Codifiche, informazioni e bit

Lezioni al Museo

contenuti

- Informazioni in simboli
  - L'essenza dell'informatica
  - Ridursi a simboli, manipolabili (cifrari)
- L'informazione mantenuta
  - Fori su carta
  - Su nastro o su scheda
- Le comunicazioni, anche fra calcolatori
  - L'internet vittoriana
  - L'internet "dei militari"

l'essenza dell'informatica

- Informazione
  - Dal latino *informare*, dare forma, sostanza
  - L'informazione si produce, si acquisisce
  - Si trasmette, si conserva... si codifica
  - Da sempre, o almeno da quando si parla di Storia
  - Che è definita dall'esistenza di una memoria concreta
  - Cioè dall'uso di strumenti per trattare informazioni
- Strumenti automatici?
  - Strumenti: metodi, procedimenti, regole
  - Anche automatici, non subito, non molto

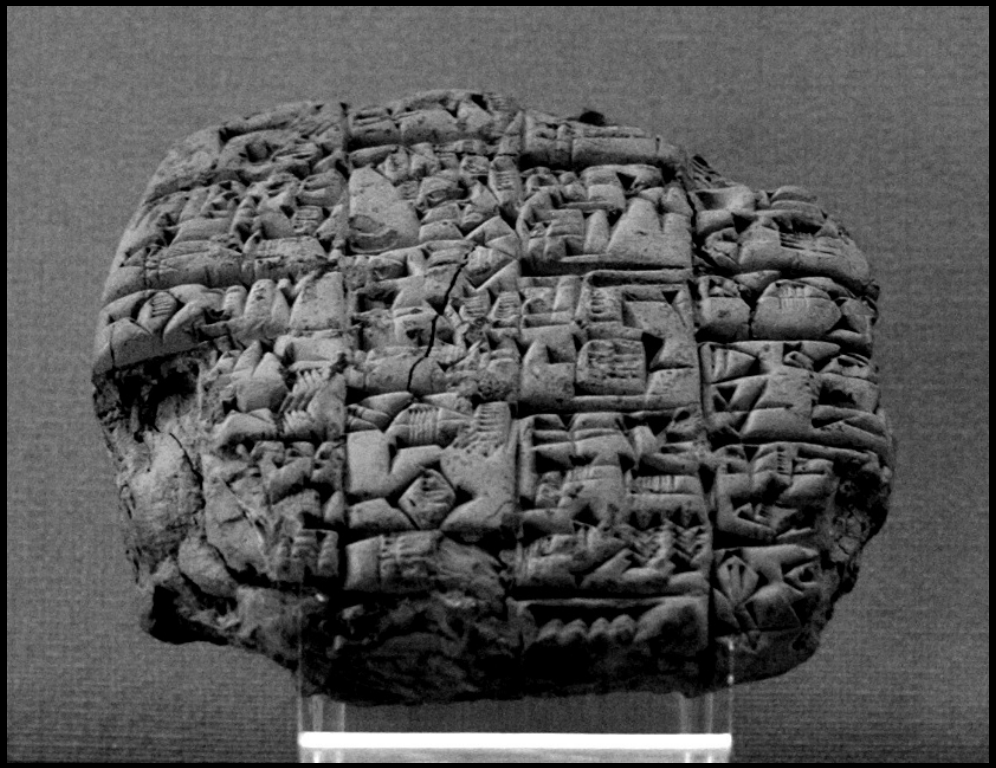
linguaggi non alfabetici

- Simboli
  - Finiti, ma poco definiti
  - Logografici
  - Ideografici
- Automatizzabili?

difficilmente

linguaggi alfabetici

- ~3000 a.C.
  - Pochi simboli
  - Sintassi
  - Fonografici

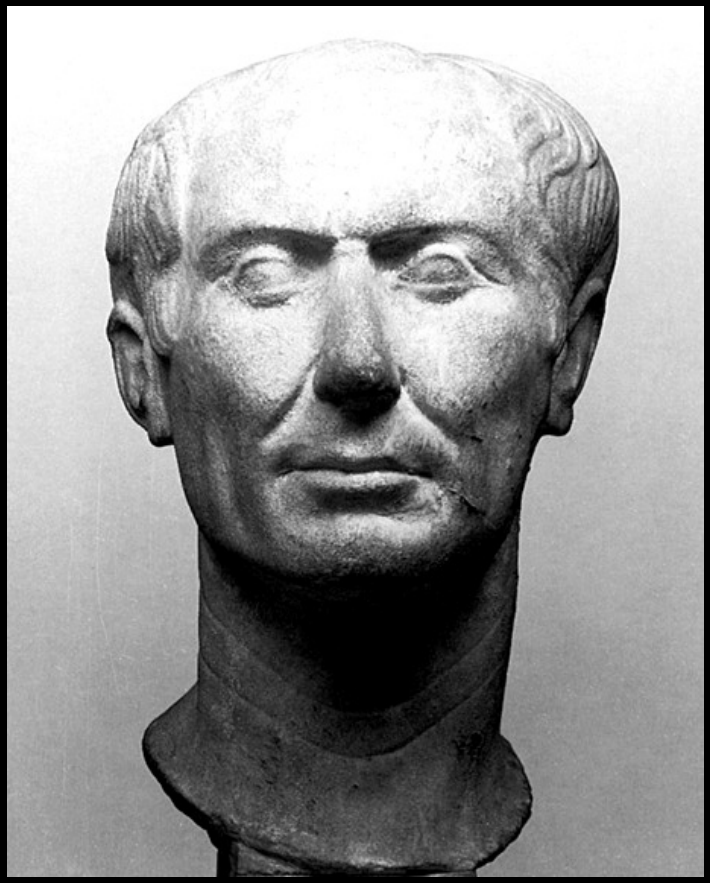


divagazioni

- Il teorema delle scimmie infinite
  - Emil Borel, 1913
  - E Aristotele, Cicerone, Pascal, Swift...
- La Biblioteca di Babele
  - Jorge Louis Borges, 1941 (libri 410 x 40 x 80 x 25)
- In un tweet?
  - Lago di Como; Renzo ama Lucia.
    Rodrigo: non s'ha da fare!
    Bravi, preti, frati, monache, tumulti, pure la peste.
    E vissero felici e credenti.
  - $1.021870238 \times 10^{295}$ (in ASCII)

