Il cifrario di Cesare

Marina Cazzola

15 marzo 2023

Una versione interattiva di questo documento è qui disponibile: WIMS : Numeri e codici

1 Cifrare un messaggio

Il problema che abbiamo è questo: abbiamo un messaggio importantissimo che vogliamo inviare ai nostri amici più cari. Ma il messaggio è segreto: vogliamo che *solo* i nostri amici siano in grado di leggerlo e che *spioni* curiosi restino a bocca asciutta!
Questo problema è molto comune e fin dall'antichità si è provato a risolverlo in vari modi.
Un esempio storico ci viene raccontato da *Svetonio* (69 circa – 122 circa) nelle *Vitae Caesarorum*, libro in cui viene raccontata la storia del grande Giulio Cesare. Quando Cesare doveva inviare un messaggio, che conteneva importanti informazioni militari segrete, sostituiva a ogni lettera del messaggio da inviare la lettera che la segue di 3 posti. Cioè alla lettera "A" sostituiva la lettera "D", alla "B" la lettera "E", e così via.
Non è difficile riflettere sul fatto che un sistema analogo si può ottenere spostando ogni lettera di un numero prefissato qualsiasi di posti. Nelle prossime pagine vedremo bene come funziona questo meccanismo, che viene ricordato proprio come *Cifrario di Cesare*.

Il problema di decifrare messaggi per trasmetterli in segretezza è una questione ancora attuale ai giorni nostri. Anzi, le tecniche moderne permettono non solo di ottenere questa segretezza, ma permettono anche di verificare che il messaggio non si sia *rovinato* durante la trasmissione. Ritroviamo queste tecniche nelle trasmissioni telefoniche e televisive (per cui spesso serve un *decoder*, cioè un *decifratore*), nei codici dei Bancomat e delle carte di credito, e in tante altre situazioni.
Ma questa è un'altra storia... proveremo a dare qualche idea proprio alla fine di questo documento.

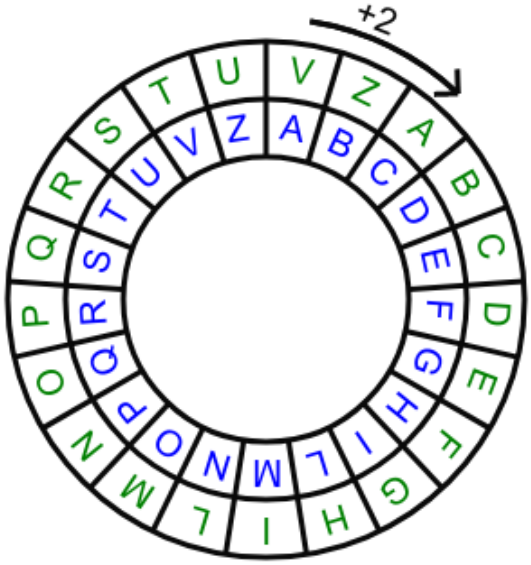
1.1 Come cifrare?

Se disponiamo le lettere dell'alfabeto in cerchio, possiamo prendere a caso un numero, che per brevità indicheremo con la lettera k, e spostare tutte le lettere avanti di k posizioni.

Esempio 1

Per esempio, se scegliamo $k = 2$, la figura ci mostra come la lettera "A" viene spostata avanti di due posti, e si trova quindi al posto della "C", la lettera "B" va al posto della "D", la "C" al posto della "E", e così via.
Dobbiamo immaginarci le lettere disposte in cerchio, così quando arriviamo alla fine (e dobbiamo spostare la "Z" in avanti di due posizioni) non dobbiamo far altro che ricominciare (la lettera "Z" si trova quindi al posto della "B").

In questa figura puoi vedere come si spostano le lettere quando $k = 2$.



Se abbiamo un messaggio che vogliamo mantenere segreto, in modo che solo i nostri amici siano in grado di leggerlo, possiamo cifrarlo scegliendo un numero k (la "chiave") e spostando le lettere in avanti di k posti.

Esempio 2

Per esempio se scegliamo $k = 2$ e vogliamo cifrare la parola "CASA", al posto della "C" scriviamo "E", al posto della "A" scriviamo "C" e al posto della "S" scriviamo... (indovinate un po'...) scriviamo "U". Quindi invece di "CASA", scriviamo "ECUC".

1.2 Mettiti alla prova

Un primo passo per capire come funziona questa procedura di *codifica* è quello di *provare a cifrare un messaggio* molto breve: un messaggio formato da una sola lettera.

