante, decodifica i seguenti messaggi:

a)	P	U	B	P	T	J	R	B	J	T	T	J	K	T	T	K	F	F	J
b)	F	K	Y	S	P	K	U	K	T	L	K	I	K	B	B	W	J	E	Z

Tavole di simboli

Nella cifratura per trasposizione è altamente sconsigliato corredare un messaggio di segni di interpunzione quali spazi, virgole, punti e apostrofi: contare tali segni darebbe infatti all'intercettatore informazioni sul numero complessivo di parole. Generalmente si preferisce fare a meno anche delle cifre a rappresentare i numeri, per cui un messaggio come "ATTACCO ALLE 17.00" verrebbe trascritto come "ATTACCO ALLE DICIASETTE" prima di essere cifrato: trasmettere le cifre 0017 in un ordine qualsiasi potrebbe infatti indurre un intercettatore a sospettare la presenza di un orario e a ricomporlo.

Queste precauzioni diventano superflue nel caso in cui si usi una tecnica di sostituzione e il seguente esempio dovrebbe chiarire il perché:

TABELLA DEL CIFRATORE																										
Alfabeto CHIARO	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
Alfabeto CIFRANTE	R	H	Q	E	C	N	3	L	Y	T	A	6	9	I	0	1	F	!	5	E	.	Y	8	J	Z	P
Alfabeto CHIARO	1	2	3	4	5	6	7	8	9	0	.	,	?	!												
Alfabeto CIFRANTE	S	,	G	4	2	V	M	B	W	X	K	?	7	O												

Con la tabella sovrastante, il messaggio "ATTACCOALLE17.00" verrebbe tradotto in "REERQQ0R66CSSMKXX" e, come si vede, la presenza di cifre è stata dissimulata.

Quando l'insieme dei simboli è ampio e soprattutto, quando i simboli sono facili da confondere fra loro (il punto con la virgola, lo zero e la lettera "O", lo spazio e un'accidentale spaziatura troppo abbondante), si preferisce abbandonare l'alfabeto cifrante a favore della tavole di cifratura mostrate in basso. In questo caso, le griglie di sostituzione, chiamate **tavole dei simboli** (o semplicemente *tavole*), sono rappresentate in forma quadrata (o più raramente rettangolare) e prevedono la sostituzione di tutti i simboli in codici esclusivamente numerici: questo spiega una parte del lessico crittografico: **CIFRATURA**, **CIFRARIO** e **CIFRA**.


Vediamo alcuni esempi:

Per una fortunata coincidenza, l'insieme delle lettere dell'alfabeto anglosassone e le dieci cifre del sistema decimale messi assieme, formano una griglia quadrata 6×6 . A fianco è mostrata una tabella del genere. Ci riferiremo ad essa con il nome "Tavola 6×6 " o anche "Tavola alfanumerica minima"

Tavola 6 × 6

o

Tavola alfanumerica minima



	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

Vediamo come utilizzare una tavola in fase di “traduzione” (parlare di “cifratura” sarebbe eccessivo dal momento che la sostituzione viene fatta senza chiave e con un repertorio ordinato).

Traduzione mediante la *tavola* 6×6

Procedimento

Esempio

- 1) È dato un messaggio alfanumerico da tradurre mediante la griglia. Ogni simbolo viene sostituito dalla coppia di cifre che individuano nell'ordine la riga e poi la colonna del simbolo stesso. A fianco è mostrato il caso della **w** che diventa 34.

