The Imagination Game

storia e fantasia
in The Imitation Game

Cap. 3: L'Enigma

Giovanni A. Cignoni

L'Enigma (dal vivo)

- La storia, i modelli
- Come funzionava
  - L'idea, le parti, i meccanismi
  - Le procedure e le convenzioni d'uso
- Come fu battuta
  - Da Rejewski & C. a Turing & C.
  - Le Bombe, polacche, inglesi e americane

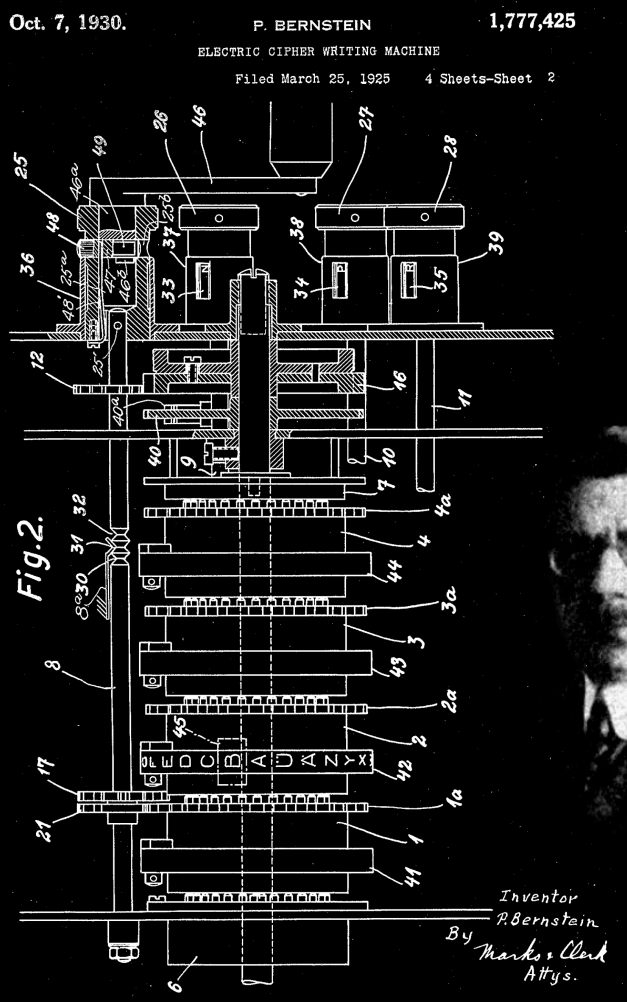
Giovanni A. Cignoni

Entra la dark lady

Giovanni A. Cignoni

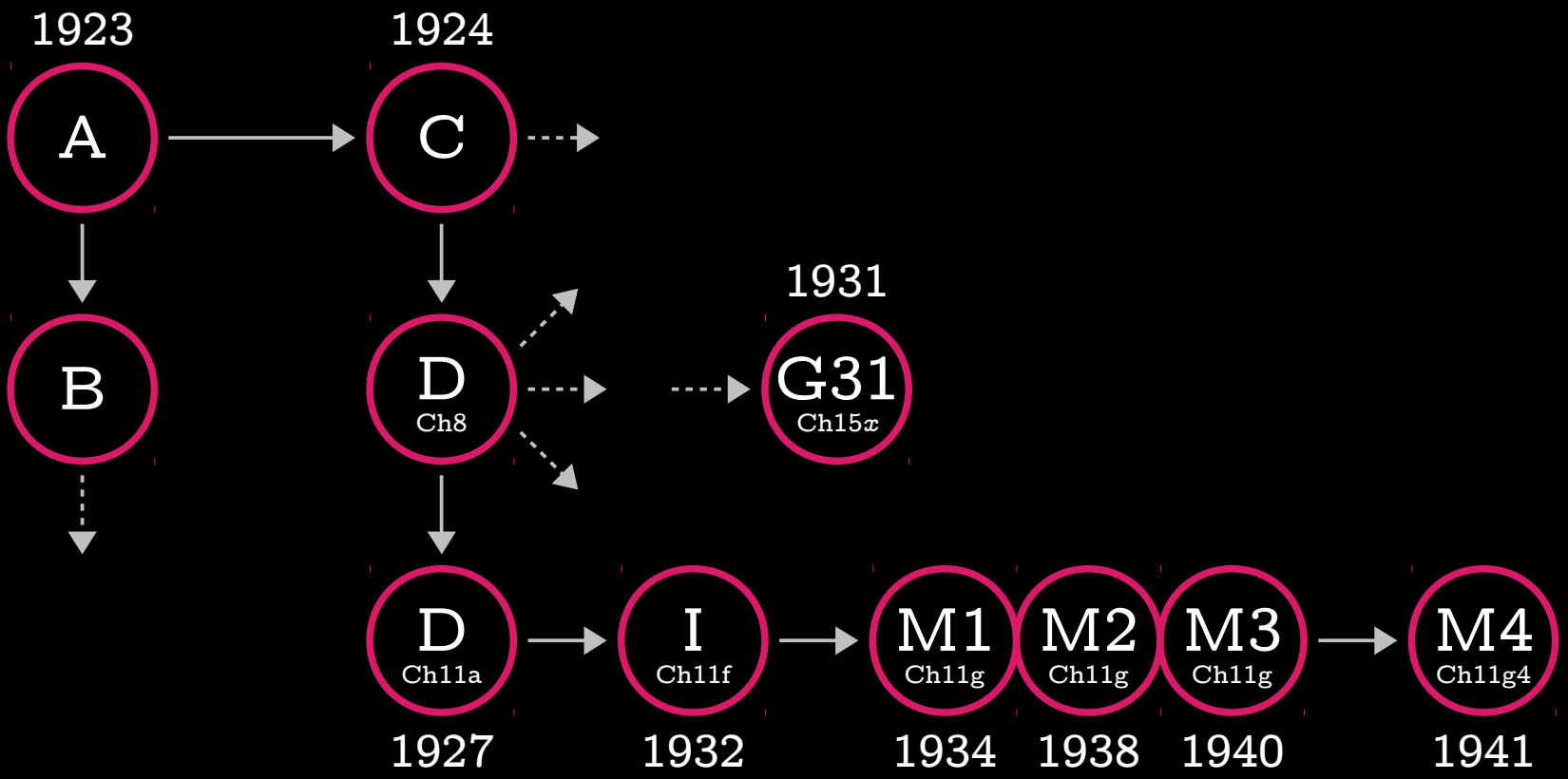
Enigma, non così segreta...