Esercizio interattivo 1

WIMS : Cifra una lettera 1: ti viene data una lettera e la chiave k e devi cifrarla. Puoi aiutarti con le ruote che ho disegnato per te.
WIMS : Cifra una lettera 2: un pochino più difficile, ora devi immaginarti da solo la ruota che muove le lettere.

Benissimo, se hai capito come codificare le singole lettere, ora sei pronto per codificare alcune semplici parole

Esercizio interattivo 2

WIMS : Cifra una parola 1: ti viene data una parola e la chiave k e devi cifrarla. Puoi aiutarti con le ruote che ho disegnato per te.
WIMS : Cifra una parola 2: un pochino più difficile, ora devi immaginarti da solo la ruota che muove le lettere.

E ora puoi provare a cifrare messaggi un po' più lunghi.

Esercizio interattivo 3

WIMS : Cifra un messaggio 1: ti viene data una frase e la chiave k e devi cifrarla. Puoi aiutarti con le ruote che ho disegnato per te.
WIMS : Cifra un messaggio 2: un pochino più difficile, ora devi immaginarti da solo la ruota che muove le lettere.

2 Decifrare un messaggio

Ora che abbiamo capito come si fa a cifrare un messaggio, mettiamoci nei panni dei nostri amici che lo ricevono. Si troveranno davanti un testo incomprensibile come questo:

Esempio 3

Grruxg or haxgzzotu joyzkyk o yauo vgtto gr yurk vkx xgyioamgxro, k yo vuyk g magxjgxk jo wag k jo rg yk vkx igyu gbkyyk vuzazu yiuxmkxk ya wakrrg ossktyg yvogtgzg j'giwag atg voiiurg hgxinkzzg iut at usotu jktzxu. Sg juvu gbkx magxjgzu hkt hktk, tut bojk grzxu jotgtfo g yk ink iokru, sgxk k wagrink bkrg jo hgyzosktzu, sg iuyo rutzgtg rutzgtg, ink vgxkbg atg suyig.

Come si fa a decifrarlo, cioè a capire che cosa c'è scritto?

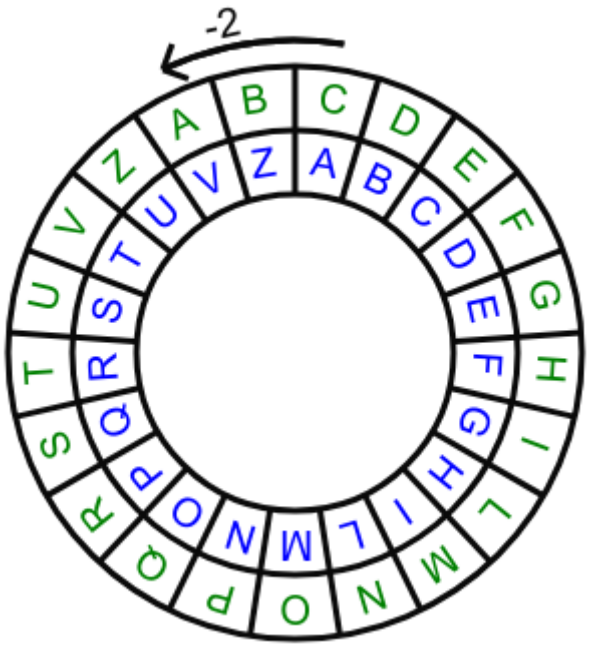
2.1 Come decifrare?

Se sappiamo che il messaggio è stato cifrato con il metodo che abbiamo appena studiato, quello che dobbiamo fare è trovare qual è il valore di k che è stato usato per codificare il messaggio e *seguire la procedura di cifratura al contrario*!

Esempio 4

Se sappiamo che il messaggio è stato cifrato utilizzando la chiave $k = 2$, cioè spostando *in avanti* le lettere di due posti, quello che dobbiamo fare è *riportare indietro* le lettere di due posti, come si può vedere nella ruota disegnata sotto. Per ricordarci che stiamo spostando le lettere in senso contrario, anziché scrivere $k = 2$, scriviamo $k = -2$.
Nell'esempio che abbiamo visto all'inizio, la parola "CASA" una volta cifrata con $k = 2$ diventa la parola "ECUC".
Chi riceve il messaggio "ECUC" deve andare a cercare, nella ruota qui sotto, dove è finita la lettera "E" e scopre che è finita al posto della "C". Questo significa che al posto della "E" dovremmo leggere "C". In modo analogo, al posto di "C" dobbiamo leggere "A", al posto di "U" dobbiamo leggere "S" e, di nuovo, al posto di "C" dobbiamo leggere "A". Ecco che siamo tornati alla parola "CASA".

