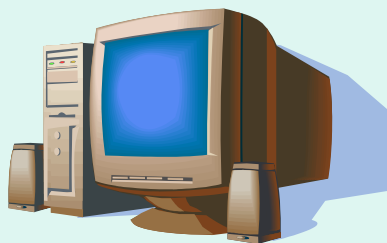


STORIA DELL'INFORMATICA E DEL CALCOLO AUTOMATICO



CLAUDE ELWOOD
SHANNON

(un appassionato di bande)

Ad opera di Fiore Giuseppina

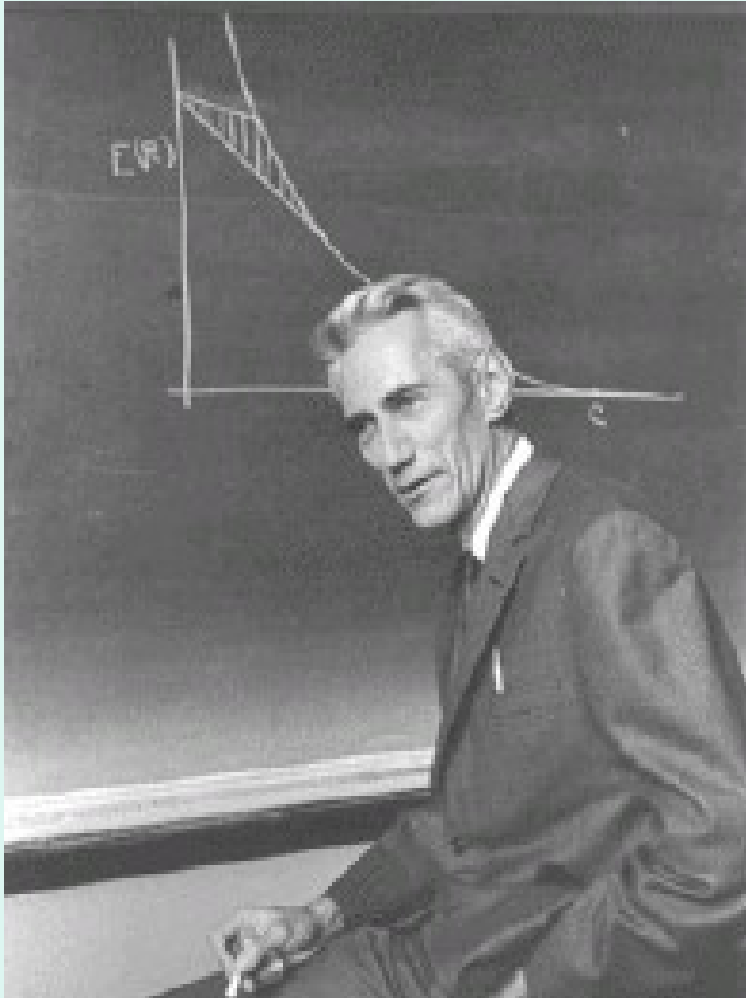
Claude Elwood Shannon

- E' considerato il padre della teoria dell'informazione.
- Gli si riconosce il merito di aver fondato le basi della moderna comunicazione digitale.
- Studioso di crittografia

MA SOPRATTUTTO.....

UN GRANDE GIOCHERELLONE E
“SMANETTATORE”

PER SAPERNE DI PIU'



- Claude Elwood Shannon nacque il 30 aprile 1916 a Petoskey, piccola città del Michigan, da Claude Sr. (1862-1934), uomo d'affari e, per un certo periodo, giudice; e da Mabel Catherine Wolf (1880-1945), insegnante di lingue e per vari anni direttrice della scuola secondaria di Gaylord, Michigan.

L'INFANZIA



- A Gaylord Claude trascorse i primi sedici anni della sua vita. Dal nonno, agricoltore e inventore, ricevette i primi incoraggiamenti in campo scientifico. L'eroe della sua infanzia fu Edison, che risultò essere un lontano cugino.

.....anche il racconto di Poe *Lo scarabeo d'oro*, in cui si parla di crittografia, ebbe su di lui una certa influenza.

LA FORMAZIONE

- Il giovane Claude esercitò il proprio talento armeggiando con svariati dispositivi elettrici e meccanici.
- All'età di 16 anni, Claude entrò alla University of Michigan, sulle orme della sorella Catherine, che qui si era appena laureata in matematica

La formazione

Nel 1936 conseguì una laurea di primo livello in matematica e ingegneria elettrica.

Per quanto non si fosse distinto in modo particolare in matematica, Claude scelse di perfezionarsi al MIT (Massachusetts Institute of Technology), dove studiò con Norbert Wiener e con Vannevar Bush, un pioniere nel campo dei computer analogici



In particolare Shannon era interessato alla teoria e alla progettazione dei complessi circuiti di relay che controllavano le operazioni dell'**analizzatore differenziale**', la macchina inventata da Bush per risolvere equazioni differenziali.