	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

- 2) Il messaggio WASHINGTON risulta per esempio “tradotto” in 34 – 00 – 30 – 11 – 12 – 21 – 10 – 31 – 22 – 21 (vedi in basso):

W	A	S	H	I	N	G	T	O	N
34	00	30	11	12	21	10	31	22	21

	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

- 3) Il fatto che la *tavola* sia quadrata ha il vantaggio che colonne e righe vengano indicate con lo stesso insieme di cifre (nell'esempio si tratta in entrambi i casi dai numeri da 0 a 5). Si preferisce in questo caso trasmettere le cifre nella solita disposizione “a cinque” mostrata a fianco:

34	00	30	11	12	21	10	31	22	21
----	----	----	----	----	----	----	----	----	----



34003 – 01112 – 21103 – 12221

Per “retrotradurre” un messaggio numerico, basterà scomporlo in coppie di numeri e utilizzare la stessa tavola usata in fase di traduzione. Vediamo a questo proposito una serie di esempi:

6.11) I seguenti messaggi sono stati cifrati con il *tavola alfanumerica minima* introdotta sopra.

	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

MESSAGGI TRADOTTI IN CIFRA

a) 00313 - 10002 - 02220 - 01515 - 04135 - 40443 - 51

b) 00330 - 02142 - 00250 - 22221 - 02003 - 23204 - 1500

Al posto della *tavola 6x6* si possono introdurre tavole più ampie e quindi capaci di contenere un vocabolario simbolico più ricco. Presento qui una tabella 8×8 , che indicherò con **Tavola standard** e che prevede una serie di simboli di interpunzione (e altri simboli utili) e infine una tavola 16×16 , detta **codice ASCII**, la tavola di simboli più usata nell'ambito dei PC.

		Tavola 8×8 o Tavola Standard							
		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		Û	`		,	.	!	?	:
6		()	+	-	*	/	=	^
7		\	@	"	€	\$	&	%	_

6.12) Riscrivi i seguenti messaggi tradotti con la *tavola standard* (8×8).

MESSAGGI TRADOTTI IN CIFRA

a) 15161 - 55202 - 51455 - 23452 - 22041 - 53100 - 52355 - 4

b) 41623 - 33664 - 34663 - 537

Come si vedrà, nella tabella sottostante relativa al codice ASCII, vi sono molte caselle barrate di rosso, corrispondenti a "caratteri virtuali": si tratta dei caratteri associati ai tasti speciali della tastiera, come ad esempio *INVIO*, *ESC*, *DEL*. Un caso diverso è rappresentato dalla casella apparentemente vuota di riga 02 e colonna 00: in questo caso si tratta semplicemente dello *spazio*.

CODICE ASCII (con numeri di colonne e righe in notazione decimale)

	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
00	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×
01	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×
02		!	"	#	\$	%	&	'	()	*	+	,	-	.	/
03	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
04	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
05	P	Q	R	S	T	U	V	W	X	Y	Z	[\]	^	_
06	`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
07	p	q	r	s	t	u	v	w	x	y	z	{		}	~	×
08	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×
09	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×
10	×	;	¢	£	¤	¥	¦	§	¨	©	ª	«	¬	–	®	—
11	°	±	²	³	´	µ	¶	·	¸	¹	º	»	¼	½	¾	¿
12	À	Á	Â	Ã	Ä	Å	Æ	Ç	È	É	Ê	Ë	Ì	Í	Î	Ï
13	Ð	Ñ	Ò	Ó	Ô	Õ	Ö	×	Ø	Ù	Ú	Û	Ü	Ý	Þ	ß
14	à	á	â	ã	ä	å	æ	ç	è	é	ê	ë	ì	í	î	ï
15	ð	ñ	ò	ó	ô	õ	ö	÷	ø	ù	ú	û	ü	ý	þ	ÿ

Il codice binario

Il passaggio da simboli di vario genere a numeri interi apre le porte all'aritmetica e le possibili manipolazioni a cui può essere sottoposto un messaggio diventano via via più matematiche (e portano un po' alla volta alla crittografia contemporanea). Noi per ora ci accontenteremo di passare da un sistema numerico all'altro, specificamente dal sistema decimale a quello binario. Quest'ultimo utilizza soltanto le cifre 0 e 1 e dà luogo alla seguente tabella (con qui rappresentati soltanto gli interi da 0 a 15)

<i>decimale</i>	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
<i>binario</i>	0	1	10	11	100	101	110	111	1000	1001	1010	1011	1100	1101	1110	1111

Per gli usi che ne faremo, conviene fissare una banda di grandezza per gli interi e uniformare la lunghezza di ciascun numero nel sistema binario anteponendo al primo 1 un numero congruo di cifre nulle. Le seguenti due tabelle mostrano questa operazione per le bande di interi 0 – 7 e 0 – 15.