- Nasce commerciale
  - Arthur Scherbius, Chiffriermaschinen AG
  - Hugo Alexander Kock, Paul Bernstein, Willi Korn
- Brevettata
  - Dal 1918, Germania
  - Dal 1919, Olanda, UK
  - Dal 1920, Francia, USA
  - Dal 1921, Svizzera



Giovanni A. Cignoni

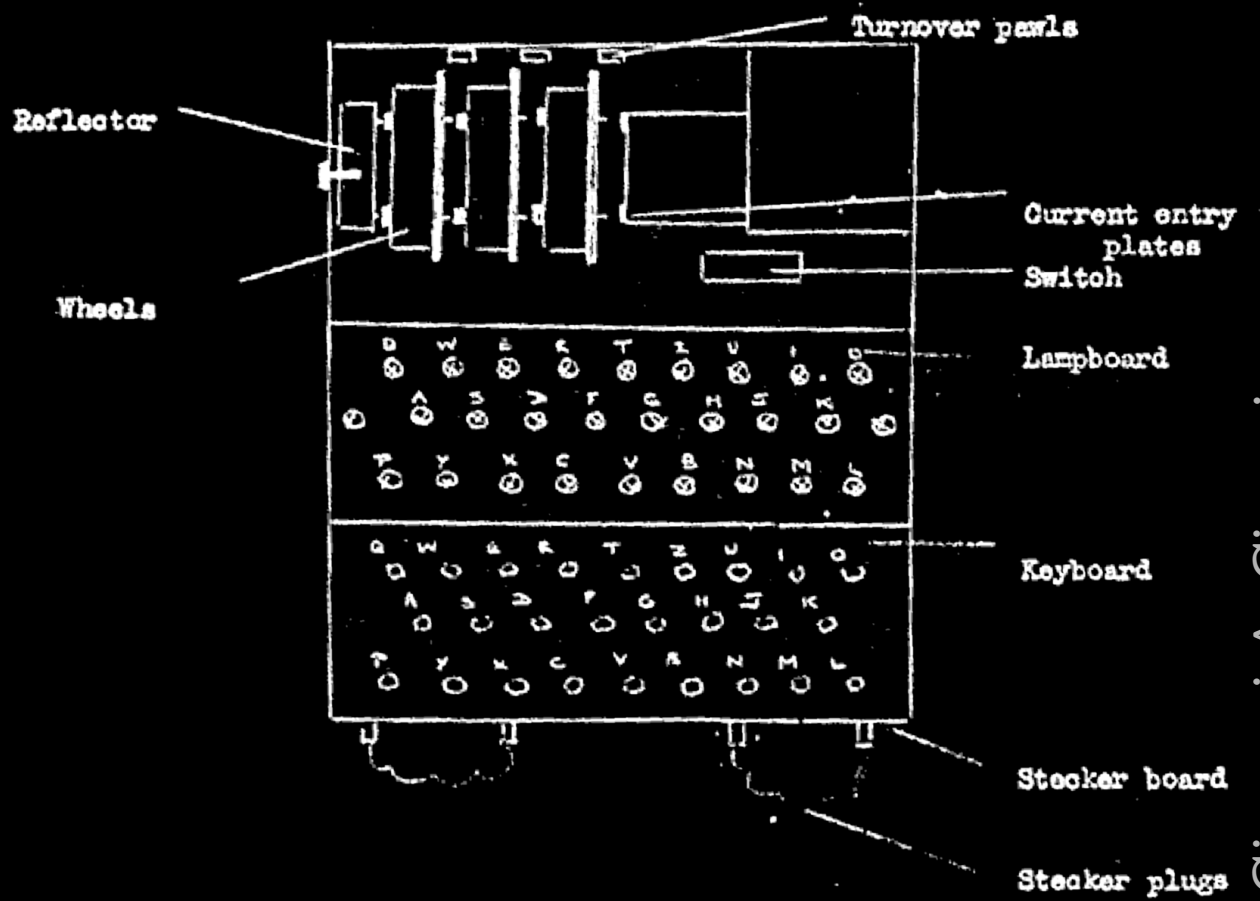
… non una



Giovanni A. Cignoni

Le parti della macchina

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