In questa figura puoi vedere come si spostano le lettere quando $k = -2$.



2.2 Mettiti alla prova

Anche in questo caso, per capire bene come funziona questa procedura di "decodifica" il modo migliore è quello di *provare a decifrare i messaggi*. Cominciamo con un messaggio molto breve: un messaggio formato da una sola lettera.

Esercizio interattivo 4

WIMS : Decifra una lettera 1: ti viene data una lettera e la chiave k e devi decifrarla. Puoi aiutarti con le ruote che ho disegnato per te.
WIMS : Decifra una lettera 2: un pochino più difficile, ora devi immaginarti da solo la ruota che muove le lettere.

Benissimo, se hai capito come decodificare le singole lettere, ora sei pronto per decodificare alcune semplici parole

Esercizio interattivo 5

WIMS : Decifra una parola 1: ti viene data una parola e la chiave k e devi cifrarla. Puoi aiutarti con le ruote che ho disegnato per te.
WIMS : Decifra una parola 2: un pochino più difficile, ora devi immaginarti da solo la ruota che muove le lettere.

E ora puoi provare a decifrare messaggi un po' più lunghi.

Esercizio interattivo 6

WIMS : Decifra un messaggio 1: ti viene data una frase e la chiave k e devi decifrarla. Puoi aiutarti con le ruote che ho disegnato per te.
WIMS : Decifra un messaggio 2: un pochino più difficile, ora devi immaginarti da solo la ruota che muove le lettere.

3 Una precisazione

Fino a qui abbiamo considerato l'alfabeto Italiano a cui siamo abituati (ABCDEFGHILMNOPQRSTUVZ: 21 lettere). Sappiamo però che sono sempre più utilizzate nella nostra lingua parole che contengono anche altre lettere (per esempio pensiamo alla parola "WEEKEND"). Tutto quello che abbiamo fatto funziona perfettamente anche se utilizziamo un alfabeto con queste lettere aggiunte (in tutto 26 lettere).

Esercizio interattivo 7

WIMS : Cifra una lettera utilizzando l'alfabeto completo con 26 lettere.
WIMS : Decifra una lettera utilizzando l'alfabeto completo con 26 lettere.

4 Un gioco

Quello che abbiamo visto fino a ora è un metodo di cifratura particolare.
Si possono utilizzare metodi di cifratura diversi: la cosa importante è avere una regola per *sostituire una lettera con un'altra*, ma questa regola deve anche permettere al destinatario del messaggio di costruire la regola inversa per *tornare indietro* quando si vuole decifrare il messaggio.
In questi giochi che ti indichiamo qui sotto potrai sperimentare il compito di decifrare messaggi che sono stati cifrati con metodi diversi.

Esercizio interattivo 8

Il cifrario di Cesare

- WIMS : Testo lungo (più facile)
- WIMS : Testo breve (più difficile)

Esercizio interattivo 9

Altri metodi di cifratura

- WIMS : Livello 1
- WIMS : Livello 2
- WIMS : Livello 3
- WIMS : Livello 4
- WIMS : Livello 5
- WIMS : Livello 6

5 Un problema

Concludiamo questa parte sulla codifica e decodifica dei messaggi con un problema difficilissimo:

29. IL MESSAGGIO PER MARZIO

Il generale romano Giulio Cesare era solito inviare i messaggi ai suoi ufficiali in modo che le spie nemiche non potessero comprenderli. Quando voleva scrivere un messaggio prendeva un disco come quello disegnato qui sotto e cambiava ciascuna lettera con il numero scritto sotto.
Se il numero era pari lo sostituiva con il secondo numero dispari che lo segue in senso orario nel disco; se il numero era dispari lo sostituiva con il secondo numero pari che lo segue ancora nel disco; poi cambiava i numeri ottenuti in lettere e spediva il nuovo testo.
In una sera piovosa di non si sa bene quale anno mandò questo messaggio all'ufficiale Marzio, appostato con l'esercito in un luogo strategico.

G R P D Q N D O Z U D P R Q Z R

Quando Marzio dovrà aspettarsi l'attacco dei nemici?

Fonte: AAVV, La formica e il Miele: 30 giochi per ragazze e ragazzi svegli, Mimesis, 2005.

6 Correzione degli errori

Le tecniche moderne di cifratura permettono anche di verificare che il messaggio non si sia *rovinato* durante la trasmissione, cioè permettono di *correggere* gli errori.
Qui un semplice esempio di cosa questo significhi.

Esercizio interattivo 10

WIMS : Sette domande e una bugia: pensa un numero tra 0 e 15 e rispondi alle domande, mentendo *al massimo una volta*. Non solo è possibile indovinare il numero che hai pensato, ma è anche possibile capire se hai mentito a una di queste domande e a quale domanda hai mentito.