calcoli con le lettere

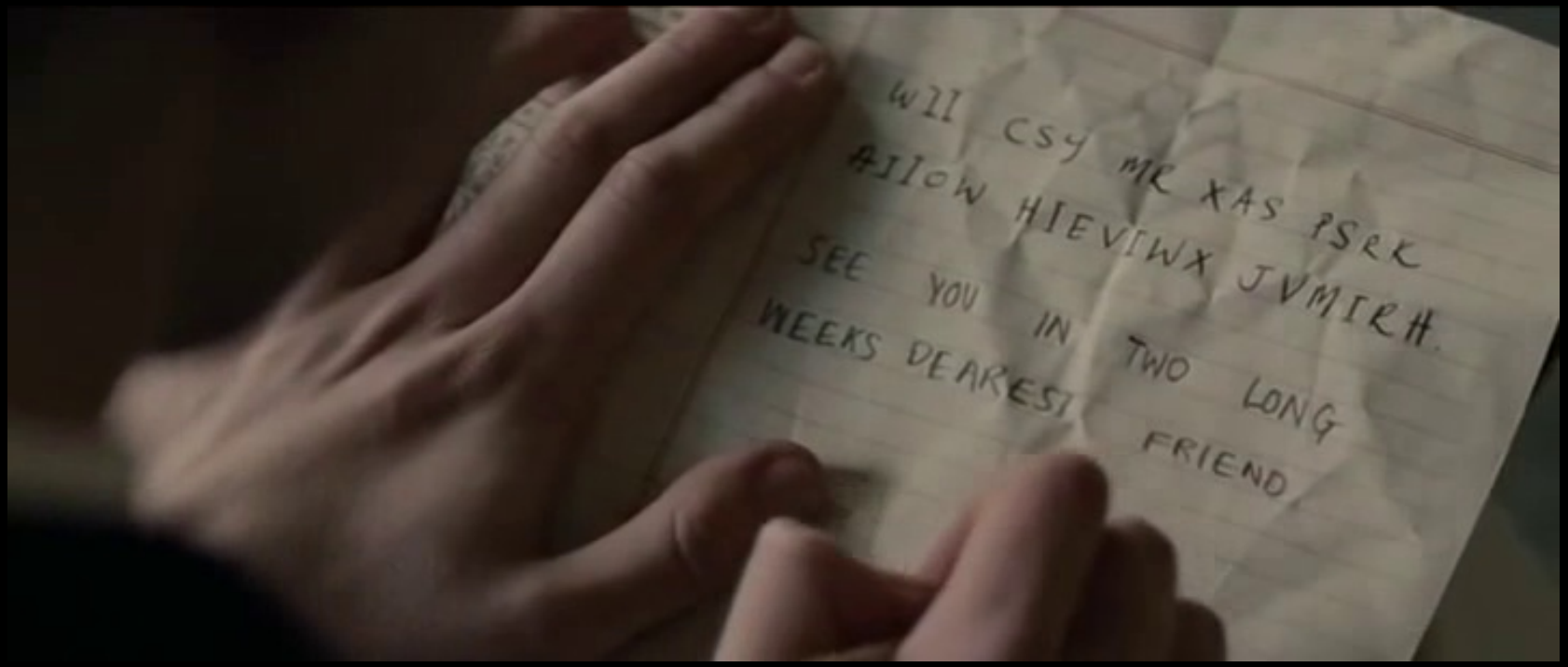
- Cifrario di Cesare
  - Campagna di Gallia, 54 a.C.
  - Corrispondenza con Quinto Tullio Cicerone
  - Vite dei Cesari di Svetonio
- Sostituzione monoalfabetica
  - Cesare usava chiave 3, A $\rightarrow$ D
  - I Galli probabilmente neanche leggevano in chiaro



pillole di crittografia

- Cifrari monoalfabetici
  - Codice di Cesare
  - `ABCDEFGHIJKLMNOPQRSTUVWXYZ`
    `DEFGHIJKLMNOPQRSTUVWXYZABC`
- Cifrari polialfabetici
  - Alberti/Trithemius/Bellaso/Vigenère, *tabula recta*
  - `ABCDEFGHIJKLMNOPQRSTUVWXYZ`
    `BCDEFGHIJKLMNOPQRSTUVWXYZA`
    `CDEFGHIJKLMNOPQRSTUVWXYZAB`
    `DEFGHIJKLMNOPQRSTUVWXYZABC`
    `...`

