Alcuni metodi di trasposizione /2

scheda di lavoro 3

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.

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

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

È importante osservare che il metodo di Sasso appena visto permette di creare sequenze numeriche a partire da sequenze letterali ma non rappresenta di per sé un sistema di cifratura.

Le trasposizioni a chiave

Introduciamo una prima tecnica che permette di cifrare una singola parola (o comunque testi molto brevi) mediante una chiave.

Passaggio 1
Supponiamo inizialmente di voler dover inviare una sola parola: "RITIRATA" (8 lettere). Per applicare il metodo servirà innanzitutto una sequenza numerica lunga quanto il messaggio stesso. Applichiamo il metodo di *Sasso* per trovarne una: utilizzando la parola AMERICA (di 7 lettere) otteniamo la chiave numerica $1-7-5-8-6-4-2-3$.

Passaggio 2
Costruiamo la seguente tabella:

Messaggio →	R	I	T	I	R	A	T	A
Chiave numerica →	1	7	5	8	6	4	2	3
Cifratura →								

Passaggio 3
La crittazione del messaggio consiste semplicemente nel rimescolamento delle lettere del messaggio secondo l'ordine indicato dalla sequenza numerica:

Messaggio →	R	I	T	I	R	A	T	A
Chiave numerica →	1	7	5	8	6	4	2	3
Cifratura →	**R**	**T**	**A**	**A**	**T**	**R**	**I**	**I**

È evidente che il metodo di trasposizione è del tutto inadatto a celare messaggi così brevi (basterebbe infatti cercare anagrammi sensati della stringa RTAATRII), si tratta però di una tecnica che, come vedremo, è facilmente trasferibile alle griglie di trasposizione e quindi a testi arbitrariamente lunghi. Vediamo altri esempi:

3.3) Cifra il messaggio "LICEOMAJORANA" con la chiave "ORAETLABORA"

Chiave letterale →	O	R	A	E	T	L	A	B	O	R	A	O	R
Messaggio →	L	I	C	E	O	M	A	J	O	R	A	N	A
Chiave numerica →													
Cifratura →													

Cimentiamoci ora con il problema inverso e mettiamoci nei panni del destinatario:

3.4) Decifra il messaggio cifrato `TEOEO – ARUMB – ENADT – DU` con la chiave “NONCEDUESENZATRE” (per brevità è già stata determinata la chiave numerici associata).

Chiave letterale →	N	O	N	C	E	D	U	E	S	E	N	Z	A	T	R	E	N
Messaggio →																	
Chiave numerica →	8	12	9	2	4	3	16	5	14	6	10	17	1	15	13	7	11
Cifratura →	**T**	**E**	**O**	**T**	**O**	**A**	**R**	**U**	**M**	**B**	**E**	**N**	**A**	**D**	**T**	**D**	**U**

La decifratura avviene in modo diverso dalla cifratura: in quest’ultimo caso le lettere si scrivono in sequenza, una dopo l’altra, nel primo caso è invece opportuno seguire l’ordine indicato dalla riga “Chiave numerica”: perché la `T` sia finita in prima posizione, essa doveva trovarsi proprio sopra il numero 1 della chiave:

Messaggio →													T				
Chiave numerica →	8	12	9	2	4	3	16	5	14	6	10	17	1	15	13	7	11
Cifratura →	**T**	**E**	**O**	**T**	**O**	**A**	**R**	**U**	**M**	**B**	**E**	**N**	**A**	**D**	**T**	**D**	**U**

Con un ragionamento identico si capisce che la `E` originariamente si trovava in quarta posizione (proprio sopra la casella del 2):

Messaggio →				E									T				
Chiave numerica →	8	12	9	2	4	3	16	5	14	6	10	17	1	15	13	7	11
Cifratura →	**T**	**E**	**O**	**T**	**O**	**A**	**R**	**U**	**M**	**B**	**E**	**N**	**A**	**D**	**T**	**D**	**U**

Proseguendo in questo modo si arriva al seguente messaggio:

