Crittografia

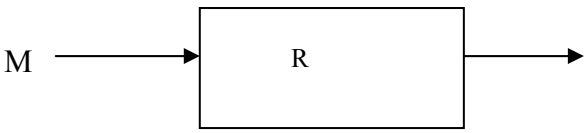
(Percorso le classi IIID e due studenti di IV D del Liceo Issel).

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.
3. Alcuni elementi teorici che verranno proposti fanno parte del programma del corso PNI.

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. Insiemi finiti e strutture algebriche modulo n.
2. Elementi di algebra lineare.
3. Elementi di teoria dei numeri, con particolare riferimento ai numeri primi.
4. Piccolo teorema di Fermat.
5. Teorema cinese del resto.
6. Algoritmo di Legendre.
7. Algoritmo RSA (per gli studenti che decideranno di seguire l'approfondimento).

Per quel che riguarda i link ai siti si rimanda ai vari documenti.