6.1 Come funziona?

L'esempio che abbiamo mostrato si basa su due principi, che ora ti raccontiamo nei prossimi due paragrafi.

6.1.1 La scrittura dei numeri in base 2

La scrittura dei numeri che siamo abituati a utilizzare è chiamata *scrittura posizionale in base 10*. Questo significa che quando scriviamo per esempio il numero 27, la *cifra* 2 sta a indicare che abbiamo due *decine*, cioè che abbiamo raccolto parte delle unità in due gruppi da 10. La *cifra* 7 invece indica che sono rimaste 7 *unità* che *avanzano* e non sono abbastanza per formare un gruppo da 10.

Esercizio interattivo 11

WIMS : Decine e unità (1) Raggruppa le decine e le unità e dimmi quanti sono i cubetti.
WIMS : Decine e unità (2) quanti sono i gettoni? Per contarli raggruppali in decine e unità.
WIMS : Fai corrispondere i numeri conta i gettoni e falli corrispondere ai numeri scritti in cifre.

Quando scriviamo per esempio 243, oltre alle decine, utilizziamo anche le *centinaia*: la cifra 2 sta a indicare che abbiamo 2 grupponi formati da 10 gruppi da 10. E 10 gruppi da 10 significa che abbiamo 100 unità. La cifra 4 rappresenta ancora le *decine*, cioè gruppi da 10 unità e infine la cifra 3 rappresenta le *unità* che avanzano e non sono abbastanza per formare un gruppo da 10.

Esercizio interattivo 12

WIMS : Centinaia, decine e unità Raggruppa le centinaia, le decine e le unità e dimmi quanti sono i cubetti.

E così via introducendo anche le *migliaia*

Esercizio interattivo 13

WIMS : Migliaia, centinaia, decine e unità Raggruppa le migliaia, le centinaia, le decine e le unità e dimmi quanti sono i cubetti.

Quello che fino a qui abbiamo fatto raggruppando *a dieci a dieci* (cioè formando le *decine*, le *centinaia* e le *migliaia*), può essere fatto formando gruppi di altre grandezze (a due a due, a tre a tre, ...).

Esercizio interattivo 14

WIMS : Raggruppa i cubetti (1) Raggruppa i cubetti e dimmi quanti sono.
WIMS : Raggruppa i cubetti (2) Raggruppa i cubetti e dimmi quanti sono.
WIMS : Raggruppa i cubetti (3) Raggruppa i cubetti e dimmi quanti sono.

Il linguaggio dei computer si basa soprattutto sui raggruppamenti *a due a due*, utilizzando cioè la *scrittura posizionale in base 2*, detta anche *scrittura binaria* del numero.

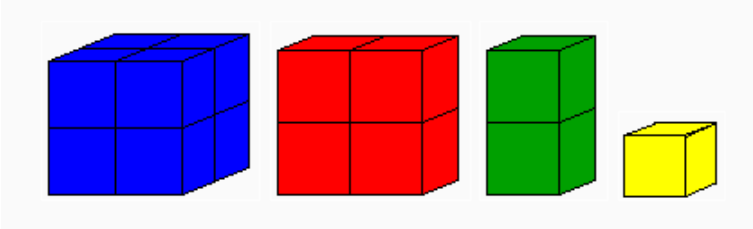
Esercizio interattivo 15

WIMS : Trova i blocchi Ti darò un numero e tu dovrai selezionare “blocchi di due in due” per formare quel numero.

Tutti i numeri da 0 a 15 possono essere scritti utilizzando la scrittura posizionale in base 2 con 4 cifre.

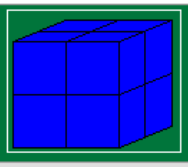
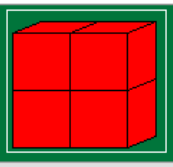
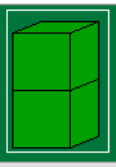
Esempio 5

Per esempio il numero **15** può essere scritto in base 2 con le cifre **1**, **1**, **1**, **1**.



Maggiori informazioni

Ecco qui una tabella completa per tutti i numeri da 0 a 15

numero				
0	0	0	0	0
1	0	0	0	1
2	0	0	1	0
3	0	0	1	1
4	0	1	0	0
5	0	1	0	1
6	0	1	1	0
7	0	1	1	1
8	1	0	0	0
9	1	0	0	1
10	1	0	1	0
11	1	0	1	1
12	1	1	0	0
13	1	1	0	1
14	1	1	1	0
15	1	1	1	1

6.1.2 L’invio di informazioni superflue

Come abbiamo visto nel paragrafo precedente i numeri da 0 a 15 possono essere scritti utilizzando 4 cifre nella scrittura posizionale in base 2.