Morcom-Turing

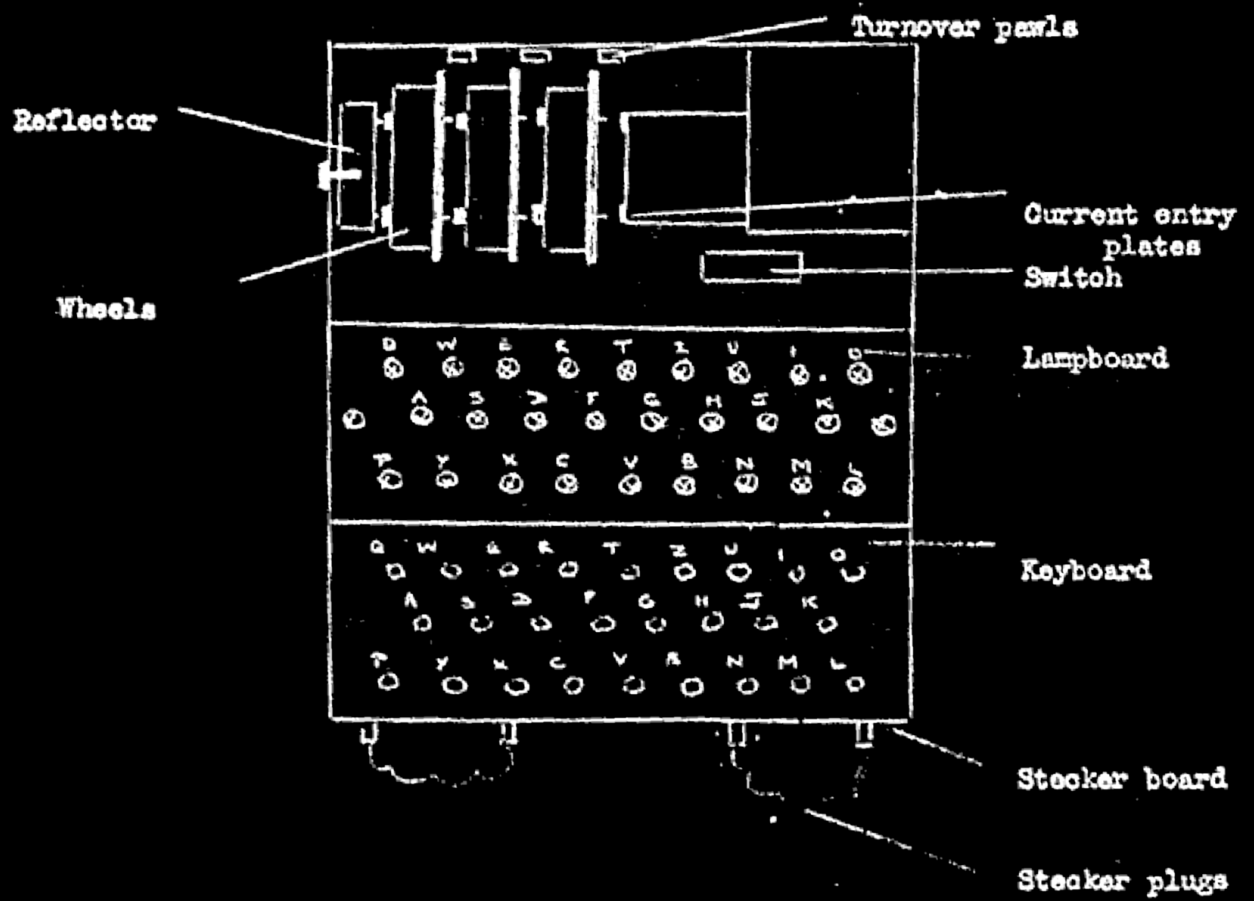


1932, Enigma I, Heeres

- Esclusiva per i militari
  - A partire dalla D Ch11a
  - – UKW ruotabile + Steckerbrett
- Cambiamenti
  - 1932 rotori I, II e III
  - 1937 riflettore UKW-B
  - 1938 rotori IV e V
  - 1941 riflettore UKW-C
  - 1944 riflettore UKW-D, UHR

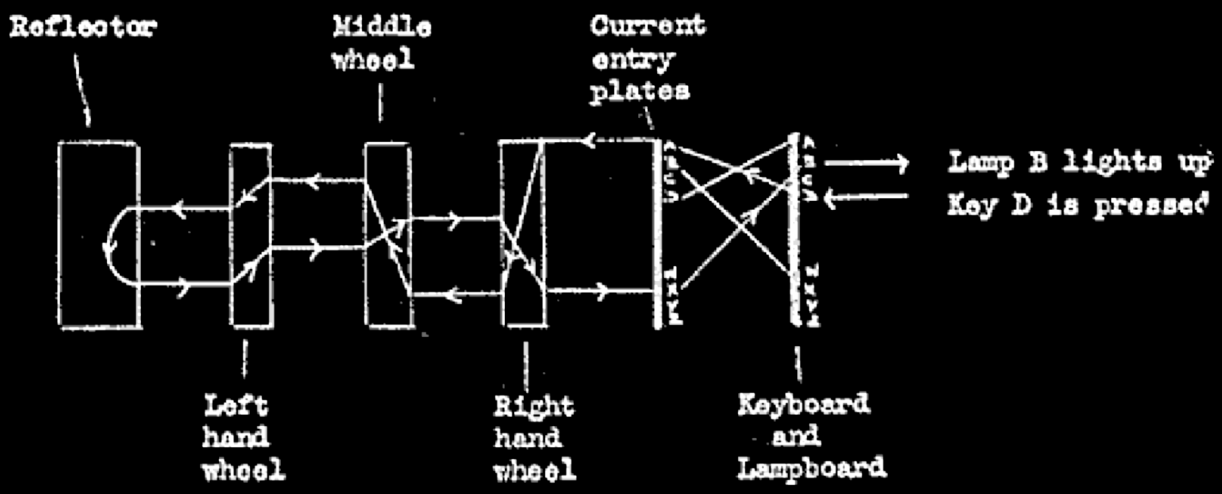
Le parti della macchina

- Esterno
  - Tastiera
  - Schermo
  - Spinotti
  - Alim. esterna
- Interno
  - Rotori
  - Riflettore
  - Batteria



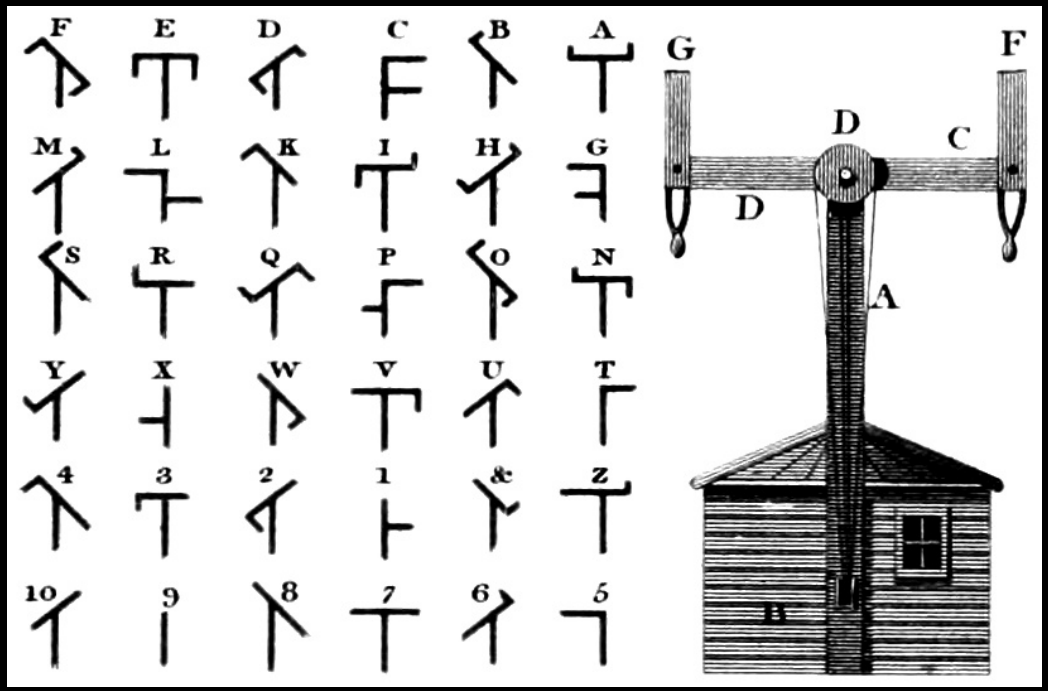
Come funziona

- Costruisce e usa al volo tabulae rectae
  - Tantissime, irregolari, lunghissime
  - Circuiti elettrici variati meccanicamente