Numeri in binario uniformati a 3 cifre				
<i>decimale</i>	<i>binario</i>			
0	0	0	0	
1	0	0	1	
2	0	1	0	
3	0	1	1	

<i>decimale</i>	<i>binario</i>			
4	1	0	0	
5	1	0	1	
6	1	1	0	
7	1	1	1	

Numeri in binario uniformati a 4 cifre																
<i>decimale</i>	<i>binario</i>					<i>decimale</i>	<i>binario</i>					<i>decimale</i>	<i>binario</i>			
0	0	0	0	0		4	0	1	0	0		0	1	0	0	
1	0	0	0	1		5	0	1	0	1		1	1	0	0	
2	0	0	1	0		6	0	1	1	0		2	1	0	1	
3	0	0	1	1		7	0	1	1	1		3	1	0	1	

<i>decimale</i>	<i>binario</i>					<i>decimale</i>	<i>binario</i>					<i>decimale</i>	<i>binario</i>			
0	0	0	0	0		4	0	1	0	0		0	1	1	0	
1	0	0	0	1		5	0	1	0	1		1	1	1	0	
2	0	0	1	0		6	0	1	1	0		2	1	1	1	
3	0	0	1	1		7	0	1	1	1		3	1	1	1	

Combinando *tavola standard* 8 × 8 e tabella dei numeri in binario (uniformati a 3 cifre), si possono tradurre messaggi in binario e dal binario in modo molto rapido.

**Tavola
8 × 8 o
Tavola
Standard**



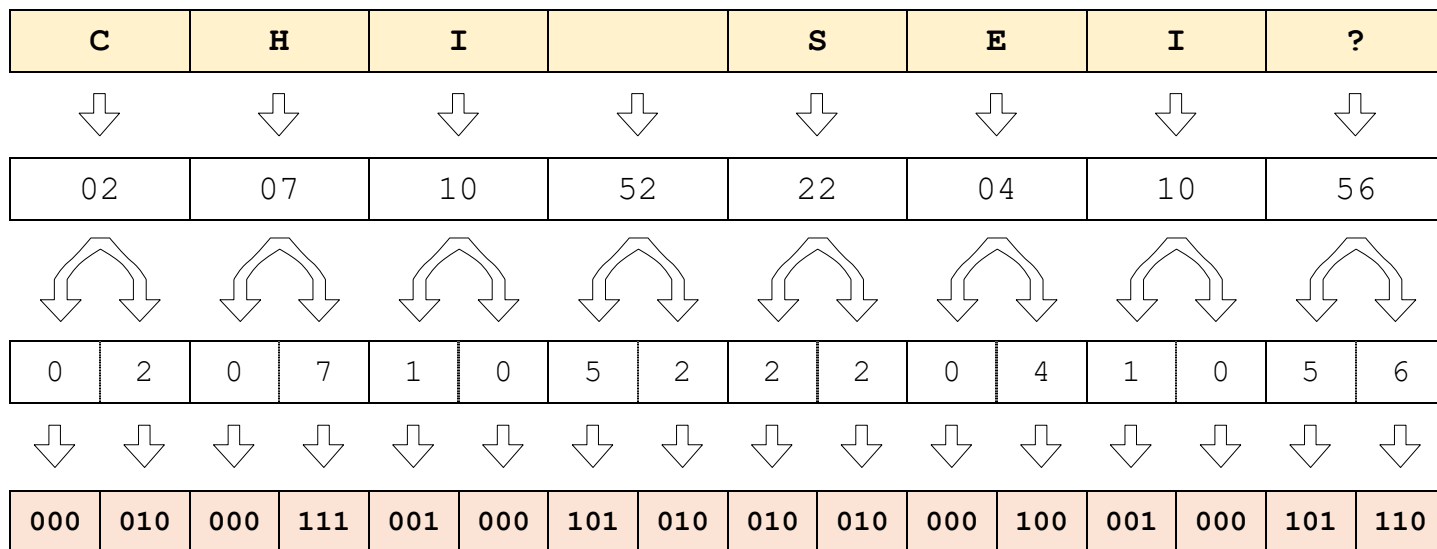
	0	1	2	3	4	5	6	7
0	A	B	C	D	E	F	G	H
1	I	J	K	L	M	N	O	P
2	Q	R	S	T	U	V	W	X
3	Y	Z	0	1	2	3	4	5
4	6	7	8	9	À	È	Ì	Ò
5	Ù	`		,	.	!	?	:
6	()	+	-	*	/	=	^
7	\	@	"	€	\$	&	%	_