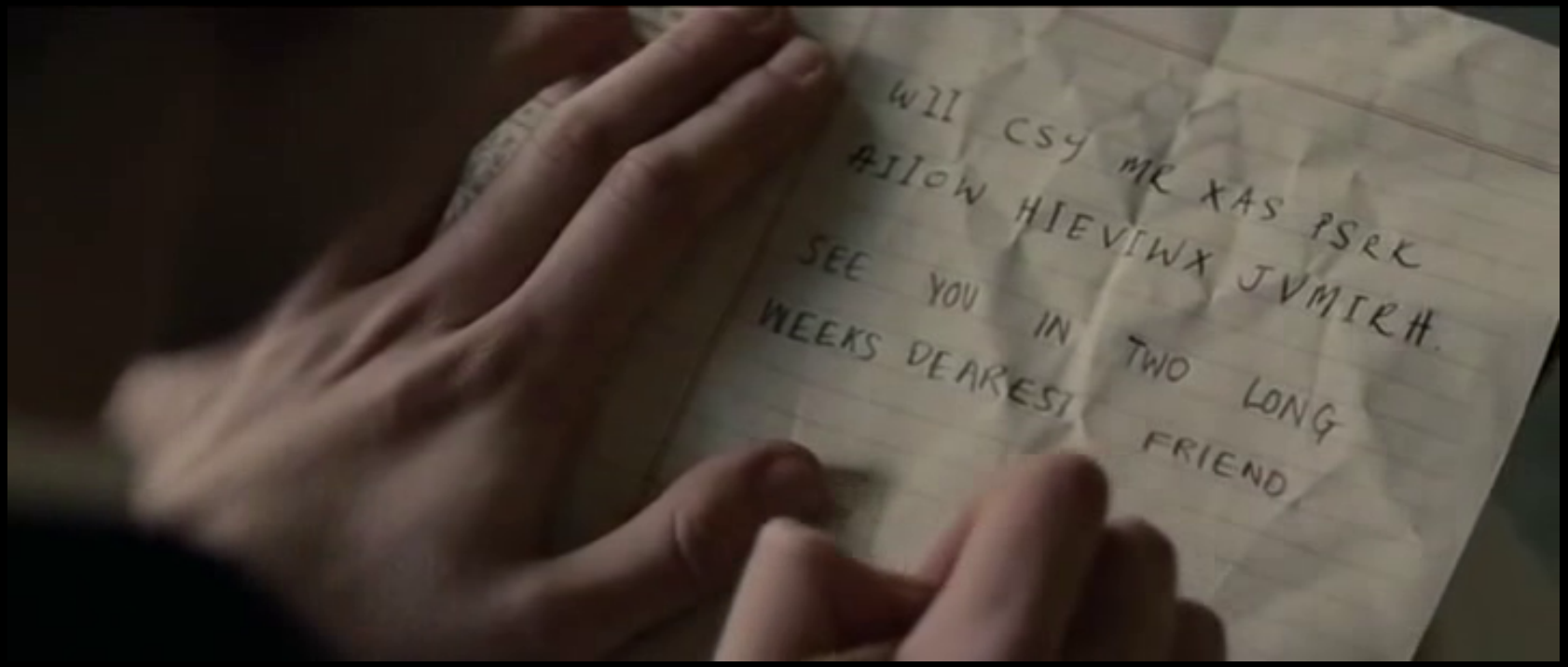


Due pillole di crittografia

- Cifrari monoalfabetici
  - Codice Morcom-Turing
  - `ABCDEFGHIJKLMNOPQRSTUVWXYZ`
    `E..HIJK.M.OP.RS..VWXY.A.C.`
- Cifrari polialfabetici
  - Alberti/Trithemius/Bellaso/Vigenère, *tabula recta*
  - `ABCDEFGHIJKLMNOPQRSTUVWXYZ`
    `BCDEFGHIJKLMNOPQRSTUVWXYZA`
    `CDEFGHIJKLMNOPQRSTUVWXYZAB`
    `DEFGHIJKLMNOPQRSTUVWXYZABC`
    ...