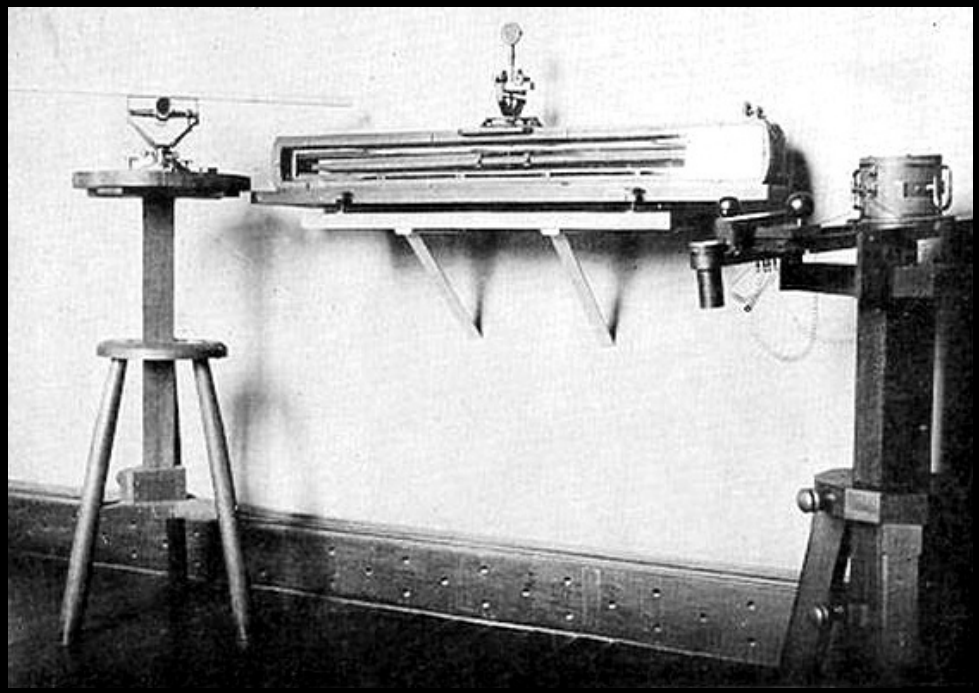
codifiche per comunicare

- Telegrafo ottico Chappe
  - Prima linea Paris-Lille
  - Servizio pubblico dal 1794 al 1852
  - A prova di sabotaggio
  - Citato da Dumas



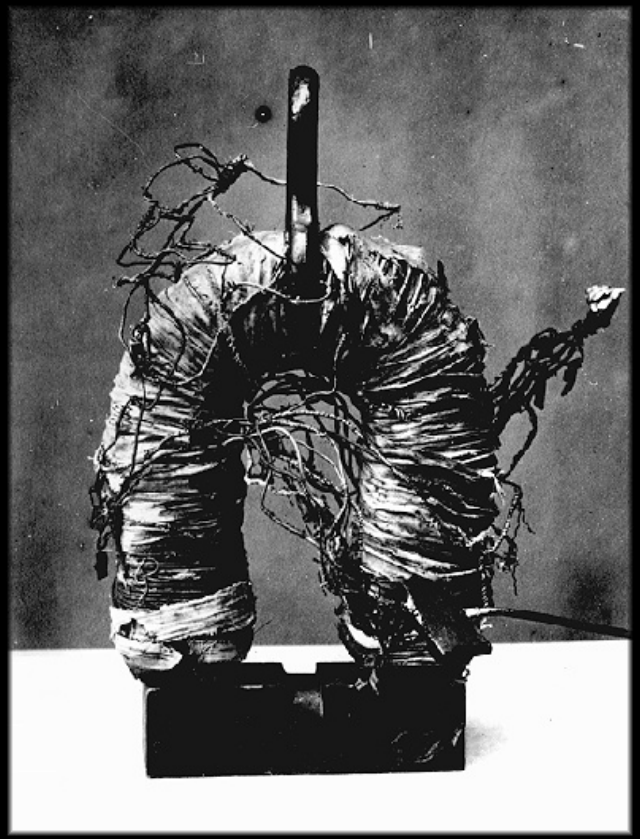
telegrafo elettrico

- Telegrafo elettrico Gauss-Weber
  - 1833, Göttingen
  - Collegava l'Istituto di Fisica all'Osservatorio
  - Circa 1 km
  - Binario
  - Verso della corrente



il relé

- Interruttore comandato, 1835
  - Joseph Henry
    primo segretario
    dello Smithsonian
  - Protagonista
    di codifiche binarie
    e operazioni booleane
  - Stato del circuito
    aperto/chiuso



