Segreti, codici e spie

Jadranka Santi*

Introduzione

Il Liceo Pedagogico ha il compito di iniziare a formare i futuri insegnanti di scuola primaria, fornendo agli allievi una vasta cultura nei campi delle scienze dell'educazione, della didattica e della pedagogia. Alle lezioni teoriche vengono sempre affiancate anche lezioni pratiche, in cui i ragazzi, attraverso la preparazione di unità didattiche ed il tirocinio in classe, hanno la possibilità di applicare le conoscenze acquisite.

Partendo da questo presupposto, ho, in primo luogo, proposto agli studenti di seconda, con cui ho deciso di partecipare alla VI edizione della manifestazione "La matematica dei ragazzi", l'analisi di un lavoro svolto in precedenza da alcuni membri del Nucleo di Ricerca Didattica (cfr. Zuccheri, 1992; Sgarro & Zuccheri, 1992; Marceddu, 2002) al fine di familiarizzarli con una situazione concreta di insegnamento della matematica attraverso la crittografia nella scuola dell'obbligo. La mia scelta è ricaduta sulla seconda classe poiché insegnavo loro matematica e fisica per il secondo anno di seguito e quindi li conoscevo bene. Gli studenti di questa classe, per di più, erano attratti dalla crittografia, che avevano "scoperto" nel momento in cui una delle ragazze aveva iniziato a scarabocchiare sul banco messaggi segreti usando un codice trovato su una rivista.

Dopo aver appreso che la crittografia può essere utilizzata nell'insegnamento della matematica a vari livelli, con diversi obiettivi e finalità, siamo passati

all'approfondimento del mondo affascinante dei codici segreti, scoprendo, oltre al cifrario a rotazione o di Cesare, anche quello a sostituzione completa. Studiando quest'ultimo, abbiamo svolto osservazioni sperimentali sulla struttura statistica dell'italiano, dello sloveno e dell'inglese scritti e abbiamo costruito degli istogrammi delle frequenze delle lettere nelle tre lingue, confrontando alla fine le statistiche ottenute con quelle riportate dai testi. Abbiamo infine sfruttato quanto avevamo imparato per risolvere alcuni schemi di parole crociate crittografate della *Settimana Enigmistica*.

In un secondo momento, i ragazzi sono stati lasciati allo sbaraglio nel decidere come presentare quanto appreso alla manifestazione.

Dopo un primo momento di incertezza, gli studenti hanno deciso di presentare quanto da loro acquisito in due laboratori distinti, l'uno rivolto ai bambini delle scuole elementari e l'altro ai ragazzi delle medie inferiori. Nel primo hanno presentato il cifrario a rotazione, illustrando il momento storico della sua nascita e facendo lavorare i bambini su esempi concreti di cifrazione e decifrazione. Nel secondo, invece, hanno proposto il cifrario a sostituzione completa, presentando il quadro storico in cui esso nacque e gli istogrammi delle frequenze delle lettere in sloveno, italiano e inglese. Alla fine di questo laboratorio i ragazzi hanno presentato la soluzione di un crittogramma tratto dalla *Settimana Enigmistica*, cercando di coinvolgere il più possibile il pubblico.

A differenza della maggior parte degli altri laboratori presenti alla manifestazione, che erano organizzati per postazioni, i ragazzi della mia classe, essendo solamente in cinque, hanno deciso di esporre gli argomenti in modo frontale, presentandoli a turno. Ciò ha richiesto loro un notevole sforzo, poiché dovevano essere in grado di sostenere un discorso per ben venti minuti. In ogni caso, tutti erano preparati a presentare entrambi i laboratori, sia in italiano sia in sloveno.

Bisogna infine notare che i ragazzi hanno lavorato con molto entusiasmo, rimanendo spesso a scuola anche in orario extracurricolare. Infatti, la costruzione dei cartelloni, tutti bilingui, ha richiesto parecchie ore di lavoro.

Il cifrario di Cesare

Attraverso la *cifratura* si vuole trascrivere un testo in modo che questo risulti leggibile solamente alla persona cui è rivolto.