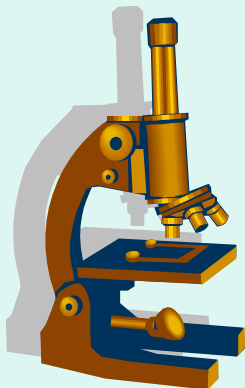
Fu in quel periodo che Shannon cominciò a pensare che con la logica a due valori di Boole si poteva fare di un computer «molto di più che una macchina per addizioni».

Nel 1937 dimostrò che l'algebra di Boole forniva uno dei mezzi più adatti per trattare i problemi dei circuiti.

LA PRIMA GRANDE INTUIZIONE

Shannon intuì che quella era la matematica appropriata per l'analisi di un simile sistema. Trovò che due interruttori in serie potevano essere descritti con l'operatore logico AND, mentre a due interruttori in parallelo poteva corrispondere l'operatore OR. L'operatore NOT poteva essere implementato tramite il contatto posteriore di un relè, piuttosto che tramite il contatto anteriore.

Bush, che era stato eletto presidente del Carnegie Institution di Washington , si occupava di genetica e suggerì a Shannon un possibile impiego dell'algebra nell'organizzazione della conoscenza genetica. Shannon lavorò all'approfondimento della questione che si concluse con la presentazione della tesi di dottorato "An Algebra for Theoretical Genetics".



Nella primavera del 1940, dopo essere faticosamente riuscito a superare gli esami in lingue straniere (*non erano proprio fatte per lui...*), Shannon ottenne un master in ingegneria elettrica e un dottorato in matematica.

Dopo il dottorato, Shannon iniziò a collaborare coi Laboratori Bell della At&T dove entrò a fare parte di un gruppo di lavoro incaricato di migliorare l'efficienza e l'affidabilità dei sistemi di trasmissione.

- Qui divenne noto per la tendenza a isolarsi. Come ricorda un collega di allora, il Dr. David Slepian:
- **"Generalmente, lavorava con la porta chiusa. Ma se entravate da lui, si dimostrava paziente e disposto ad aiutarvi. Riusciva ad afferrare il problema al volo. Era realmente un genio. La sola persona che abbia conosciuto che meriti tale definizione."**

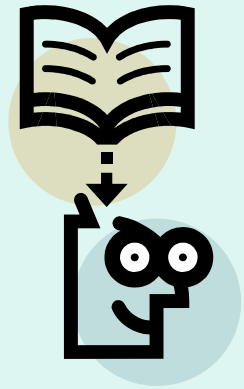
Ma in ogni caso

Non pare che Shannon fosse molto tollerante nei confronti di chi non si dimostrasse abbastanza pronto a seguire il filo dei suoi ragionamenti!!!!.

Durante la Seconda Guerra Mondiale, Shannon entrò in contatto con il grande Alan Turing, in occasione di una visita di questi negli Stati Uniti. Entrambi gli scienziati erano attratti dalla possibilità di costruire una macchina in grado di imitare il cervello umano.

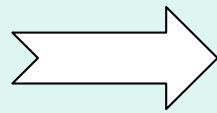
Essi lavorarono alla costruzione di un apparato telefonico criptato (il "Sistema X"), che consentisse a Roosevelt e Churchill di conversare attraverso l'Atlantico in maniera sicura. All'interno dei Bell Labs, Shannon si occupò anche di dispositivi antiaerei per contrastare le V1 e V2 tedesche.

Ciò che lo rese famoso...



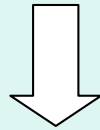
Nel 1948 pubblicò il suo lavoro più importante, la **Teoria matematica della comunicazione**, uno dei pilastri della moderna teoria dell'informazione e in parte, quindi, dell'informatica.

Il problema era ancora una volta di natura pratica. Come trasmettere messaggi impedendo che "rumori" di disturbo ne alterassero il contenuto?



Per cominciare, il problema era di definire in maniera precisa cos'era il contenuto di informazione di un messaggio.

L'idea geniale di Shannon fu che il contenuto di informazione non ha nulla a che vedere col contenuto del messaggio, ma col **numero di 0 e 1**, necessari per trasmetterlo.



La natura del messaggio, numeri, musica, immagini, era irrilevante. In ogni caso si trattava di sequenze di 0 e 1.

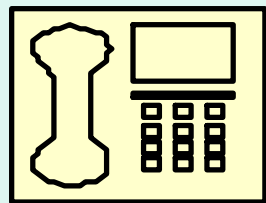
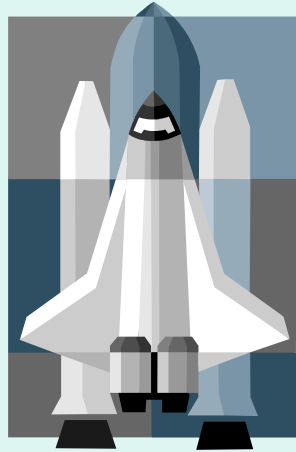
In quell 'articolo compariva per la prima volta il termine bit.

Le cifre binarie diventavano l'elemento fondamentale in ogni comunicazione.