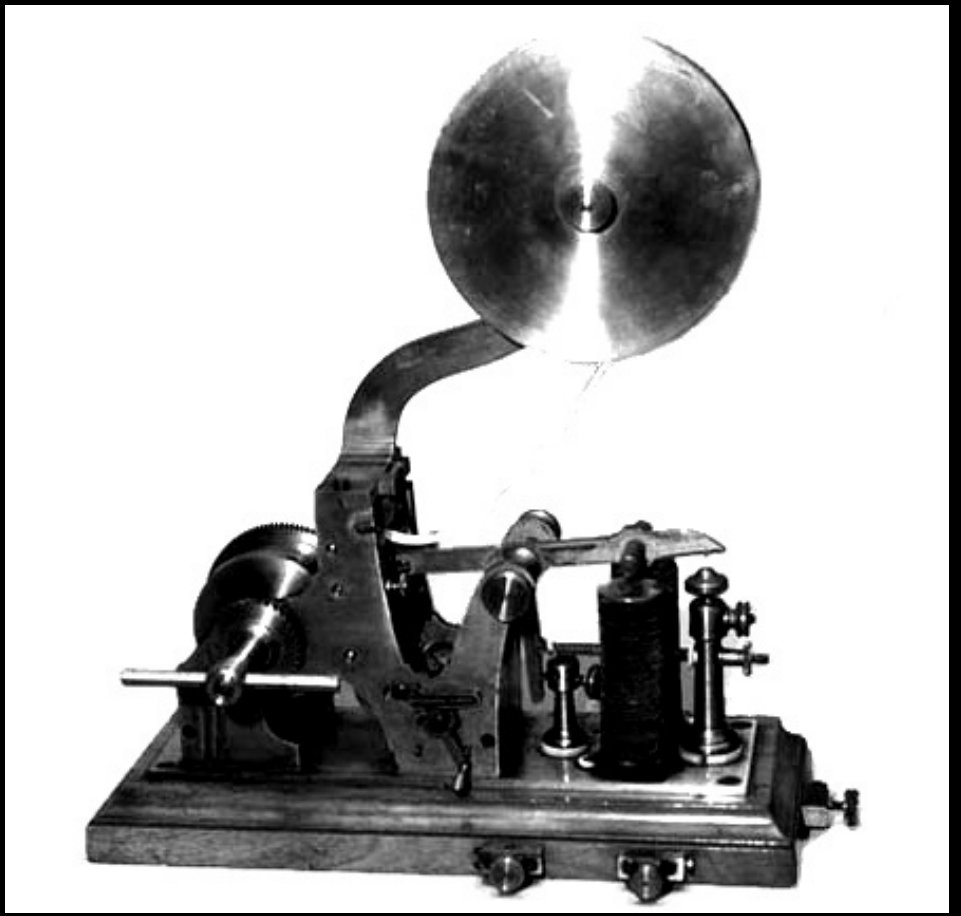
il telegrafo Morse

- Basato sul relé
  - 1836

    Joseph Henry
    Samuel Morse
    Alfred Vail
  - 1844

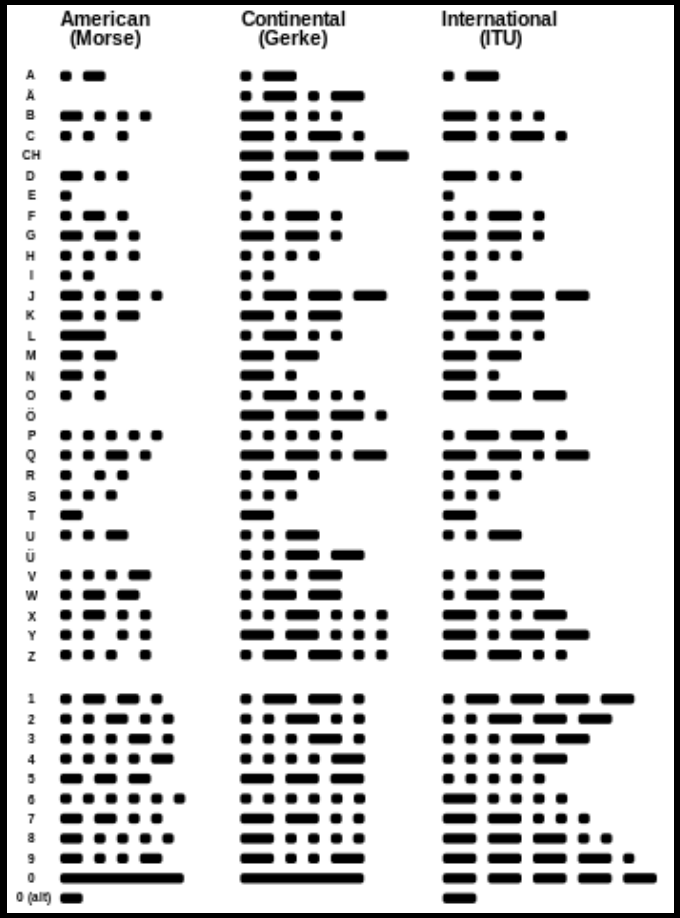
    inizio servizi
  - 1861

    costa-costa in USA



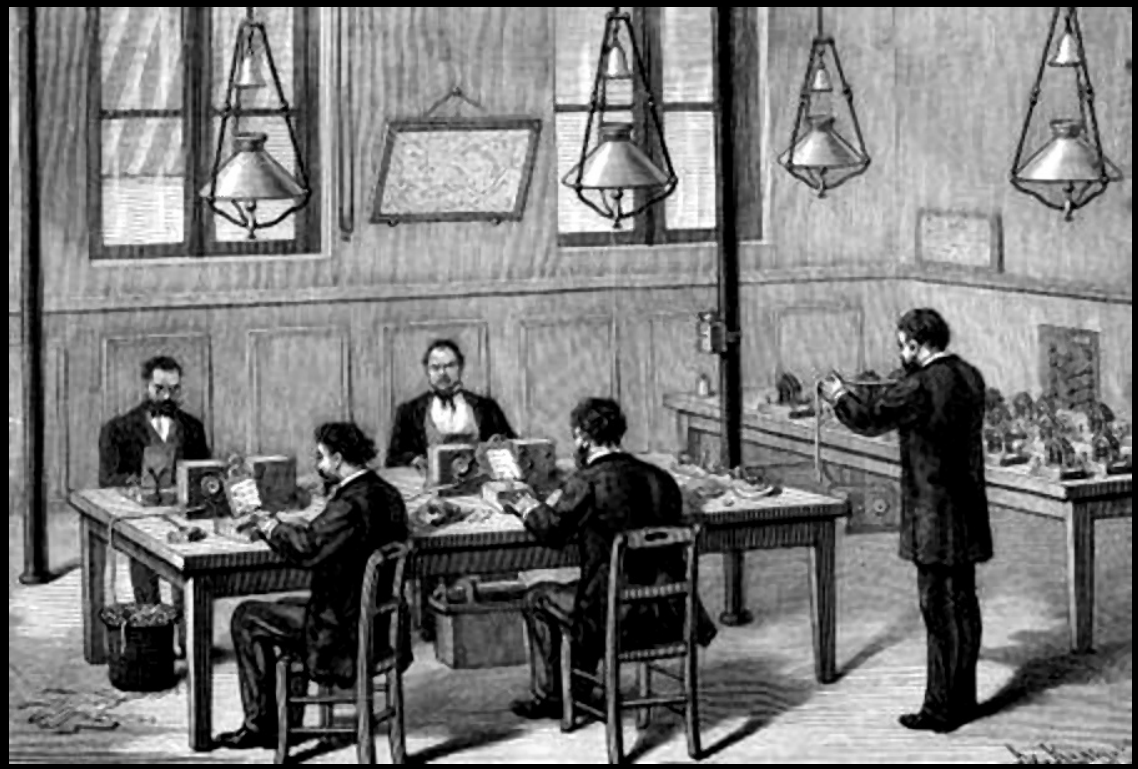
la codifica Morse

- Codifica su 5 simboli
  - Costruita sul tempo e sul circuito aperto/chiuso
  - *dit*, unità minima
  - 1 dit on, *dot*
  - 3 dit on, *dash*
  - 1 dit off, *dit-dash gap*
  - 3 dit off, *short gap*
  - 7 dit off, *medium gap*