La *crittologia*, scienza che studia le scritture segrete, è composta da due rami: la *crittografia* studia i diversi modi di cifrare un messaggio, mentre la *crittoanalisi* si occupa del contrario, ossia di come decifrare un messaggio di cui non conosciamo la chiave, di come cioè "rompere" la chiave del messaggio.

Entrambi i rami hanno, da tempi remoti, un ruolo fondamentale sul piano diplomatico e politico. Gli inizi dell'uso della crittografia risalgono a prima dell'era cristiana. Nei secoli si sono sviluppati innumerevoli modi per occultare un

messaggio. L'intercettazione della posta diplomatica era una pratica comune, non solamente in tempo di guerra. Nelle corti esistevano le cosiddette "stanze nere", in cui si tentava di risolvere i messaggi trascritti o intercettati.

Uno dei casi storici più famosi risale al 1589, quando, durante la guerra franco-spagnola, il matematico francese Vieté, su ordine del re, riuscì a trovare la chiave della scrittura segreta usata dagli Spagnoli nei loro piani di guerra. La scrittura era, per l'epoca, così complicata che gli Spagnoli si sentivano totalmente al sicuro. Oggi la sua analisi, grazie all'uso del computer, probabilmente non sarebbe un osso troppo duro. All'epoca, però, lasciò talmente sbigottiti gli Spagnoli che essi si lamentarono con il Papa per i presunti poteri magici usati dai Francesi durante la guerra.

Nell'era dei computer la crittografia ha un ruolo sempre maggiore per l'importanza che risulta avere la conservazione di dati personali e d'affari. La crittografia viene spesso utilizzata anche nei giochi d'azzardo, per evitare imbrogli con falsi.

I crittogrammi più semplici sono basati sulle permutazioni delle lettere della lingua in cui sono scritti. Questo vuol dire che si scambia, attraverso una regola ben precisa, ogni singola lettera dell'alfabeto con un'altra lettera definita. Un metodo di questo tipo venne impiegato da Giulio Cesare. I suoi messaggi erano cifrati in modo che ogni singola lettera fosse sostituita da quella che la segue di tre posizioni nell'alfabeto e le ultime tre lettere dell'alfabeto con le prime tre, scritte nel loro ordine usuale. Nell'alfabeto italiano esteso, il cifrario di Cesare può essere rappresentato mediante la tabella seguente:

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
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

Come esempio di utilizzo di tale cifrario, consideriamo la seguente trascrizione:

– messaggio in chiaro: COSÌ CIFRAVA CESARE

– messaggio trascritto in cifra: FRVLFLIUDYDFHVDUH

Nella trascrizione, abbiamo volutamente omesso gli spazi tra le parole, in modo che un potenziale intercettatore avesse maggiore difficoltà nella decrittazione del messaggio. Con ciò, abbiamo presupposto che la frase COSÌ CIFRAVA CESARE fosse abbastanza familiare al destinatario, che avrebbe aggiunto gli spazi senza alcuna difficoltà.

Tre, ovviamente, non è un numero magico. Le lettere dell'alfabeto si possono traslare, generalizzando il metodo usato da Cesare, per un numero qualunque di posti. I cambiamenti significativi si ottengono però per traslazioni (di almeno 1 posto e) di meno di 26 posti.

La procedura può venir descritta anche con una formula matematica, se sostituiamo, ad esempio, le lettere dell'alfabeto con i numeri che indicano la loro posizione alfabetica. La chiave è il complesso di informazioni che serve per decifrare un messaggio. In questo caso, noto tutto il contesto, si può dire che la chiave per decifrare una tale scrittura è un numero d tale che $0 \leq d \leq 25$. Infatti, la trasformata di una qualunque lettera di posto n è quella di posto $n + d$. Bisogna però ricorrere all'addizione modulo 26, quindi risulta più pratico servirsi di uno strumento, il cifrario a rotazione, che verrà descritto di seguito.