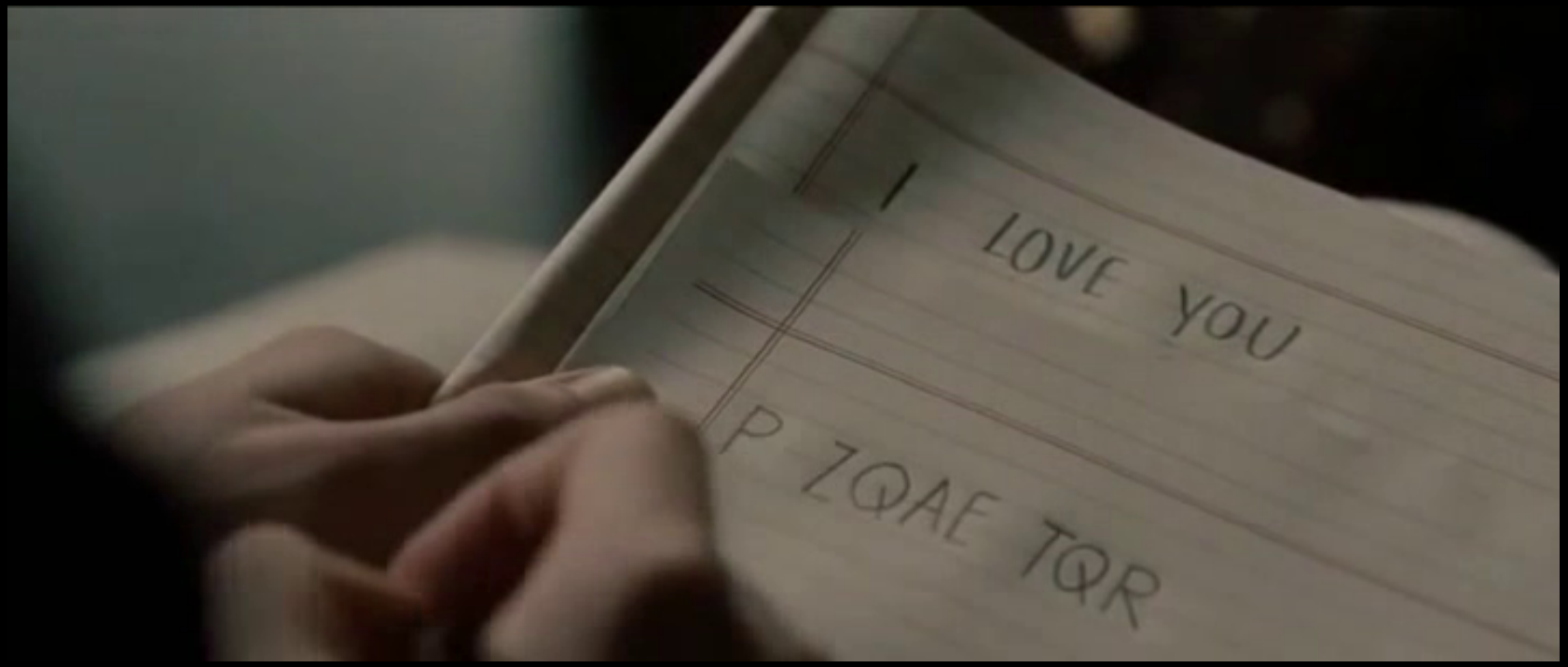
Giovanni A. Cignoni

Morcom-Turing



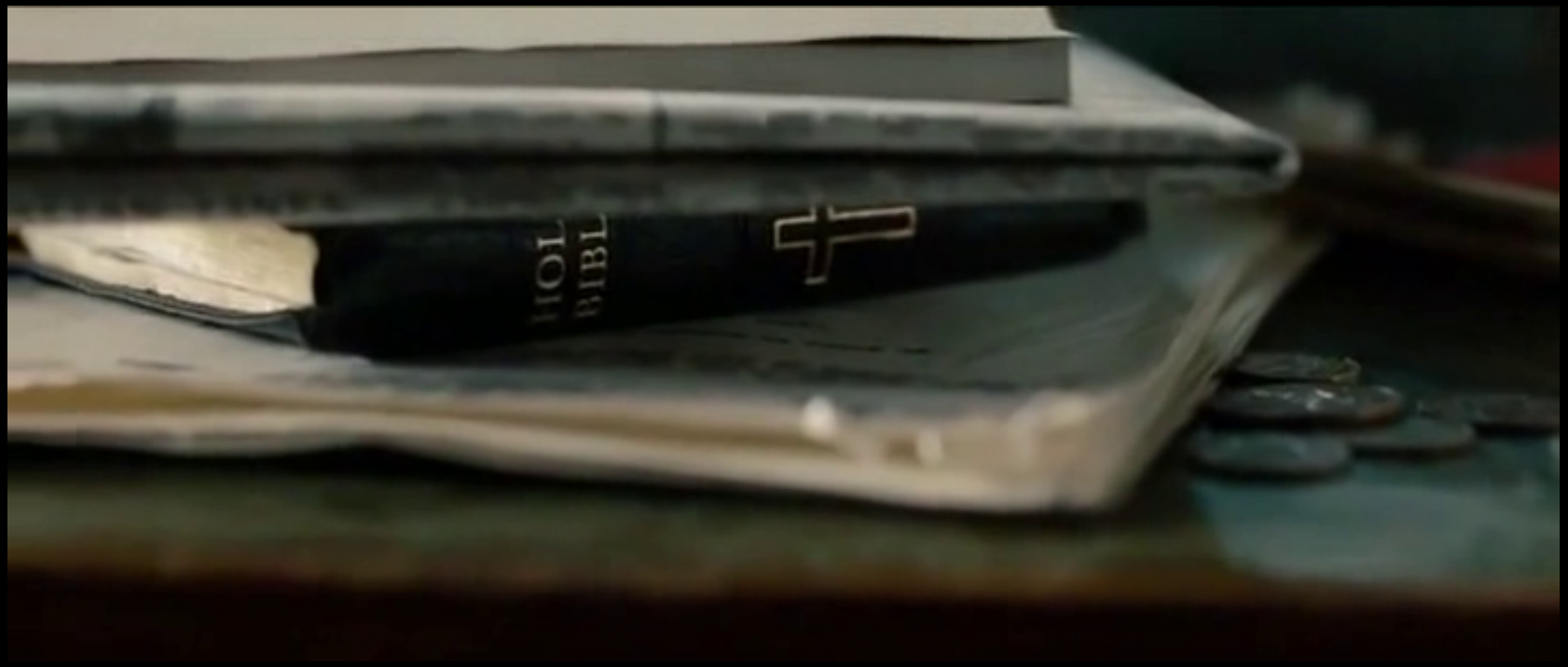