la codifica Baudot

- Codifica su 5 bit
  - Emile Baudot
  - Brevetto 1874
  - Inizialmente a mano

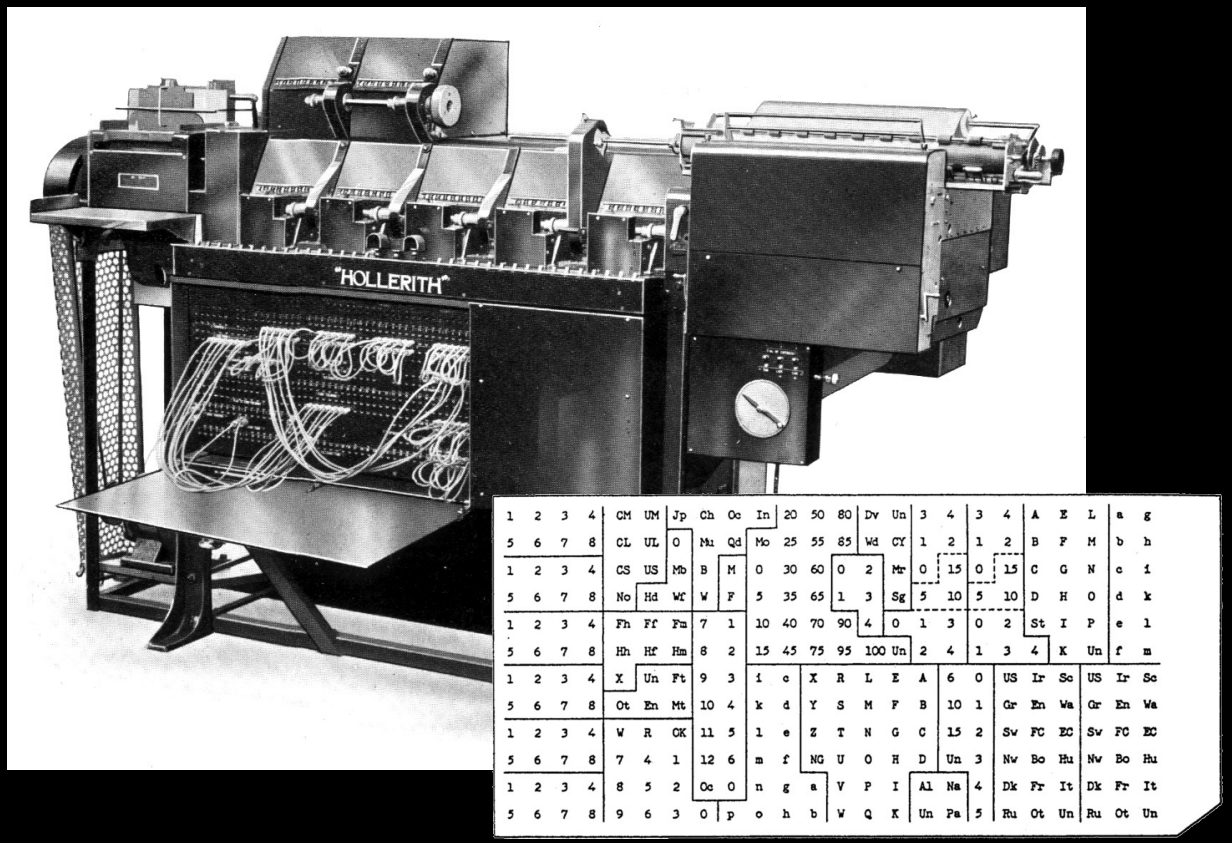


buchi su carta

- Il telaio Jacquard, 1801
  - Codifica di disegni
  - Programmazione dei movimenti di macchina
  - Digitale
  - Sincrono
  - Sabotabile come i predecessori

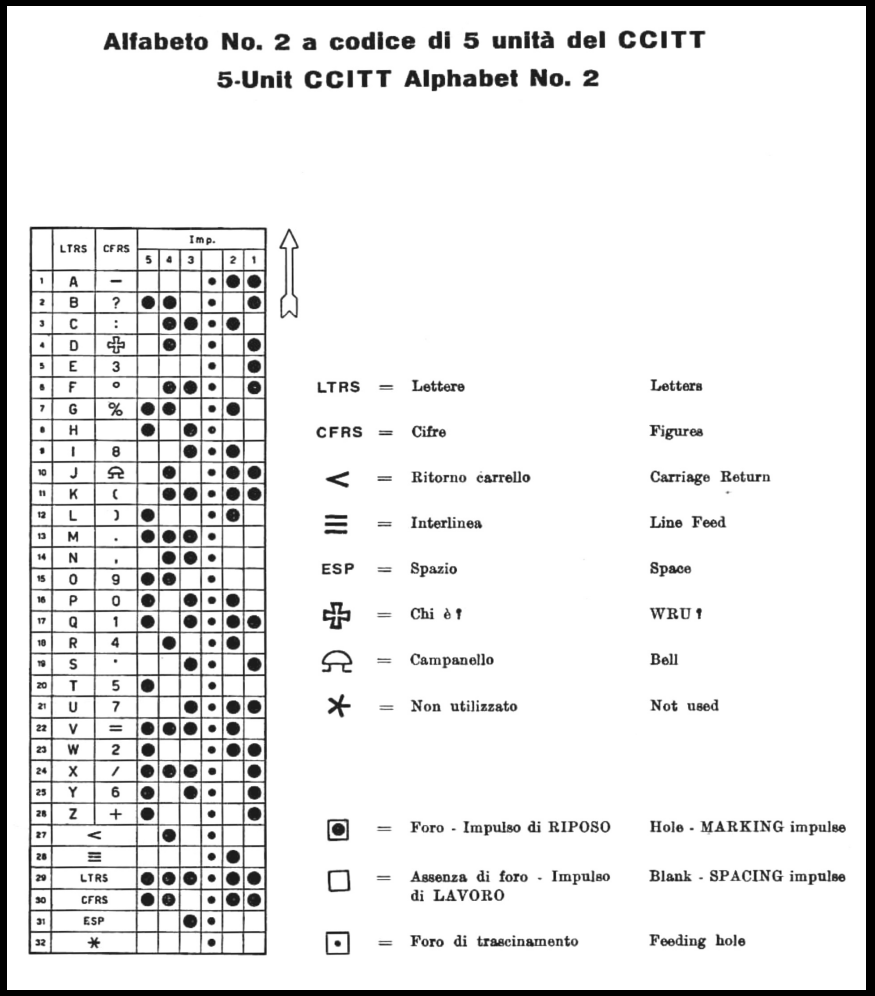
altri buchi

- Hollerit
  - 1890
  - Censimento federale
  - Codifica per elaborare



finalmente standard

- CCITT ITA2
  - Comité Consultatif International Téléphonique et Télégraphique
  - International Telegraph Alphabet
  - Dagli Anni ’30



Alfabeto No. 2 a codice di 5 unità del CCITT
5-Unit CCITT Alphabet No. 2

	LTRS	CFRS	Imp. 5	4	3		2	1
1	A	–				●	●	●
2	B	?	●	●		●		●
3	C	:		●	●	●	●	
4	D	WRU		●		●		●
5	E	3				●		●
6	F	°		●	●	●		●
7	G	%	●	●		●	●	
8	H		●		●	●		
9	I	8			●	●	●	
10	J	BELL		●		●	●	●
11	K	(		●	●	●	●	●
12	L	)	●			●	●	
13	M	.	●	●	●	●		
14	N	,		●	●	●		
15	O	9	●	●		●		
16	P	0	●		●	●	●	
17	Q	1	●		●	●	●	●
18	R	4		●		●	●	
19	S	'			●	●		●
20	T	5	●			●		
21	U	7			●	●	●	●
22	V	=	●	●	●	●	●	
23	W	2	●			●	●	●
24	X	/	●	●	●	●		●
25	Y	6	●		●	●		●
26	Z	+	●			●		●
27	<			●		●		
28	≡					●	●	
29	LTRS		●	●	●	●	●	●
30	CFRS		●	●		●	●	●
31	ESP				●	●		
32	*					●		

LTRS = Lettere — Letters
CFRS = Cifre — Figures
< = Ritorno carrello — Carriage Return
≡ = Interlinea — Line Feed
ESP = Spazio — Space
WRU = Chi è ? — WRU ?
BELL = Campanello — Bell
* = Non utilizzato — Not used

