Crittografia

(Percorso con la scuola elementare, classe IV B; studenti del liceo con ruolo di tutor).

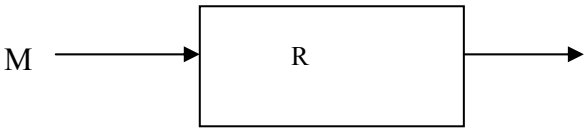
Aspetti motivazionali

1. Si tratta di una disciplina oggi in gran volga negli ambienti dell'informatica e delle telecomunicazioni, che riguarda la sicurezza dei dati (cartelle cliniche, contenuti nei grandi date base o anche semplicemente nei personal computer...) e dei messaggi che viaggiano su ogni sorta di canale (posta ordinaria, telefono, via etere, internet, come le transazioni bancarie, le informazioni riservate).
2. Si tratta di una scienza antichissima. Nelle società primitive qualunque tipo di scrittura è di per se stesso un codice per iniziati e ha spesso a che fare con la magia. Se è vero che si scrive per comunicare, la comunicazione è per iniziati, per pochi eletti e non è un caso che il cifrario di Cesare sia così semplice e ingenuo, ormai decodificabile da chiunque. Esempi da proporre: cifrario di Cesare, su cui si lavorerà tecnicamente, generalizzandolo e, magari, un accenno alla storia di Enigma, la macchina utilizzata nella seconda guerra mondiale, il cui funzionamento fu compreso grazie al lavoro di Turing e di alcuni matematici polacchi.

Aspetti concettuali

Ogni sistema crittografico e i relativi problemi sono caratterizzati dalle seguenti variabili:

M = messaggio o testo in chiaro (che chi scrive vuole fare arrivare al destinatario preservandolo dai rischi di essere letto da altri).
C = crittogramma o testo in cifra (che chi scrive invia la destinatario, confidando che non possa essere compreso da altre persone che dovessero entrarne in possesso).
R = chiave, ossia le regole di cifratura (usate da chi scrive). In termini matematici si può scrivere che R(M) = C, oppure



(analogia con le operazioni unarie)

R^{-1} = chiave inversa, ossia le regole di decrittazione Usate dal destinatario).
In termini matematici si può dire che $R^{-1}(C) = M$

T = canali di trasmissione (del messaggio e della chiave, eventualmente diversi)
S = persone diverse dal destinatario (dette per comodità spie, ma sarebbe bene far notare che non necessariamente la decrittazione di un messaggio non indirizzato a S è illegale: S potrebbe essere un magistrato che cerca di capire che cosa si dicono due trafficanti di droga).

Si può anche poi pensare a un dispositivo D, meccanico o manuale che realizza la codifica (secondo R) e a un dispositivo D' eventualmente diverso da D che realizza la decodifica (secondo R^{-1}).
Infine è utile considerare un cifrario, o meglio un sistema di regole SR di cui R e R^{-1} sono casi particolari fra i tanti possibili. In genere i dispositivi D consentono di codificare secondo varie regole, ma facenti parte tutte di una stessa classe o tipo.
Il problema essenziale è quello della codifica – decodifica.
Dal punto di vista di chi codifica: garantire la sicurezza del messaggio, rendendo la sua decodifica semplice per l'utente, ma praticamente impossibile per altri, dove il praticamente si intende riferito

ai tempi mediamente richiesti per la decodifica rapportati al tempo per cui il messaggio deve restare segreto.
Dal punto di vista di chi decodifica: determinare metodi di individuazione delle regole R^{-1} che consentono di decifrare il messaggio.

Nei problemi di codifica – decodifica, valgono due principi:

1. La decodifica deve risultare facile al destinatario, ma proibitiva per la spia;
2. La spia è sempre al corrente del tipo di cifrario utilizzato (principio di Kerchoffs).

Concetti matematici interessati

1. Ordinamento circolare
2. Rotazione
3. Misura degli angoli e uso del goniometro
4. Proprietà di simmetria della circonferenza
5. Permutazione
6. Notazione funzionale
7. Primi elementi di calcolo combinatorio: calcolo delle permutazioni di un dato numero di oggetti distinti.

Esempi di cifrari

1. Cifrario di Cesare, come esempio particolare di cifrario a rotazione con sostituzione monoalfabetica (ogni lettera dell'alfabeto viene sostituita con quella che la *segue* di tre posizioni *nell'ordinamento circolare* dell'alfabeto).
   Attività possibili:
   1.1 un gruppo di bambini, che rappresenta chi scrive, cifra un messaggio. Un gruppo lo decodifica (il destinatario). Gli altri gruppi (le spie) devono decifrarlo messi in due situazioni:
      a) non conoscono il cifrario (situazione possibile solo nella prima attività)
      b) conoscono il cifrario, ma non la rotazione.

   Si fanno almeno tre – quattro attività di codifica – decodifica di questo tipo.
   2.1 Si costruisce un cifrario che possa rendere automatica una qualunque codifica di tipo monoalfabetico a rotazione (con carta, forbici, matita, perno e goniometro per gli studenti; con Cabri per l'insegnante o i tutor). Si lavora con il cifrario riflettendo su quante operazioni si possono fare al più per decodificare un messaggio cifrato di tipo "sostituzione circolare monoalfabetica".
   2.2 Generalizzazione dei cifrari a sostituzione monoalfabetici: quante sono le possibili chiavi per cifrari monoalfabetici a sostituzione? Si inizia con due lettere, poi tre, poi quattro e si vede se nasce nei bambini l'idea di come si calcola il numero di permutazioni di un numero fissato di lettere (il fattoriale di un numero). Gli studenti di scuola secondaria fanno da tutor. e potrebbero costruire un algoritmo e poi tradurlo in linguaggio di programmazione, che decodifichi un testo cifrato con sostituzioni circolari monoalfabetiche. Con questo programma potrebbero decodificare brevi messaggi inviati dai bambini.

   Link a siti:

http://www.liceofoscarini.it/studenti/crittografia/critto/caesar.htm#Prova
http://it.wikipedia.org/wiki/Cifrario_di_Cesare
http://sicurezza.html.it/guide/lezione.asp?IdGuida=6&idlezione=87