Giovanni A. Cignoni

Turing-Morcom



Giovanni A. Cignoni

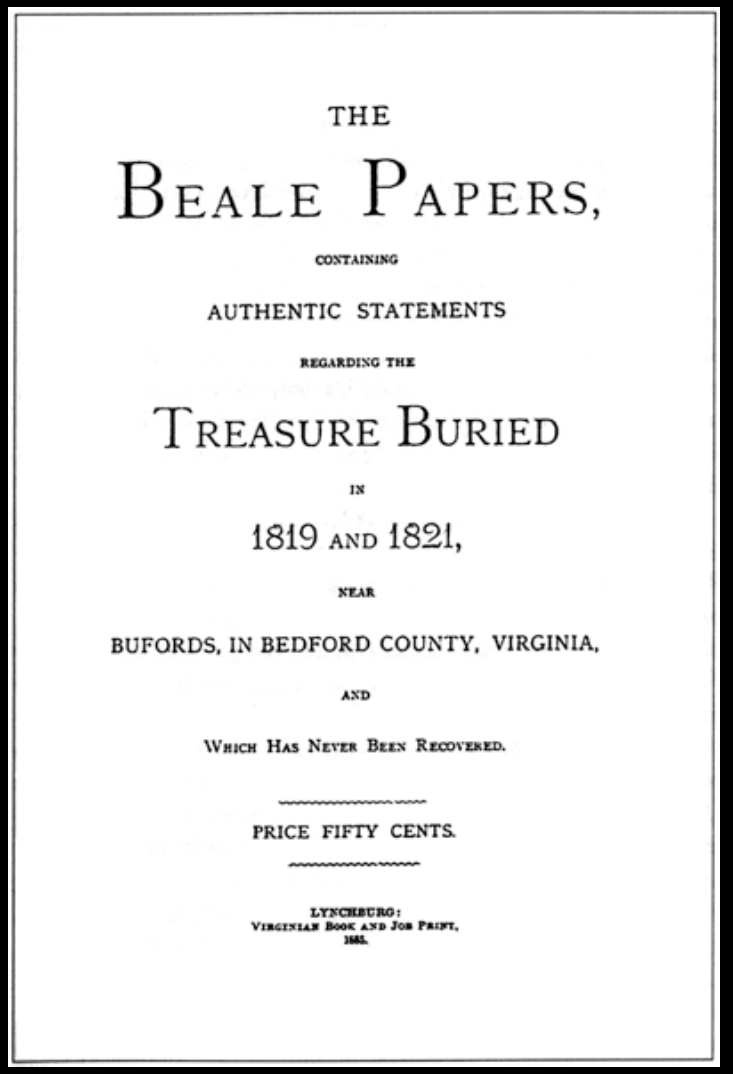
Una divagazione...