Le prime 4 domande del gioco servono proprio a individuare queste 4 cifre

1. Il numero che hai pensato è maggiore di 7 (e diverso da 7): se si risponde sì significa che la prima cifra del numero, in notazione binaria, è 1 (in altre parole nella scrittura "a blocchi" serve un blocco blu formato da 8 cubetti), altrimenti la prima cifra è 0 (verificate!).

2. È uno tra i numeri 4, 5, 6, 7, 12, 13, 14, 15: se si risponde sì significa che la seconda cifra del numero, in notazione binaria, è 1 (quindi serve un blocco rosso formato da 4 cubetti), altrimenti la seconda cifra è 0.

3. È uno tra i numeri 2, 3, 6, 7, 10, 11, 14, 15: se si risponde sì significa che la terza cifra del numero, in notazione binaria, è 1 (quindi serve un blocco verde formato da 2 cubetti), altrimenti la terza cifra è 0.

4. È dispari: se si risponde sì significa che l'ultima cifra del numero, in notazione binaria, è 1 (quindi serve un blocco giallo formato da un unico cubetto), altrimenti è 0.

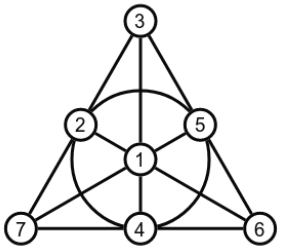
Per esempio, il numero 12 nella scrittura posizionale in base 2 si scrive 1100 e se rispondete alle quattro domande (senza mentire!) per il numero 12 vi accorgete che le risposte sono rispettivamente *sì*, *sì*, *no*, *no* (a ogni 1 corrisponde un *sì*, a ogni 0 corrisponde un *no*).
A che cosa servono allora le tre domande successive?

5. È uno tra i numeri 2, 3, 4, 5, 8, 9, 14, 15

6. È uno tra i numeri 1, 2, 4, 7, 9, 10, 12, 15

7. È uno tra i numeri 1, 3, 4, 6, 8, 10, 13, 15

Le domande dalla 5 alla 7 sono informazioni *inutili* se non ci sono menzogne, ma servono proprio per capire se c'è stata una menzogna!
Per capire se c'è stata una menzogna conviene segnarsi le risposte alle sette domande utilizzando uno schema un po' particolare. Nel diagramma che ti copio qui sotto colora i numeri che corrispondono alle domande a cui hai risposto sì



Esercizio 1. Per i numeri da 0 a 15, che sono quelli utilizzati nel nostro gioco, prova a compilare il diagramma rispondendo alle 7 domande **senza menzogne!** e colorando i numeri che corrispondono alle domande a cui hai risposto sì.
Che cosa osservi sui diagrammi così creati?

Maggiori informazioni

In caso di risposte tutte sincere, ci sono 4 possibilità:

- tutti i pallini sono bianchi;
- tutti i pallini sono colorati;
- 4 pallini sono bianchi e 3 i pallini colorati sono allineati o disposti sulla circonferenza;
- 4 pallini sono colorati e 3 i pallini bianchi sono allineati o disposti sulla circonferenza.

Ora che hai visto quali sono le caratteristiche dei diagrammi nel caso non ci siano menzogne, ti raccontiamo cosa succede nel caso ci sia una menzogna (ma **una sola** menzogna!). In questo c'è un unico modo di cambiare un punto per ricondursi ad una delle 4 possibilità elencate sopra, quindi c'è un solo modo per *correggere* la risposta sbagliata.
Una volta corretto l'eventuale errore, il numero che hai pensato in forma binaria si ottiene guardando le risposte alle prime quattro domande, cioè i pallini corrispondenti alle posizioni 1, 2, 3, 4 e scrivendo una cifra 1 per ogni pallino colorato e 0 per ogni pallino bianco.

Esercizio interattivo 16

WIMS : Prova a indovinare Ti aiuterò a disegnare il diagramma. Puoi anche lavorare in coppia con un tuo compagno.

Credits

Attività sui codici a cura di Daniela Bertacchi, Marina Cazzola, Francesca dalla Volta e Veronica Felli. Queste attività sono state proposte la prima volta nell'ambito dell'evento *Un giorno tra le scienziate in Bicocca* per l'iniziativa *I talenti delle donne* promossa dal Comune di Milano.
Successive modifiche sono state poi introdotte in questo documento.