<i>decimale</i>	<i>binario</i>		
0	0	0	0
1	0	0	1
2	0	1	0
3	0	1	1
4	1	0	0
5	1	0	1
6	1	1	0
7	1	1	1

Tabella dei
numeri in
binario
uniformati a
tre cifre

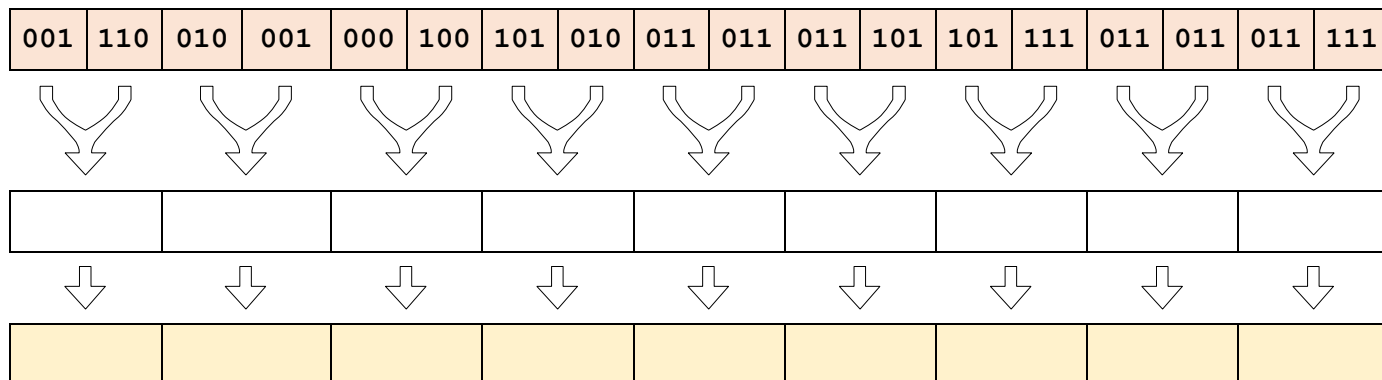


Vediamo subito un esempio e cerchiamo di tradurre in binario (attraverso la *tavola standard*) il messaggio "CHI SEI?", punteggiatura compresa (cioè compresi lo spazio e il punto interrogativo).



Il messaggio risultante può ora essere trasmesso nelle canoniche cinque, in gruppi da otto cifre (per richiamare il byte formato da 8 bit) o anche lasciando le triplette come appaiono sopra.

6.13) Traduci nell'alfabeto della tavola 8 × 8 il seguente messaggio in binario:



6.14) Sul muro che affaccia sul parcheggio interno del liceo Majorana, si vedono un serie di byte (gruppi di 8 cifre binarie) scritti in bianco su sfondo nero. Affacciati e traduci il messaggio in italiano utilizzando il codice ASCII.