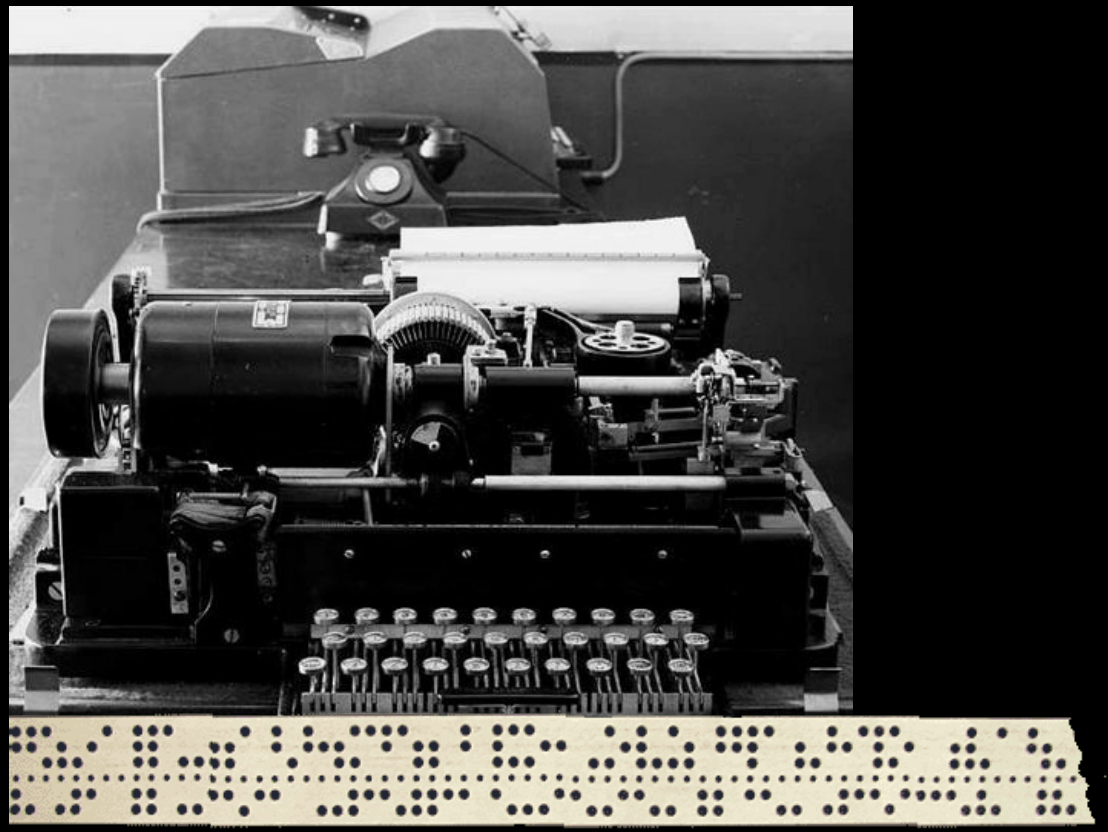
● = Foro - Impulso di RIPOSO — Hole - MARKING impulse
□ = Assenza di foro - Impulso di LAVORO — Blank - SPACING impulse
⊡ = Foro di trascinamento — Feeding hole

ticker tape

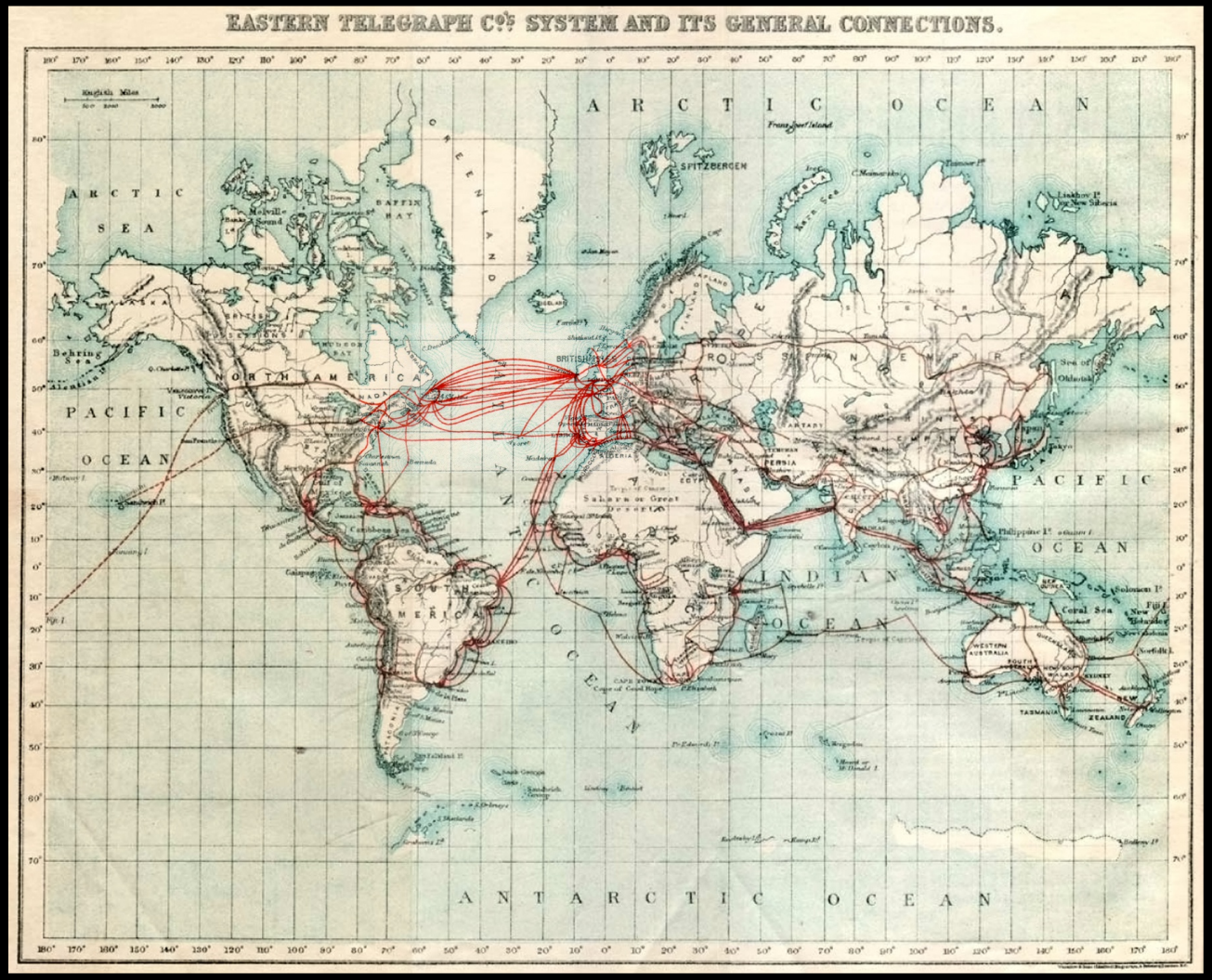
- Servizio
  - Informazione finanziaria in tempo reale
  - Dal 1870 al 1970
  - Fuori mercato con Bloomberg