Questo tipo di cifratura, anche nel caso di d qualsiasi, viene denominato cifratura di Cesare ed è molto semplice da utilizzare, ma anche da "forzare". Se la chiave *d* viene cambiata molto spesso, il metodo diventa più sicuro. Abbiamo però in questo caso la difficoltà di far recapitare più volte la chiave al destinatario. Se l'intercettatore capisce che stiamo usando la cifratura di Cesare, non gli resta che provare tutte le 26 possibili chiavi per decifrare il messaggio. Con molta probabilità ci sarà solamente una chiave che produrrà un messaggio in chiaro che abbia senso.

Il problema maggiore è costituito dallo spiegare i concetti appena esposti ai bambini delle scuole elementari. Per fare ciò, abbiamo in primo luogo costruito un cifrario a rotazione (cfr. Figura 1), costituito da due dischi sovrapposti, l'uno più grande e l'altro più piccolo. Il disco maggiore è fisso, quello minore è libero di ruotare.

I due dischi sono stati divisi in 26 spicchi. Sul disco maggiore abbiamo scritto le lettere dell'alfabeto italiano esteso, sul disco più piccolo l'alfabeto per cifrare i messaggi. Nel nostro caso abbiamo scelto un alfabeto costituito da simboli di nostra invenzione, ma ritenuti familiari per i bambini. In questo modo a ogni lettera si associa un simbolo e il simbolo che sta sotto alla lettera A costituisce la *chiave* del messaggio segreto. Nei lavori in precedenza svolti dai componenti del Nucleo di Ricerca Didattica (cfr. Zuccheri, 1992) le lettere venivano codificate mediante numeri, anche perché questo stratagemma portava alle applicazioni nel campo dell'aritmetica modulare, ma ai ragazzi della mia classe pareva più simpatico farlo con i simboli e, in questo caso, non si pensava di arrivare a trattare tale argomento.

Una volta costruita la ruota, si è cercato il modo più appropriato per comunicare con i bambini. I ragazzi hanno constatato che i bambini sono di solito attratti dalle favole e che quindi il modo migliore sarebbe stato quello di inventarsi una favola, come la seguente:

> "Una volta in un paese molto lontano viveva una principessa bellissima, estremamente intelligente e coraggiosa. Un giorno sfortunato la principessa venne rapita da

un mago cattivo che la rinchiuse in una cella in cima alla sua torre. Il mago però non sapeva che la principessa comunicava con un principe attraverso dei messaggi segreti. La principessa e il principe usavano, per scambiarsi messaggi, il cifrario di Cesare. Ognuno di loro era in possesso del disco cifrante e conosceva la chiave per decifrare i messaggi. Il disco era in realtà costituito da due dischi sovrapposti, uno più grande e uno più piccolo, che si muoveva rispetto al disco più grande. Sul disco esterno c'erano le lettere della lingua in cui si scriveva il messaggio e su quello più piccolo i simboli per scrivere il messaggio segreto. Per comporre il messaggio segreto serviva anche una chiave, che è costituita dal simbolo posto sotto la lettera A. La nostra principessa scelse ♡.
Una volta posto il simbolo stabilito sotto la lettera A, si doveva sostituire ogni lettera del messaggio con il simbolo che compare sotto la lettera sul disco piccolo. Il suo messaggio, scritto in italiano, era: SOS SONO PRIGIONIERA e, cifrato

La principessa consegnò il messaggio a un piccione viaggiatore, ma il mago, che la stava controllando, riuscì a intercettarlo. Lui, però, non essendo in possesso della chiave per decifrare il messaggio, dovette procedere per tentativi. Prima provò A = ☾ e ottenne: VRV VRQR SULJLRQLHUD.

