Cenni storici

Stenografia

La stenografia è un metodo di scrittura veloce, che impiega segni, abbreviazioni o simboli per rappresentare lettere, suoni, parole o frasi. Probabilmente era già in uso ai tempi di Senofonte. Con certezza era in uso presso i Romani conosciute come *notae tironianae.* Erano derivare dall'alfabeto corsivo, furono inventate dal segretario di Cicerone Marco Tullio Tirone.

La stenografia moderna ha inizio verso la fine del XVI secolo e si sviluppa per circa due secoli con l'invenzione di diversi linguaggi, soprattutto in Inghilterra.

In tempi più recenti ha avuto grande diffusione il sistema inventato dal tedesco Franz Xaver Gabelsberger nel 1834. Era alfabetico e ortografico, e i suoi segni erano derivati dalle forme della scrittura corsiva. Fu rapidamente adattato a molte lingue, tra cui l'italiano (nel 1863 da Enrico Carlo Noë). È stato dichiarato nel 1928 sistema nazionale.

Crittologia

La crittologia è la scienza delle scritture segrete, sia dell'ideazione di metodi sempre più sicuri per occultarne il significato (crittografia) che la sua controparte: il decifrare testi occultati senza conoscerne a priori il metodo (crittanalisi).

Crittografia e crittanalisi sono le due facce della stessa medaglia, una medaglia che nel corso della storia ha dato più importanza all'una o all'altra, alternativamente.

Una delle prime tracce storiche di uso di queste tecniche risale a *Gaio Giulio Cesare* che si narra utilizzasse un cifrario (*detto Cifrario di Cesare*) consistente nel sostituire ad ogni lettera la terza lettera successiva.

Ben presto per metodi così arcaici vennero scoperti metodi di soluzione generali (uno dei primi è stata l'analisi delle frequenze), segnando anche la nascita della crittanalisi.

Nel corso della storia le due arti contrapposte hanno affinato sempre più le loro armi, dando spesse volte l'impressione che una delle due fosse destinata a prevalere sull'altra... oggigiorno la guerra si è spostata nella teoria dei numeri, la branca più astratta della matematica, dimostrando che perfino la scienza più astratta può avere decisivi effetti sulla vita di tutti i giorni. Gli ultimi prodotti della crittografia sembrano a tutti gli effetti inattaccabili... ma la storia ci insegna che è forse troppo presto per giudicare, benché gli odierni risultati siano basati su metodi sempre più precisi e controllati e non sull'intuito personale del crittologo.

Il cifrario di Cesare

Il cifrario di Cesare è il più antico algoritmo crittografico di cui si abbia traccia storica. È un cifrario a sostituzione monoalfabetica in cui ogni lettera del testo in chiaro è sostituita nel testo cifrato dalla lettera che si trova un certo numero di posizioni dopo nell'alfabeto. In particolare, Cesare utilizzava uno spostamento di 3 posizioni (la chiave era dunque "3"), secondo il seguente schema:

Testo in chiaro	a b c d e f g h i l m n o p q r s t u v z
Testo cifrato	D E F G H I L M N O P Q R S T U V Z A B C

Il cifrario di Cesare prende il nome da Giulio Cesare, che lo utilizzò con una chiave 3 per proteggere un messaggio d'importanza militare per Cicerone. Al tempo era sicuro, perché i nemici spesso non erano in grado di leggere nemmeno un testo in chiaro, figuriamoci uno cifrato; inoltre, non esistevano metodi di crittanalisi in grado di rompere una simile cifra. Conosciamo altri che usarono questo cifrario prima di Cesare, dunque non fu certamente inventato da lui. Dalla scoperta dell'analisi delle frequenze da parte degli Arabi attorno all'anno 1000, tutti i cifrari di questo tipo sono diventati rompibili in modo facile, spesso banale. Nessuno è adatto per comunicazioni sicure, ora, e neanche negli ultimi 1000 anni. Un vecchio libro romano sulla crittografica, andato perso, sembra parlasse ampiamente dell'uso di simili cifrari. Lo conosciamo tramite riferimenti da parte di altri scritti arrivati fino a noi, come ad esempio Svetonio.