Con i suoi lavori dedicati alla teoria dell'informazione, all'affidabilità dei circuiti, al problema della sicurezza della comunicazione e alla crittografia, Shannon ha profondamente cambiato la teoria e la pratica della comunicazione.

Ha posto particolare attenzione al problema della velocità di trasmissione di un segnale legandola alla banda del canale di trasmissione. (*ma sulla banda viaggia il rock?*)

Egli affermò, anticipando i tempi, quanto si vide nel 1969 nella trasmissione TV dello sbarco dell'uomo sulla Luna: le immagini erano da "video-lento", non continue come siamo abituati a vederle in TV: la larghezza di banda del canale (reale e perciò rumoroso) limita la velocità massima alla quale è trasmissibile il segnale attraverso quel canale, senza distorsione.



**Evidentemente
il canale che
Armstrong
poteva aprire
dalla Luna era
stretto per la
limitata
potenza
disponibile.**

La crittografia elevata a scienza

Nel 1949, venne pubblicato "Communication Theory of Secrecy Systems". In questo lavoro, Shannon applicava la teoria della comunicazione ai problemi della crittografia e dei sistemi di segretezza. Affermò:

"Dal punto di vista della crittanalisi, un sistema di segretezza è pressoché identico a un sistema di comunicazione disturbato. Si interviene sul messaggio (il segnale trasmesso) per mezzo di un elemento statistico, il sistema di cifratura, che è una chiave scelta statisticamente. Il risultato di questa operazione è il criptogramma (analogo al segnale perturbato), che è disponibile per l'analisi."

L'unico sistema criptografico totalmente sicuro fu quello proposto da G. S. Vernam nel 1926, che perfezionò il cifrario di Vigenère (1586), con l'uso di una chiave illimitata, o comunque lunga almeno quanto il testo da cifrare, totalmente casuale e utilizzabile solo una volta.

È stato comunque utilizzato dai servizi segreti e per il telefono rosso tra Washington e Mosca. Un cifrario di questo genere era usato anche da Che Guevara in Bolivia ..

Nello stesso anno accadde che



Nei Bell Labs, Shannon conobbe Mary Elizabeth (Betty) Moore, che lavorava come analista numerica (era una "computer", come si diceva allora) e il 27 marzo 1949, i due si sposarono. Da quest'unione nasceranno tre figli: Robert James , Andrew Moore e Margarita.

Appassionato giocatore di scacchi, in un suo pionieristico articolo del 1950 parlava già della programmazione dei computer per giocare a

scacchi

Nel 1965 ne aveva discusso a Mosca con Mikhail Botvinnik, ingegnere elettrico e a lungo campione mondiale di scacchi.

Stavano prendendo forma le prime idee di Profondo Blu, il programma che trent'anni dopo avrebbe sconfitto Kasparov.

La STANZA DEI GIOCHI

In occasione di un Natale, Betty pensò di regalare al marito un monociclo. In poco tempo, Claude imparò a guidare l'insolito veicolo, e lo utilizzò per spostarsi all'interno sia dei Bell Labs che del MIT, dove fece ritorno nel 1958.

I colleghi presero l'abitudine di mettersi in guardia a vicenda nel caso un traballante Shannon vagasse pericolosamente lungo i corridoi.

Shannon costruì un monociclo a due posti, per quanto fosse difficile trovare qualcuno disposto a dividerlo con lui.

La sua curiosità sempre viva e totalmente disinteressata si concretizzò in una quantità di congegni e progetti: macchine per il gioco degli scacchi, pupazzi giocolieri, il computer THROBAC-I che calcolava in numeri romani, un frisbee con propulsione a razzo, una macchina per risolvere il cubo di Rubik, ecc.

"Ho sprecato un sacco di tempo in cose totalmente inutili", disse;

in realtà si dimostrò sempre fiero dei suoi giocattoli e sempre lieto di mostrarli ai suoi visitatori, nella stanza in cui li conservava.

Manifestò piuttosto una certa insofferenza nei confronti dell'eccessivo interesse rivolto alla teoria dell'informazione, trasformata in una specie di moda del momento:

"La teoria dell'informazione si è forse gonfiata a un livello oltre i suoi effettivi adempimenti."



Per esplorare le possibilità di realizzare macchine capaci di imparare, costruì un topo elettromeccanico chiamato Theseus, che doveva trovare la strada in un labirinto alla ricerca del "pezzo di formaggio", un terminale elettrico che faceva suonare una campanella se veniva toccato dalle vibrisse di rame di Theseus.

... è stato uno dei primi tentativi di "insegnare" ad una macchina ad imparare e uno dei primi esperimenti pratici di Intelligenza Artificiale.

Colpito dal morbo di Alzheimer, Claude Shannon trascorse gli ultimi anni di vita in una casa di cura di Medford, Massachusetts. È deceduto il 24 febbraio 2001, all'età di 84 anni.

This document was created with Win2PDF available at <http://www.win2pdf.com>.
The unregistered version of Win2PDF is for evaluation or non-commercial use only.
This page will not be added after purchasing Win2PDF.