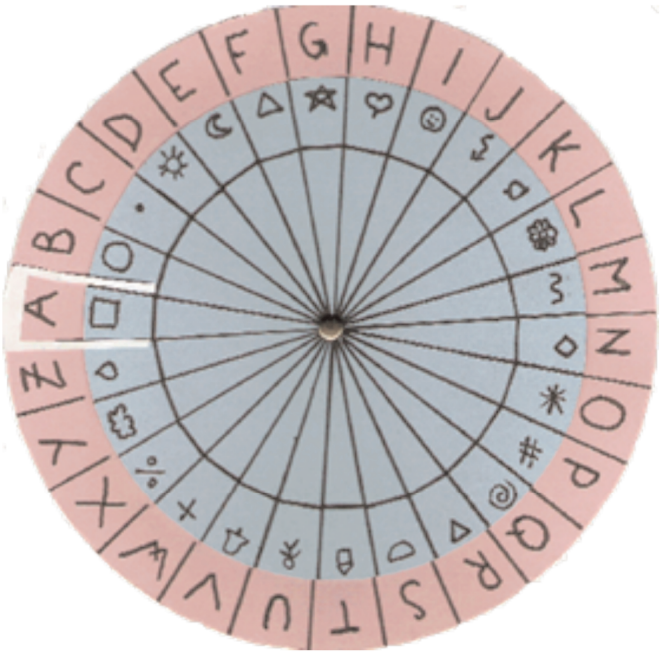

Figure 1 e 2
Cifrario di Cesare

La nostra storia però non finisce qui... La principessa, rendendosi conto della possibilità che il mago intercettasse il messaggio, ne inviò subito un secondo, che il mago, essendo occupato con la decifrazione del primo, non riuscì a captare. Così il principe poté venire a salvarla.

Durante lo svolgimento del meeting "La matematica dei ragazzi", quindi, la visita di ogni classe al nostro laboratorio iniziava con questo racconto. Nel corso della narrazione, i ragazzi facevano attenzione a interagire il più possibile con i bambini. Di solito, poi, continuavano facendo riflettere i visitatori sul numero di chiavi possibili per la decifrazione dei messaggi. I bambini di scuola primaria, la maggior parte delle volte, dopo aver contato i simboli della ruota, rispondevano che c'erano 26 chiavi possibili. Poi si passava alla parte pratica: si prendeva un volontario che scrivesse una frase alla lavagna, si faceva scegliere a turno la chiave e trascrivere la frase cifrata con i simboli.

Come si è avuto modo di osservare nel corso del meeting, anche i bambini molto piccoli si rendono conto che scrivere messaggi con il cifrario di Cesare non è molto sicuro, proprio perché ci sono solo 26 modi possibili per scegliere la chiave.

Il passo successivo perciò consiste nel prendere in considerazione, invece che una traslazione dell'alfabeto, il caso in cui le lettere possono venir permutate in modo arbitrario. In questo caso la chiave è composta da una tabella che associa a ogni singola lettera in codice la lettera in chiaro.

Le chiavi possibili sono tantissime: nel caso dell'alfabeto italiano esteso sono ben 26!, cioè $26 \times 25 \times 24 \times \ldots \times 2 \times 1$. Questo metodo può venire, però, facilmente forzato con il metodo dell'analisi statistica delle frequenze delle lettere.

La tabella seguente ci mostra le frequenze relative (in percentuale) delle lettere nella lingua italiana, trovate dai ragazzi della mia classe esaminando un articolo di circa 1.000 lettere tratto dal *Corriere della Sera*:

E	A	I	O	R	N	L	T	S	D	C	U	M
12,3	11,8	10,8	7,9	7,4	7,3	7,0	6,6	5,5	3,8	3,7	2,9	2,6

P	G	V	F	Z	B	H	Q	Y	K	J	X	W
2,3	1,9	1,6	1,1	1,0	0,8	0,6	0,4	0,1	0,0	0,0	0,0	0,0

Analogamente, per lo sloveno è stata ottenuta la seguente tabella:

E	A	I	O	N	R	S	L	J	T	V	D	K
10,8	10,2	8,9	8,8	6,9	5,3	5,2	4,7	4,5	4,5	4,0	3,6	3,5

M	P	U	Z	B	G	Č	H	Š	C	Ž	F
3,3	3,1	2,2	2,1	1,8	1,5	1,5	1,1	1,0	0,7	0,7	0,1

Bisogna comunque dire che i testi, specialmente quelli brevi, non rispecchiano del tutto le statistiche e che quindi è meglio prendere in considerazione anche la probabilità delle lettere di apparire alla fine delle parole oppure la probabilità che hanno di apparire in coppia, ecc. Un testo risulta essere tanto più semplice da decrittare quanto più è lungo, perché rispecchia meglio le proprietà statistiche della lingua in cui è scritto. Perciò i messaggi in codice devono essere brevi e la chiave deve venire cambiata spesso.