Il cifrario di Leon Battista Alberti

Nel 1466 Leon Battista Alberti pubblicò un suo libro, scritto qualche anno prima, in cui descriveva i principali metodi di cifratura conosciuti all'epoca e introduceva una nuova tecnica inventata personalmente che consisteva in una sostituzione simile a quella di Cesare con sostituzione periodica della chiave.

Se utilizziamo il nostro solito esempio:

```
PROVA DI CIFRATURA
```

E di utilizzare la chiave 4 per la prima parola, la chiave 6 per la seconda e la chiave 5 per la terza. Il risultato della cifratura sarà quindi:

```
TVSZE JO HNKWFYZVF
```

La chiave era quindi costituita dalla concatenazione delle varie chiavi usate per ogni parola in modo ciclico. Successivamente Alberti elaborò un sistema che permetteva di inserire all'interno del messaggio l'informazione per il cambiamento della chiave. Il particolare che fa ricordare le idee di Alberti è però un semplicissimo dispositivo "meccanico" di cifratura composto da due dischi concentrici sovrapposti, con quello superiore (il più piccolo) in grado di ruotare che permetteva di trovare, impostando la chiave, tutte le corrispondenze in modo molto rapido.

Per quanto riguarda il su cifrario polialfabetico, non riuscì ad ottenere il successo che meritava soprattutto per la decisione dell'autore di tenerla segreta per parecchi anni e quando fu pubblicato il suo trattato la tavola di Vigenère era diventata ormai troppo conosciuta.

Cifrario di Vigénère

Il cifrario di Vigenère è il più semplice dei cifrari polialfabetici; fu pubblicato nel 1586 in un trattato di Blaise de Vigenère; ritenuto per secoli un cifrario inattaccabile, ha goduto di una fama dovuta soprattutto alla sua semplicità e in buona parte immeritata essendo molto più debole di altri codici polialfabetici precedenti quali il disco dell'Alberti, o le cifre del Bellaso; una fama che è durata fino alla I guerra mondiale molti anni dopo la scoperta del primo metodo di crittanalisi: il metodo Kasiski del 1863.

Il metodo si può considerare una generalizzazione del cifrario di Cesare; invece di spostare sempre dello stesso numero di posti la lettera da cifrare, questa viene spostata di un numero di posti variabile, determinato in base ad una parola chiave, da concordarsi tra mittente e destinatario, e da scriversi sotto il messaggio, carattere per carattere; la chiave era detta anche verme, per il motivo che, essendo in genere molto più corta del messaggio, deve essere ripetuta molte volte sotto questo, come nel seguente esempio:

```
Testo chiaro  - ARRIVANOIRINFORZI
Verme         - VERMEVERMEVERMEVE
Testo cifrato - VVIUZVRFUVDRWAVUM
```

Il testo cifrato si ottiene spostando la lettera chiara di un numero fisso di caratteri, pari al numero ordinale della lettera corrispondente del verme. Di fatto si esegue una somma aritmetica tra l'ordinale del chiaro (A = 0, B = 1, C = 2 ...) e quello del verme; se si supera l'ultima lettera, la Z, si ricomincia dalla A, secondo la logica delle aritmetiche finite. Il vantaggio rispetto ai cifrari monoalfabetici è evidente: la singola lettera del testo chiaro non è sempre cifrata con la stessa lettera; e questo rende più difficile la crittanalisi statistica del testo cifrato.