telescriventi

- 1901
  - Donald Murray
  - Standard per i servizi telegrafici



internet vittoriana

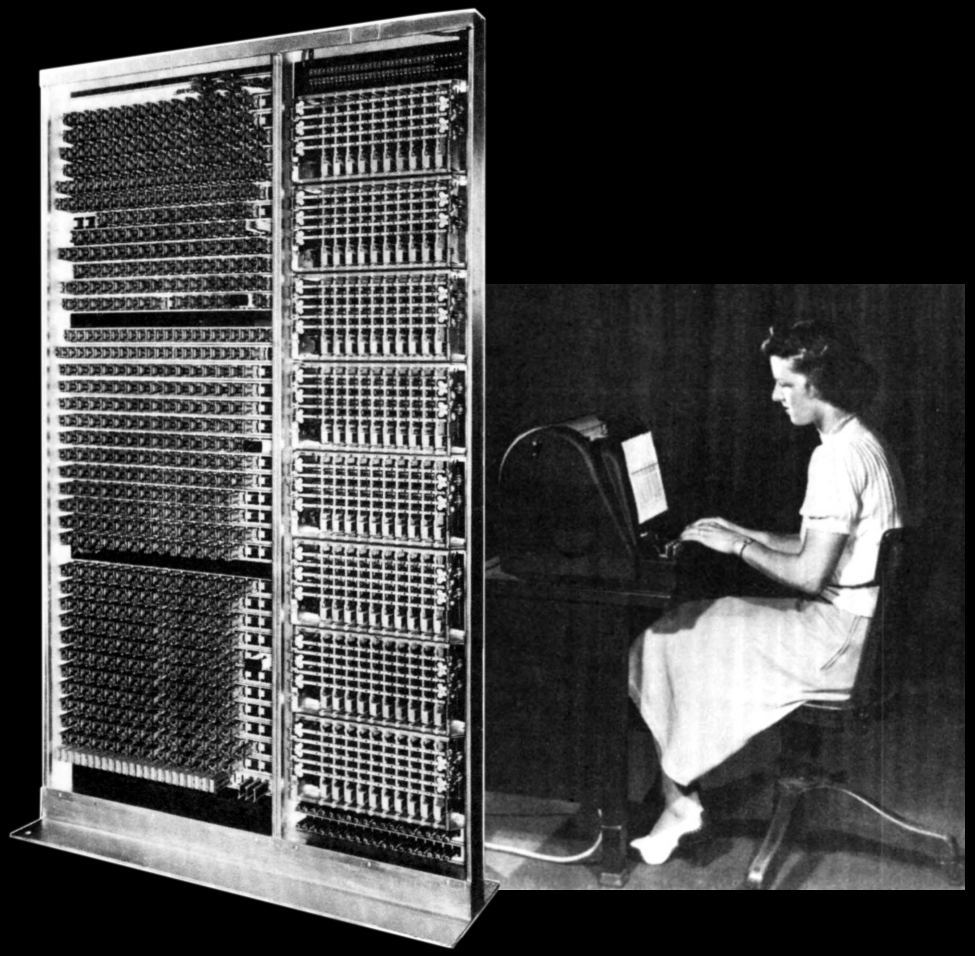


nuovi cifrari

- Lorenz SZ 40/42
  - Cifrario Vernam, xor con valore pseudocasuale
  - Trasparente
  - Su alfabeto ITA2
  - Comunicazioni strategiche

reti di calcolatori

- CNC, 1940
  - George Stibitz
  - In rete, naturalmente

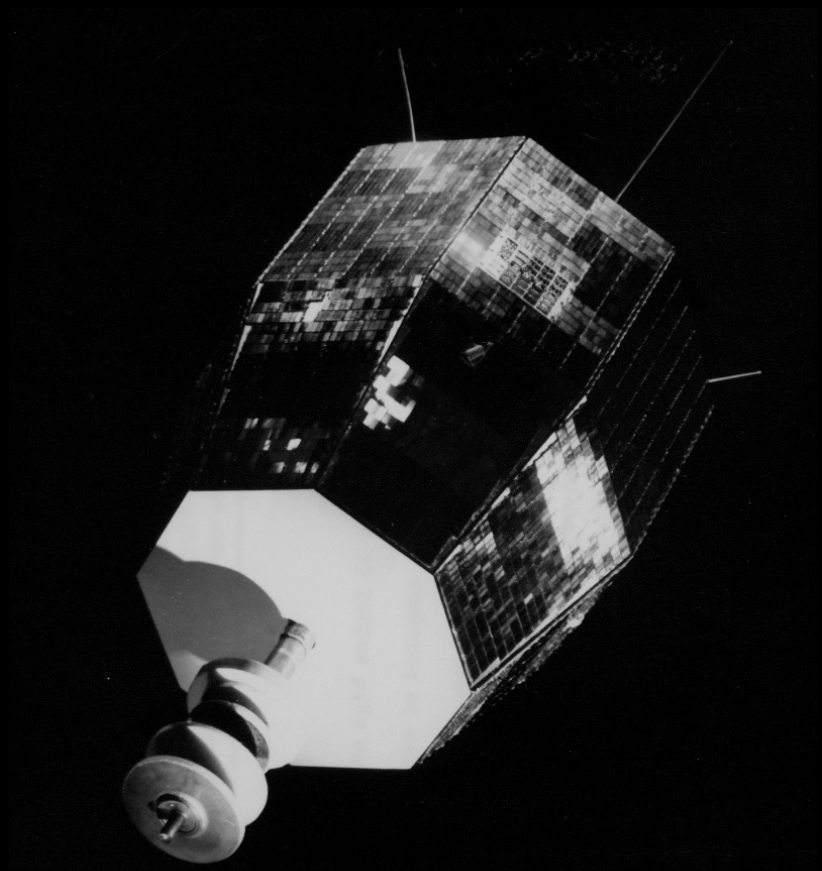


internet dei protocolli

- I 4 nodi
  - Univ. Cal. Los Angeles
    SDS Sigma, L. Kleinrock
  - Stanford Research Institute
    SDS 940, D.C. Engelbart
  - Univ. Cal. Santa Barbara
    IBM 360/75, G. Culler
  - University of Utah
    PDP10, I.E. Sutherland

false robustezze

- Relay 1 e Telstar1
  - Lanciati nel 1962
  - Tuttora in orbita
  - Operativi per poco tempo
  - Per... fuoco amico



1975, ultimi buchi