Coi ragazzi abbiamo deciso di spiegare il cifrario a sostituzione completa servendoci delle parole crociate crittografate della *Settimana Enigmistica*. I ragazzi si sono messi all'opera risolvendo vari enigmi. Il problema era però quello di trovarne uno in cui le frequenze relative delle lettere rispecchiassero quelle da noi ottenute. Ovviamente, essendo i crittogrammi composti da poche parole e, per lo più, non collegate in frasi dell'italiano scritto, ciò non accade spesso. Alla fine ci siamo soffermati sul quesito n. 5.402 che non era troppo complicato da risolvere, rispecchiava le nostre frequenze e non conteneva troppe parole "difficili". Il cruciverba (che conteneva le informazioni: 3 = *a*, 7 = *e*, 11 = *n* e 12 = *t*) è riportato in Figura 2.

Nel corso del laboratorio presentato al meeting "La matematica dei ragazzi", si chiedeva ai visitatori di contare quante volte apparissero i singoli numeri, ottenendo:

Numero	7	3	5	12	8	11	4	1	2	10	13	6	15	14	9
Frequenza	18	15	15	15	13	12	9	6	4	4	4	4	3	2	2
Lettera	e	a		t		n									

Questa tabella doveva essere confrontata con le tabelle delle frequenze da noi ottenute per la lingua italiana. Si poteva così ipotizzare che il numero 5 rappresentasse la *i* e l'8, spesso presente alla fine delle parole, la *o* (invito i lettori a provare a inserire le lettere nel cruciverba per seguire meglio quanto qui esposto). Così facendo si otteneva una parola completa, *tetano*, che confermava che si era sulla strada giusta.

La successiva lettera più frequente, secondo le nostre tabelle, era la *r*. Associando al numero 4 la lettera *r* si ottenevano due parole che hanno senso, cioè *rio* e *nere*, che confermavano che si era fatta una scelta corretta. A questo punto si poteva associare al numero 1 la *s* e ottenere, ad esempio, la parola *interessante*. Bisogna a questo punto notare che la *s* è una delle lettere che più frequentemente appaiono come doppie nelle parole italiane. Si scriveva poi la *v* al posto del

numero 14 , ottenendo nella terza riga la parola *neve*. Osservando il crittogramma, già quasi completato, si vedeva che, inserendo la *p* al posto del 2, si ottenevano due parole complete: *panetterie* e *trapasso*. A questo punto, con un po' d'intuizione, si potevano inserire ancora le lettere mancanti: 6 = *d*, 9 = *c*, 13 = *l*, 15 = *b* e 10 = *m*.

Il problema maggiore di questa esposizione fu quello di trovare un modo per poter completare il crittogramma in modo chiaro nel minor tempo possibile. Per fare ciò erano stati costruiti due cartelloni: su uno erano esposte le tabelle con i dati statistici e sull'altro il crittogramma. Le lettere erano state scritte su dei post-it, così da poter essere posizionate al momento opportuno: il gioco era fatto.