Messaggio →	U	N	M	E	T	O	D	O	D	A	B	U	T	T	A	R	E
Chiave numerica →	8	12	9	2	4	3	16	5	14	6	10	17	1	15	13	7	11
(De)Cifratura →	**T**	**E**	**O**	**T**	**O**	**A**	**R**	**U**	**M**	**B**	**E**	**N**	**A**	**D**	**T**	**D**	**U**

Come vi sarete accorti, e come il contenuto del messaggio stesso suggerisce (“Un metodo da buttare”), questo modo di procedere è molto meno agevole della cifratura stessa. Esiste però una scorciatoia, che consiste nella creazione dello *Retrochiave*, concetto che ci tornerà utile anche negli sviluppi successivi. Senza farla troppo lunga, torniamo al messaggio cifrato `TEOEO – ARUMB – ENADT – DU` e supponiamo di cifrarlo nuovamente, stavolta con la chiave $13,4,6,5,8,\ldots$ mostrata in basso (i numeri della *retrochiave* e il nome stesso “retrochiave” verranno spiegati in seguito):

3.5) Cifra nuovamente il messaggio cifrato `TEOEO – ARUMB – ENADT – DU` con la nuova chiave numerica $13,4,6,5,8,10,16,1,3,11,17,2,15,9,14,7,12$.

Messaggio →	T	E	O	T	O	A	R	U	M	B	E	N	A	D	T	D	U
Retrochiave →	13	4	6	5	8	10	16	1	3	11	17	2	15	9	14	7	12
Decifratura →																	

Chiaramente la “retrochiave” è una particolare chiave che permette di decifrare cifrando.

Definizione
Dato un sistema di *trasposizione a chiave* che permette di passare da un messaggio in chiaro **A** ad un messaggio cifrato **B**, si chiama **retrochiave** la chiave che permette di ottenere **B** da **A** applicando lo stesso procedimento.

Vediamo un’altra magia della *retrochiave*: utilizziamo l’ultima trovata $(13,4,6,5,8,\ldots)$ come chiave per cifrare un messaggio nuovo, per esempio “Oggi è previsto sole”

Messaggio →	O	G	G	I	E	P	R	E	V	I	S	T	O	S	O	L	E
Chiave numerica →	13	4	6	5	8	10	16	1	3	11	17	2	15	9	14	7	12
Cifratura →	**E**	**T**	**V**	**G**	**I**	**G**	**L**	**E**	**S**	**P**	**I**	**E**	**O**	**O**	**O**	**R**	**S**

Indovinate un po’: quale sarà la *retroretrochiave*? Ovviamente la chiave iniziale! Per gli scettici non resta che provare:

3.6) Cifra nuovamente il messaggio ETVGI – GLESP – IEOOO – RS con la primissima chiave $8,12,9,2,4,3,16,5,14,6,10,17,1,15,13,7,11$ (quella derivata da “Non c’è due senza tre”).

Messaggio →	E	T	V	G	I	G	L	E	S	P	I	E	O	O	O	R	S
Chiave numerica →	8	12	9	2	4	3	16	5	14	6	10	17	1	15	13	7	11
(De)Cifratura →																	

Adesso è arrivato il momento di mettere alla prova la vostra creatività:

3.7) Inventa un sistema per ricostruire velocemente la *retrochiave* di una chiave:

Il “trucco” consiste nel cifrare non un messaggio scritto ma la semplice sequenza numerica 1,2,3,4…: il risultato sarà $CHIAVE -> RETROCHIAVE$ o se volete $RETROCHIAVE -> CHIAVE$ (vedi esempio in basso):

Messaggio →	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Chiave numerica →	8	12	9	2	4	3	16	5	14	6	10	17	1	15	13	7	11
Cifratura →	**13**	**4**	**6**	**5**	**8**	**10**	**16**	**1**	**3**	**11**	**17**	**2**	**15**	**9**	**14**	**7**	**12**

Messaggio →	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Chiave numerica →	13	4	6	5	8	10	16	1	3	11	17	2	15	9	14	7	12
Cifratura →	**8**	**12**	**9**	**2**	**4**	**3**	**16**	**5**	**14**	**6**	**10**	**17**	**1**	**15**	**13**	**7**	**11**