Per semplificare la cifratura, il Vigenère propose l'uso della seguente tavola quadrata, composta da alfabeti ordinati spostati. Volendo ad esempio cifrare la prima R di ARRIVANO si individuerà la colonna della R, quindi si scenderà lungo la colonna fino alla riga corrispondente della corrispondente lettera del verme (qui E); la lettera trovata all'incrocio è la lettera cifrata (qui V); la seconda R invece sarà cifrata con la lettera trovata sulla riga della R di VERME, e cioé con la I

```
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
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 A
C 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
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
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 D
F G H I J K L M N O P Q R S T U V W X Y Z A B C D E
G H I J K L M N O P Q R S T U V W X Y Z A B C D E F
H I J K L M N O P Q R S T U V W X Y Z A B C D E F G
I J K L M N O P Q R S T U V W X Y Z A B C D E F G H
J K L M N O P Q R S T U V W X Y Z A B C D E F G H I
K L M N O P Q R S T U V W X Y Z A B C D E F G H I J
L M N O P Q R S T U V W X Y Z A B C D E F G H I J K
M N O P Q R S T U V W X Y Z A B C D E F G H I J K L
N O P Q R S T U V W X Y Z A B C D E F G H I J K L M
O P Q R S T U V W X Y Z A B C D E F G H I J K L M N
P Q R S T U V W X Y Z A B C D E F G H I J K L M N O
Q R S T U V W X Y Z A B C D E F G H I J K L M N O P
R S T U V W X Y Z A B C D E F G H I J K L M N O P S
S T U V W X Y Z A B C D E F G H I J K L M N O P Q R
T U V W X Y Z A B C D E F G H I J K L M N O P Q R S
U V W X Y Z A B C D E F G H I J K L M N O P Q R S T
V W X Y Z A B C D E F G H I J K L M N O P Q R S T U
W X Y Z A B C D E F G H I J K L M N O P Q R S T U V
X Y Z A B C D E F G H I J K L M N O P Q R S T U V W
Y Z A B C D E F G H I J K L M N O P Q R S T U V W X
Z 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
```

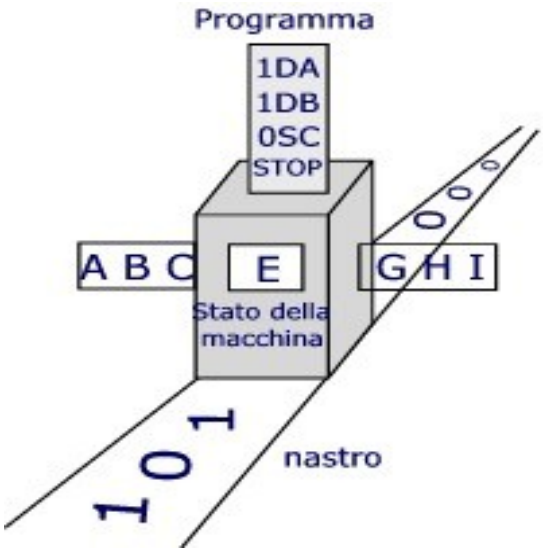
Enigma

L'Enigma fu una macchina per cifrare (e decifrare) elettro-meccanica, al servizio dell'esercito tedesco. La sua facilità d'uso e la sua indecifrabilità furono le maggiori ragioni per il suo ampio utilizzo. Nonostante gli sforzi dei più valorosi scienziati, ricordiamo il contributo di Alan Turing e di apposite macchine decifranti da lui ideate, resi vani dall'algoritmo di cifratura per l'epoca inimmaginabile, e che non sarebbero riuscite a provare l'alto numero di chiavi in tempo (in realtà provavano a caso una ristretto insieme, quindi era possibile che a volte la decifratura avvenisse) il cifrario venne penetrato dagli inglesi soltanto successivamente al recupero di un esemplare da un sottomarino tedesco. la lettura delle informazioni contenute nei messaggi da quel momento non più protetti portò alla conclusione della Seconda Guerra Mondiale con almeno un anno di anticipo.

Macchina di Turing

Una macchina di Turing è una macchina formale, cioè un sistema formale che può descriversi come un meccanismo ideale, ma in linea di principio realizzabile concretamente, che può trovarsi in stati ben determinati, opera su stringhe in base a regole ben precise e costituisce un modello di calcolo. Essa ha la particolarità di essere retta da regole di natura molto semplice, ovvero di potersi descrivere come costituita da meccanismi elementari molto semplici; inoltre è possibile presentare a livello sintetico le sue evoluzioni mediante descrizioni meccanicistiche piuttosto intuitive. D'altra parte essa ha la portata computazionale (potere computazionale) che si presume essere la massima: si dimostra infatti che essa è equivalente, ossia in grado di effettuare le stesse elaborazioni di tutti gli altri modelli di calcolo di più ampia portata. Tra questi modelli di calcolo ricordiamo le funzioni ricorsive di Jacques Herbrand e Kurt Gödel , il lambda calcolo di Alonzo Church e Stephen Kleene, la logica combinatoria di Moses Schönfinkel e Haskell Curry, gli algoritmi di Markov, i sistemi di Thue, i sistemi di Post, le macchine di Hao Wang e le macchine a registri elementari o RAM astratte di Marvin Minsky. Di conseguenza si è consolidata la