Giovanni A. Cignoni

Il cifrario Beale

- Una storia di tesori
  - Tre testi cifrati
  - Uno, il secondo, risolto
    “When in the course...”
  - Gli altri due no,
    quelli mportanti, ovvio
- Una probabile beffa
  - Comunque appassionante
  - E molti ancora scavano...



THE

BEALE PAPERS,

CONTAINING

AUTHENTIC STATEMENTS

REGARDING THE

TREASURE BURIED

IN

1819 AND 1821,

NEAR

BUFORDS, IN BEDFORD COUNTY, VIRGINIA,

AND

WHICH HAS NEVER BEEN RECOVERED.

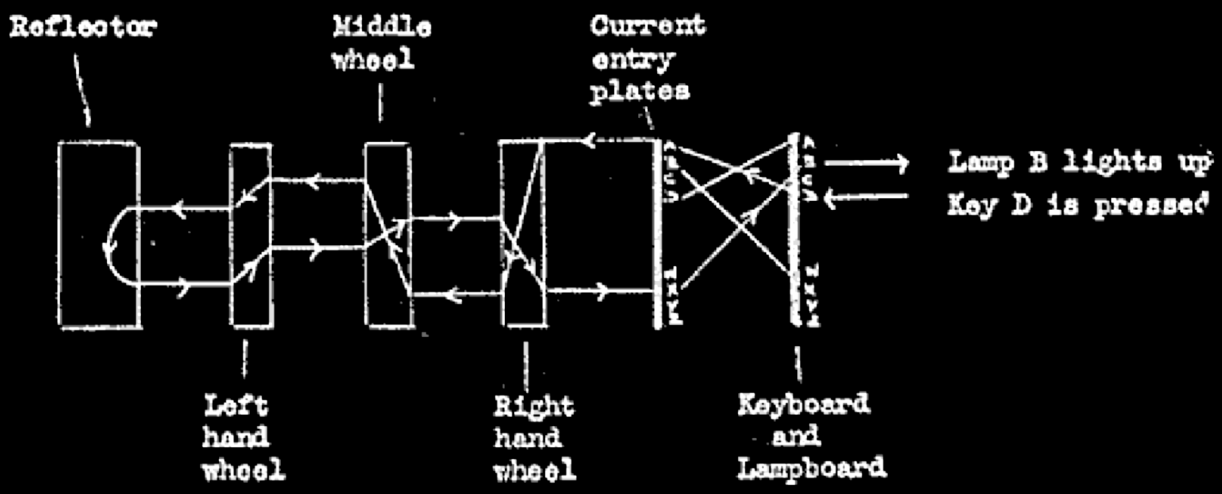
PRICE FIFTY CENTS.

LYNCHBURG:
VIRGINIAN BOOK AND JOB PRINT,
1885.