Come abbiamo già sottolineato, gli ultimi argomenti, cioè “tavole dei simboli” e “codice binario”, non comportano nessuna segretezza del messaggio, dal momento che costituiscono una mera riscrittura dei simboli tramite una tavola pubblica (come il famosissimo codice ASCII). Esiste un'altra “tavola”, più spesso indicata come alfabeto, ancora più celebre dell'ASCII: il *codice Morse*.

Il codice Morse

Il *codice Morse* è composto una tavola costruita da due simboli visibili (o udibili) e un simbolo accessorio invisibile. I due simboli visibili sono la linea e il punto, il simbolo invisibile, non presente materialmente nella tavola, rappresenta un'interruzione di sequenza e viene prodotto con una pausa (si suppone in questa

descrizione che tutte le pause, quindi *brevi*, *medie* e *lunghe*, siano giustapposizioni di una singola pausa minima). La regola è che ogni simbolo venga tradotto con punti e linee (secondo la tavola in basso) e si concluda con la pausa breve; la pausa media separa fra loro due parole e la pausa lunga due frasi.

Simbolo	Codice	Simbolo	Codice	Simbolo	Codice
A	• —	J	• — — —	S	• • •
B	— • • •	K	— • —	T	—
C	— • — •	L	• — • •	U	• • —
D	— • •	M	— —	V	• • • —
E	•	N	— •	W	• — —
F	• • — •	O	— — —	X	— • • —
G	— — •	P	• — — •	Y	— • — —
H	• • • •	Q	— — • —	Z	— — • •
I	• •	R	• — •		

Potremmo tradurre il *codice Morse* con un sistema ternario usando le tre cifre 0,1,2 in luogo rispettivamente di punto, linea e pausa. Avremmo in questo modo una tavola apparentemente binaria (del tipo $A \rightarrow 01$, $B \rightarrow 1000$) ma realmente ternaria per “colpa” del simbolo *interruzione* $\rightarrow 2$. La domanda è...

6.15) Perché nel *codice Morse* è necessario usare un simbolo di interruzione?

SOLUZIONE 6.15

Il motivo è che nel *codice Morse* la lunghezza delle “parole” è variabile e questo porta a possibili ambiguità: in assenza di pause, la sequenza *punto – linea*, cioè — • , potrebbe significare tanto TE quanto N. Studieremo in seguito altre tavole di questo tipo.

Concludiamo il *codice Morse* con una serie di video e un piccolo allenamento:

Descrizione	Link
Tavola “sonora”	https://www.youtube.com/watch?v=eXjbtXWWEiQ
Apparecchio cecoslovacco utilizzato durante la seconda guerra mondiale	https://www.youtube.com/watch?v=ii3k_pMIHmk

6.16) Trascrivi le seguenti sequenze audio in punti, linee e pause e stabilisci il significato delle comunicazioni:

File	Trascrizione
------	--------------

[MORSE1.WAV](#)

Significato:

[MORSE2.WAV](#)

Significato:

[MORSE3.WAV](#)

Significato:

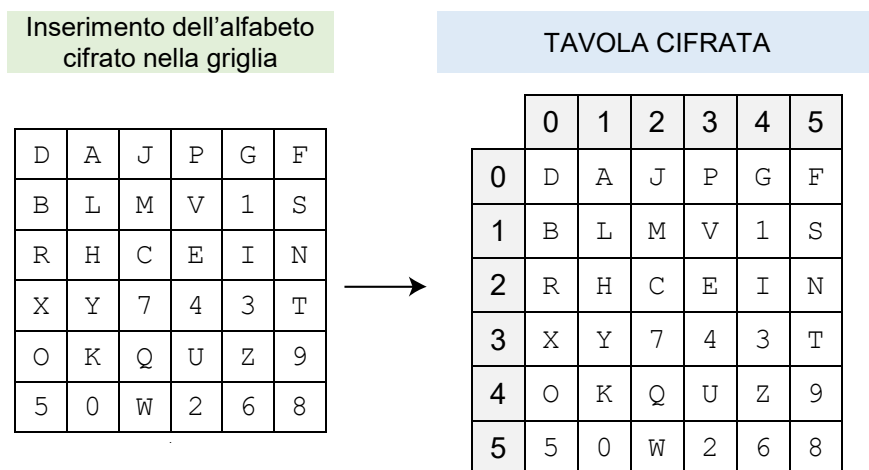
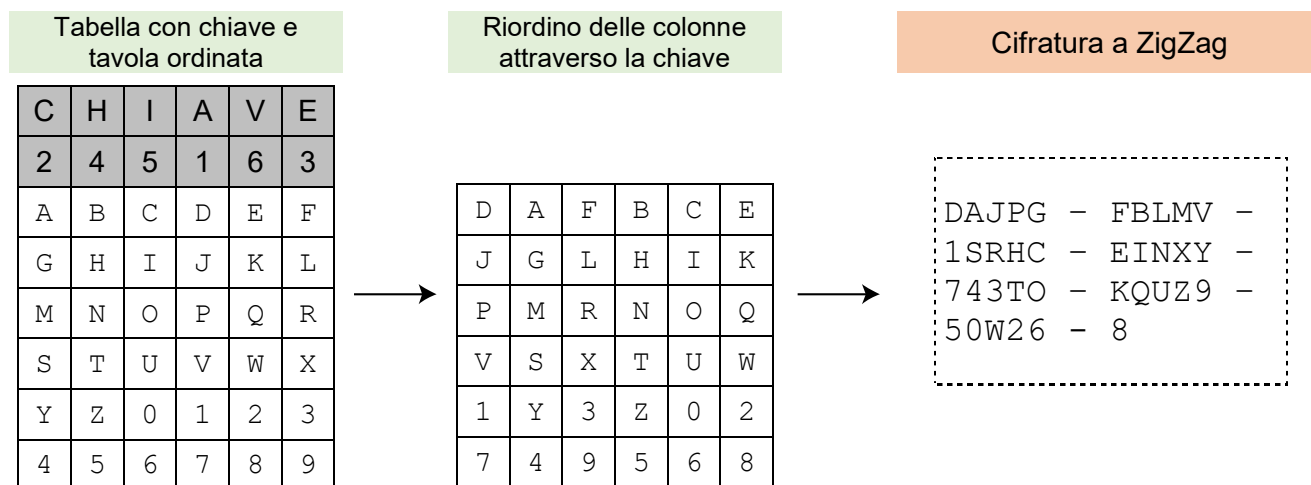
[MORSE4.WAV](#)

Significato:

Cifrature di tavole

Concludiamo questa prima parte relativa alla sostituzione con il pezzo mancante: usare una tavola dei simboli per cifrare un messaggio mediante una parola chiave. Questo si può realizzare nel modo più ovvio, cioè trasponendo la tavola dei simboli prima di operare la traduzione. Si può traslare la forma lineare dell'alfabeto simbolico (magari usando una traccia di permutazione iterata) o mantenere direttamente la tavola nella forma quadrata e dare fondo ai metodi crittografici basati sul rettangolo, dalla trasposizione a colonna fino a quella alla cifratura a *ZigZag* (ricordando in quest'ultimo caso di usare una chiave con un numero di lettere pari al lato del quadrato). Vediamo subito un esempio:

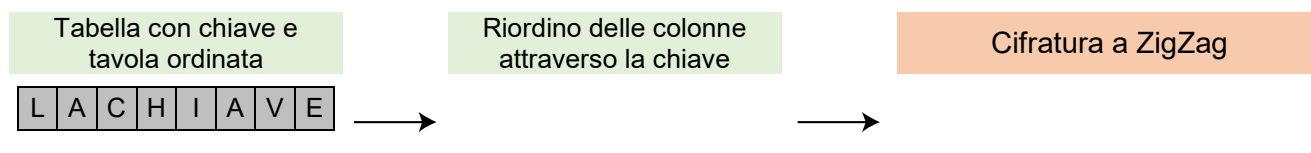
Utilizzando la trasposizione a *ZigZag* e la chiave **CHIAVE**, si cifra la tavola alfanumerica minima (cioè 6×6):



Mettendo ora in cifra il messaggio "Natale è il 25 dicembre", cioè "NATALEEIL25DICEMBRE" si ottiene

25013 - 50111 - 23232 - 41153 - 50002 - 42223 - 12102 - 023

Utilizzando invece la chiave **LACHIAVE** per trasporre la tavola standard (quindi 8×8) a *ZigZag*, otteniamo:



7	1	3	5	6	2	8	4
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	0	1	2	3	4	5
6	7	8	9	À	È	Ì	Ò
Ù	`		,	.	!	?	:
()	+	-	*	/	=	^
\	@	"	€	\$	&	%	_

B	F	C	H	D	E	A	G
J	N	K	P	L	M	I	O
R	V	S	X	T	U	Q	W
Z	3	0	5	1	2	Y	4
7	È	8	Ò	9	À	6	Ì
`	!		:	,	.	Ù	?
)	/	+	^	-	*	(=
@	&	"	_	€	\$	\	%

BFJRN - CHKVZ -
 73SPD - ELX0È -
 ')!85 - TMAGI -
 U1Ò / - @&+:9 -
 2QOWY - À,^" -
 -.64Ì - Ù*€\$(-
 ?=\%

Inserimento dell'alfabeto
cifrato nella griglia

B	F	J	R	N	C	H	K
V	Z	7	3	S	P	D	E
L	X	0	È	`)	!	8
5	T	M	A	G	I	U	1
Ò		/	@	&	+	:	9
2	Q	O	W	Y	À	,	^
"	_	-	.	6	4	Ì	Ù
*	€	\$	(?	=	\	%



TAVOLA CIFRATA

	0	1	2	3	4	5	6	7
0	B	F	J	R	N	C	H	K
1	V	Z	7	3	S	P	D	E
2	L	X	0	È	`)	!	8
3	5	T	M	A	G	I	U	1
4	Ò		/	@	&	+	:	9
5	2	Q	O	W	Y	À	,	^
6	"	_	-	.	6	4	Ì	Ù
7	*	€	\$	(?	=	\	%

Stavolta il messaggio "Natale è il 25 dicembre", non è "NATALEEIL25DICEMBRE" ma "NATALE È IL 25 DICEMBRE" (grazie alla tavola con più simboli) e la traduzione in cifra è

04333 - 13320 - 17412 - 34135 - 20415 - 03041 - 16350 - 51732 - 00031 - 7

Usando il codice binario e i numeri uniformati a 3 cifre si ottiene ...

000 100 011 011 011 - 001 011 011
 010 000 - 001 111 100 001 010 - 011
 100 001 011 101 - 010 000 010 001
 101 - 000 011 000 010 001 - 001 011
 011 101 000 - 101 001 111 011 010 -
 000 000 000 011 001 - 111

... e quindi i byte...

00010001 - 10110110 - 01011011 - 01000000 - 11111000 - 01010011
 10000101 - 11010100 - 00010001 - 10100001 - 10000100 - 01001011
 01110100 - 01010011 - 11011010 - 00000000 - 00110011 - 11000000

(dove si sono aggiunti 6 zeri alla fine per completare l'ottetto)

Ultima annotazione importante: per non confondere i simboli O (la vocale) e 0 (la cifra), conviene usare per lo zero un simbolo barrato come \emptyset .