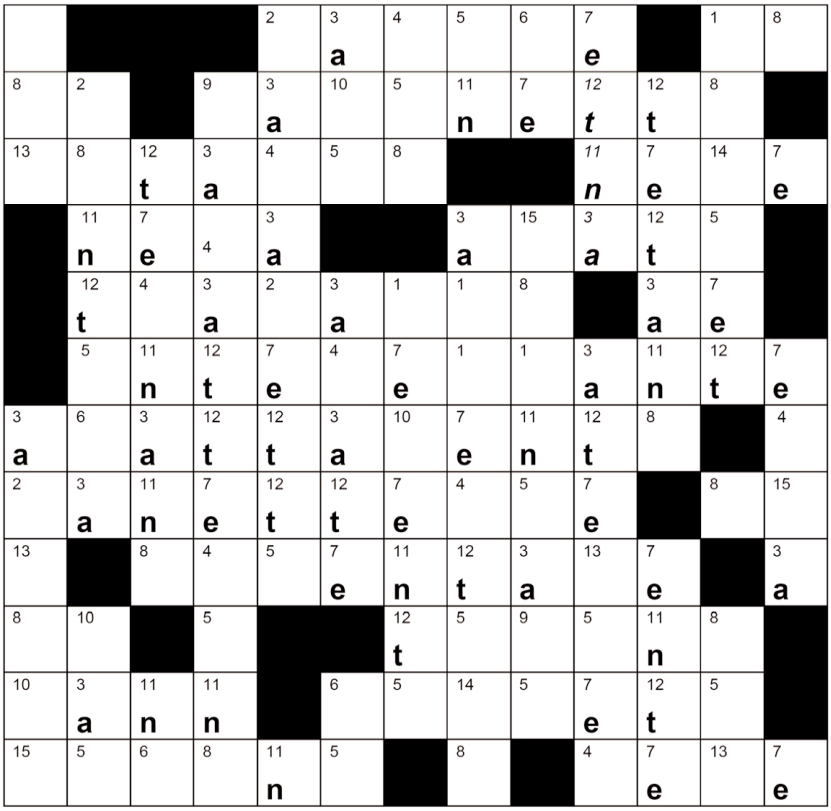

Figura 3
Parole crociate crittografate

I ragazzi hanno scoperto, attraverso la partecipazione a "La matematica dei ragazzi", che la matematica può essere anche divertente e che probabilmente avevano scelto la scuola giusta, poiché lavorare con i bambini li aveva affascinati parecchio.

Trasportati dall'entusiasmo, gli studenti hanno in seguito espresso il desiderio di presentare quanto da loro appreso anche ai bambini della Scuola Elementare con lingua d'insegnamento slovena Oton Zupančič, con sede nel medesimo edificio del Liceo Pedagogico.

Presi gli accordi con le maestre, siamo stati così ospiti della scuola elementare per ben due volte. In questi due incontri gli allievi hanno presentato quanto da loro esposto a "La matematica dei ragazzi", prima ai bambini della prima e della seconda classe, poi a quelli delle classi terza, quarta e quinta. Anche in queste due occasioni i ragazzi sono rimasti molto soddisfatti del lavoro svolto in classe con i bambini. Infatti gli allievi delle elementari sono risultati essere più motivati a scoprire concetti nuovi di quanto non lo siano stati gli studenti d'età più avanzata.

NOTE

* Liceo Pedagogico Statale con
lingua d'insegnamento slovena
"A. M. Slomšek", Via Caravaggio 4,
I-34128 Trieste
e-mail: amslomsek@tiscalinet.it

BIBLIOGRAFIA

Marceddu M.C., 2002, "Il gioco dell'agente segreto", in Zuccheri L., Leder D., Scheriani C. (a cura di), 2002, *La matematica dei ragazzi: scambi di esperienze tra coetanei. Antologia delle edizioni 1996-1998*, EUT, Trieste, pp. 43-49.

Sgarro A., 1986, *Crittografia*, Muzzio, Padova.

Sgarro A., 1989, *Codici segreti*, Mondadori, Milano.

Sgarro A., Zuccheri L., 1992, "I codici segreti nell'insegnamento della matematica", *Atti del Convegno "Media e metodi III: la matematica tra didattica e cultura"* (Trieste 6-7 maggio 1992), pp. 131-139.

Singh S., 1999, *Codici & Segreti*, Rizzoli, Milano.

Zuccheri L., 1992, "Crittografia e Statistica nella Scuola Elementare", *L'insegnamento della matematica e delle scienze integrate*, vol. 15 (1), pp. 19-38.