Giovanni A. Cignoni

Come funziona

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



Giovanni A. Cignoni

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

Giovanni A. Cignoni

1941, Enigma M4

- L'ultima
  - + Zusatswalze β e γ
  - Solo per gli U-Boot
- Cambiamenti nelle M
  - 1934, M1, rotori I, II, III
  - 1937, riflettore UKW-B
  - 1938, M2, + IV e V
  - 1939, + VI, VII e VIII, M3
  - 1941, riflettore UKW-C

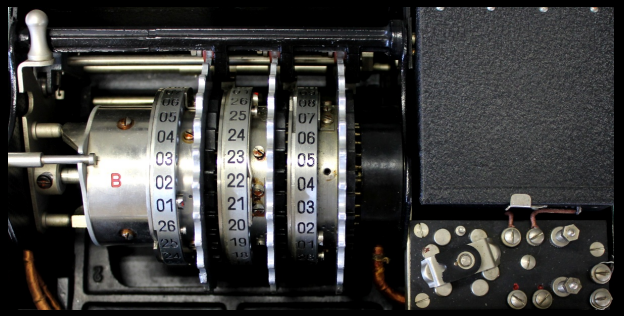
Giovanni A. Cignoni

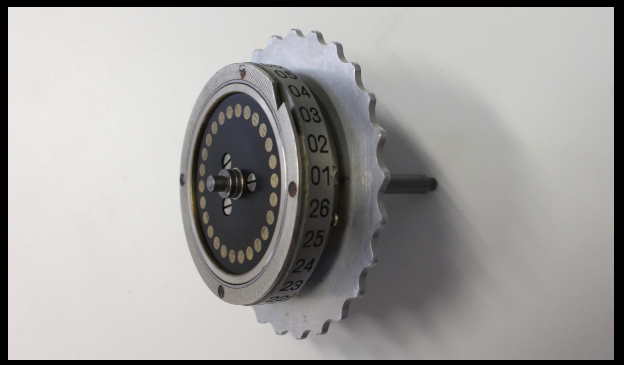
Le impostazioni, nel film

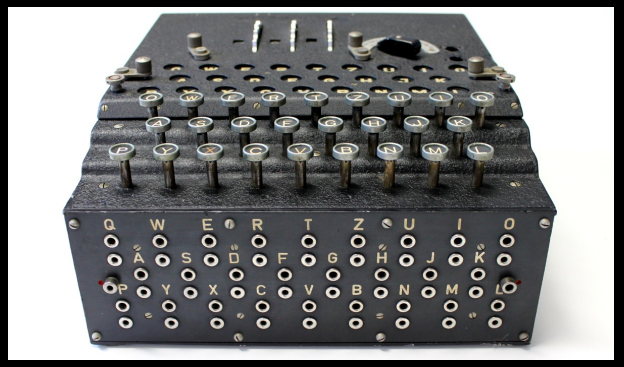
Giovanni A. Cignoni

Le impostazioni

- Giornaliere
  - Walzenlage,
  - Ringstellung
  - Steckerverbindungen
  - La tabula recta generata
- Per messaggio
  - Grundstellung
  - La riga della tabula recta da cui iniziare







Giovanni A. Cignoni

Le combinazioni

Enigma I – 1.589×10^{20}		
Walzenlage	5x4x3	60
Ringstellung	26x26x26	17 576
Steckerverbindungen	10 su 13	150 738 274 900 000

Enigma M4 – 4.628×10^{22}		
Walzenlage	8x7x6	336
Ringstellung	26x26x26	17 576
Zusatswalze	2x26	52
Steckerverbindungen	10 su 13	150 738 274 900 000

Giovanni A. Cignoni

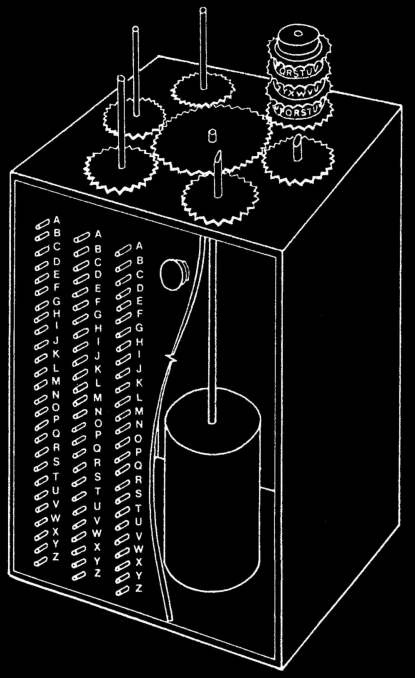
Come attaccare Enigma

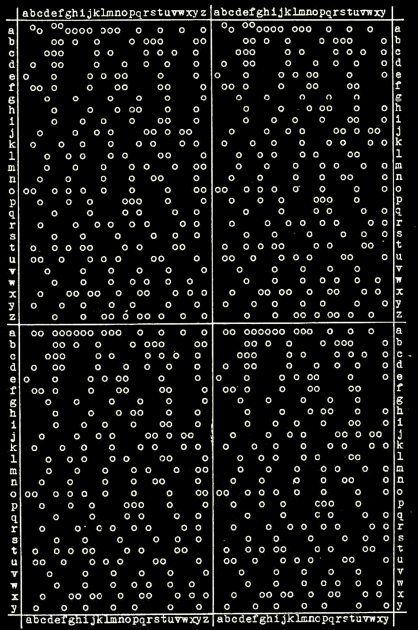
- Le combinazioni sono tante, ma tante
  - Metodi, per ridurre lo spazio di ricerca
  - Macchine, molte, per le combinazioni che restano