convinzione che per ogni problema calcolabile esista una MdT (**M**acchina **d**i **T**uring) in grado di risolverlo: questa è la cosiddetta congettura di Church-Turing, la quale postula in sostanza che per ogni funzione calcolabile esista una macchina di Turing equivalente, ossia che l'insieme delle funzioni calcolabili coincida con quello delle funzioni ricorsive.



La MdT come modello di calcolo è stato introdotta nel 1936 da Alan Turing per dare risposta all'Entscheidungs-problem (problema di decisione) proposto da Hilbert nel suo programma di fondazione formalista della matematica.

Per le sue caratteristiche, il modello della MdT è un efficace strumento teorico che viene largamente usato nella teoria della calcolabilità e nello studio della complessità degli algoritmi. Per definire in modo formalmente preciso la nozione di algoritmo oggi preferenzialmente si sceglie di ricondurlo alle elaborazioni effettuabili con macchine di Turing.

Funzionamento della Macchina di Turing

La macchina può agire sopra un nastro che si presenta come una sequenza di caselle nelle quali possono essere registrati simboli di un ben determinato alfabeto finito; essa è dotata di una testina di lettura e scrittura (I/O) con cui è in grado di effettuare operazioni di lettura e scrittura su una casella del nastro. La macchina si evolve nel tempo e ad ogni istante si può trovare in uno stato interno ben determinato facente parte di un insieme finito di stati. Inizialmente sul nastro viene posta una stringa che rappresenta i dati che caratterizzano il problema che viene sottoposto alla macchina. La macchina è dotata anche di un repertorio finito di istruzioni che determinano la sua evoluzione in conseguenza dei dati iniziali. L'evoluzione si sviluppa per passi successivi che corrispondono a una sequenza discreta di istanti successivi. Le proprietà precedenti sono comuni a molte macchine formali (automa a stati finiti, automa a pila, ...). Caratteristica delle MdT è quella di disporre di un nastro potenzialmente infinito, cioè estendibile quanto si vuole qualora questo si renda necessario.

Ogni passo dell'evoluzione viene determinato dallo stato attuale s nel quale la macchina si trova e dal carattere c che la testina di I/O trova sulla casella del nastro su cui è posizionata e si concretizza nell'eventuale modifica del contenuto della casella, nell'eventuale spostamento della testina di una posizione verso destra o verso sinistra e nell'eventuale cambiamentodello stato. Quali azioni vengono effettuate ad ogni passo viene determinato dalla istruzione, che supponiamo unica, che ha come prime due componenti s e c; le altre tre componenti dell'istruzione forniscono nell'ordine il nuovo stato, il nuovo carattere e una richiesta di spostamento verso sinistra, nullo o verso destra.

Una evoluzione della macchina consiste in una sequenza di sue possibili configurazioni, ogni configurazione essendo costituita dallo stato interno attuale, dal contenuto del nastro

(una stringa di lunghezza finita) e dalla posizione sul nastro della testina di I/O. Nei casi più semplici l'evoluzione ad un certo punto si arresta in quanto non si trova nessuna istruzione in grado di farla proseguire. Si può avere un arresto in una configurazione "utile" dal punto di vista del problema che si vuole risolvere; in tal caso quello che si trova registrato sul nastro all'atto dell'arresto rappresenta il risultato dell'elaborazione. Si può avere però anche un arresto "inutile" che va considerato come una conclusione erronea dell'elaborazione. Va subito detto che può anche accadere che un'evoluzione non abbia mai fine (Vedi la successiva sezione e Problema dell'arresto).