3.8a) Trova la *retrochiave* della seguente (ottenuta dalla frase “Se son rose fioriranno”):

Chiave numerica →	17	2	18	10	7	14	11	19	3	4	5	12	15	6	16	1	8	9	13
Retrochiave →																			

3.8b) Cifra con la chiave iniziale il messaggio

Messaggio →	I	L	M	E	S	S	A	G	G	E	R	O	E	P	R	O	N	T	O
Chiave numerica →	17	2	18	10	7	14	11	19	3	4	5	12	15	6	16	1	8	9	13
Cifratura →																			

3.8c) Mettiti nei panni del destinatario e decifra il messaggio con il metodo della *retrochiave* (ti toccherà ricopiare la retrochiave del punto **a** e la cifratura da **b**)

Cifratura →																			
Retrochiave →																			
(De)Cifratura →																			

3.9) Chiudiamo questo cappello introduttivo con una piccola attività, al confine tra crittografia ed enigmistica: per chiavi brevi è possibile inventare *retrochiavi* letterali (in modo da poter tenere a mente entrambe senza bisogno di alcun calcolo), come mostrato nel seguente esempio:

Chiave letterale →	E	U	L	E	R	O
Chiave numerica →	1	6	3	2	5	4
Messaggio →	1	2	3	4	5	6
Retrochiave →	1	4	3	6	5	2
Retrochiave letterale →	?	?	?	?	?	?

Come si vede a fianco, la *retrochiave* della chiave generata da Eulero è 1,4,3,6,5,2. Si tratta ora di trovare una parola di senso compiuto che generi proprio la sequenza *Sacco 1,4,3,6,5,2*.

Tra le tante possibilità cito **ANCONA**. Possiamo quindi dire che la chiave EULERO ha la *retrochiave* ANCONA (e viceversa).

Trova delle *retrochiavi* letterali per le seguenti chiavi da 5 e 6 lettere:

a) AMORE **b)** ISOLA **c)** GAUSS **d)** INIZIO **e)** ARRIVO

Vediamo ora come combinare le tecniche di trasposizione (ottenute con il rettangolo) con il sistema della *chiave*. Come al solito spieghiamo il procedimento mediante un esempio e iniziamo con la trasposizione a colonna (in pratica il metodo dello *scitale*) a cifrare il messaggio "La mia prima vera trasposizione con chiave", cioè LAMIAPRIMATRASPOSIZIONECONCHIAVE con la chiave LICEO.

Trasposizione a colonna **con chiave**

Procedimento	Esempio

1) La chiave stessa determina il numero di colonne. Scriviamo quindi nella prima riga LICEO (5 colonne) e calcoliamo la sequenza di *Sacco* associata.

L	I	C	E	O
4	3	1	2	5

2) Formiamo il rettangolo scrivendo il nostro messaggio sulle 5 colonne e ricordando di completare la figura se necessario (nel nostro caso abbiamo chiuso con le lettere HLA, evidentemente scollegate dal resto).

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

3) Possiamo ora considerare le colonne e finire la cifratura: invece di scorrerle in ordine, da sinistra a destra, seguiamo la numerazione indotta dalla chiave. Ne risulta il messaggio cifrato a fianco:

MESSAGGIO CIFRATO
(trasmesso in gruppi da 5)

MIRSZ – HIMAP – ILARE
AIELP – VRSNA – ATOOA

Per decrittare il messaggio sottostante, si può determinare la retrochiave di 4,3,1,2,5 o, più semplicemente, incolonnare le lettere secondo l'ordine indotto dalla chiave stessa (vedi a fianco l'inizio del procedimento)

MESSAGGIO DA DECIFRARE
(trasmesso in gruppi da 5)

MIRSZ – HIMAP – ILARE
AIELP – VRSNA – ATOOA

L	I	C	E	O
4	3	1	2	5
		M		
		I		
		R		
		S		
		Z		
		…		

Il metodo appena vista si presta bene a rimescolamenti a *colonna* o *serpentina*, male per sistemi più complessi come lo *ZigZag*. In casi del genere non basta "leggere" il codice a seconda del numero delle colonna, è necessario scambiare fisicamente le colonne fra loro e il prossimo esempio mostra il procedimento: il messaggio è di nuovo "La mia prima vera trasposizione con chiave", cioè `LAMIAPRIMATRASPOSIZIONECONCHIAVE` con la chiave `LICEO`.

Trasposizione a ZigZag **con chiave** (*il procedimento è applicabile a qualsiasi rimescolamento rettangolare*)

Procedimento (cifratura)	Esempio

1) La chiave stessa determina il numero di colonne. Scriviamo quindi nella prima riga `LICEO` (5 colonne) e calcoliamo la sequenza di *Sacco* associata.

L	I	C	E	O
4	3	1	2	5

2) Formiamo il rettangolo scrivendo il nostro messaggio sulle 5 colonne e ricordando di completare la figura se necessario (nel nostro caso abbiamo chiuso con le lettere `HLA`, evidentemente scollegate dal resto).

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

3) Stavolta riordiniamo le colonne del rettangolo secondo la chiave numerica.

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

4) Possiamo ora percorrere il rettangolo secondo lo schema prefissato (in questo caso lo *ZigZag*). Otteniamo così…

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

MESSAGGIO CIFRATO
(trasmesso in gruppi da 5)

`MIIRM – ALRAS – ZPEPA`
`AVAIH – LIRTO – SENOA`

Stavolta la decrittazione è leggermente più lunga.

Procedimento (decifratura)	Esempio

MESSAGGIO DA DECIFRARE (con chiave *LICEO*)
(trasmesso in gruppi da 5)

`MIIRM – ALRAS – ZPEPA`
`AVAIH – LIRTO – SENOA`

L	I	C	E	O
4	3	1	2	5

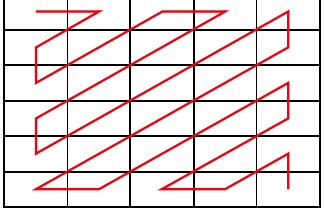
1) Prima di tutto calcoliamo la *retrochiave* della nostra chiave. Applicando il sistema vista in precedenza, riordiniamo la sequenza banale 1,2,3,4,5 secondo la chiave 4,3,1,2,5 ("LICEO"): il risultato è la *retrochiave*, nel nostro caso 3,4,2,1,5.

L	I	C	E	O	
4	3	1	2	5	Chiave
1	2	3	4	5	
					Retrochiave

L	I	C	E	O	
4	3	1	2	5	Chiave
1	2	3	4	5	
3	**4**	**2**	**1**	**5**	Retrochiave

3) Disegniamo il rettangolo con le misure esatte (il numero delle colonne è dato dalla chiave, il numero di righe si inferisce dal messaggio stesso). Approntiamo lo schema a ZigZag, premettendo la riga con la retrochiave.

3	4	2	1	5	retrochiave



4) Ricopiamo le lettere nel rettangolo secondo l'ordine prefissato.

3	4	2	1	5	retrochiave
M	I	A	L	A	
I	M	R	P	A	
R	A	E	V	T	
S	P	A	R	O	
Z	I	I	S	O	
H	L	E	N	A	

5) Scambiamo fra loro le colonne secondo l'ordine indicato dalla *retrochiave*. Leggendo in orizzontale, apparirà il messaggio in chiaro:

LAMIAPRIMATRASPOSIZIONECONCHIAVE

1	2	3	4	5	retrochiave
L	A	M	I	A	
P	R	I	M	A	
V	E	R	A	T	
R	A	S	P	O	
S	I	Z	I	O	
N	E	H	L	A	

3.10) Esegui le seguenti cifrature:

	Messaggio	Chiave	Trasposizione
a)	Il liceo Majorana è una scuola di Spinaceto	CERCHIO	A ZigZag
b)	Il nemico sta avanzando da settentrione	LECCE	A colonna
c)	Probabili agenti infiltrati al reparto analisi	FIORE	A ZigZag
d)	Domani interroga la prof di Latino	SCUOLA	A colonna