Giovanni A. Cignoni

I Polacchi dimenticati

- Metodi e macchine
  - Marian Rejewski
  - Henryk Zygalski, Jerzy Rozycki

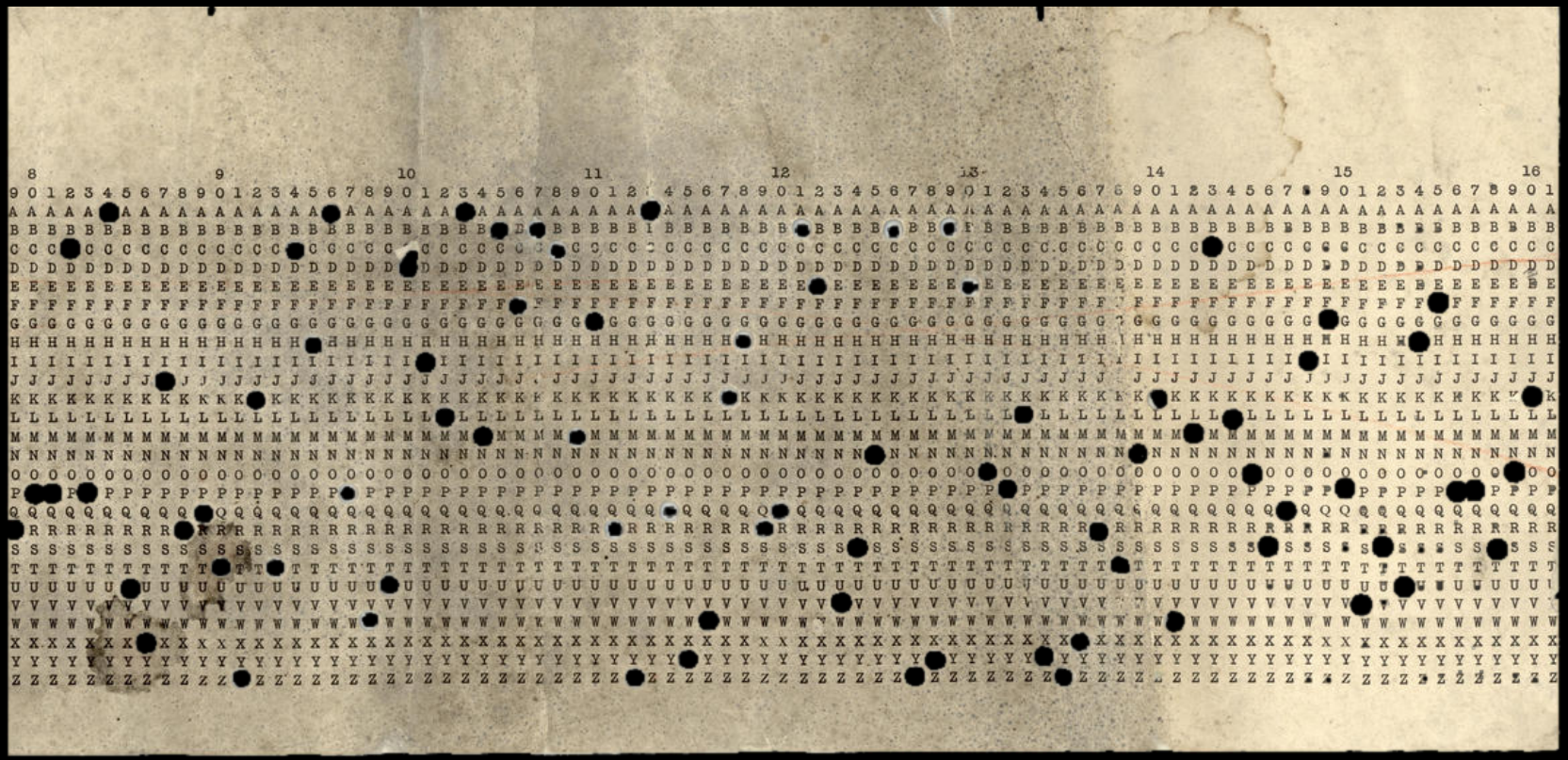




... ma citati

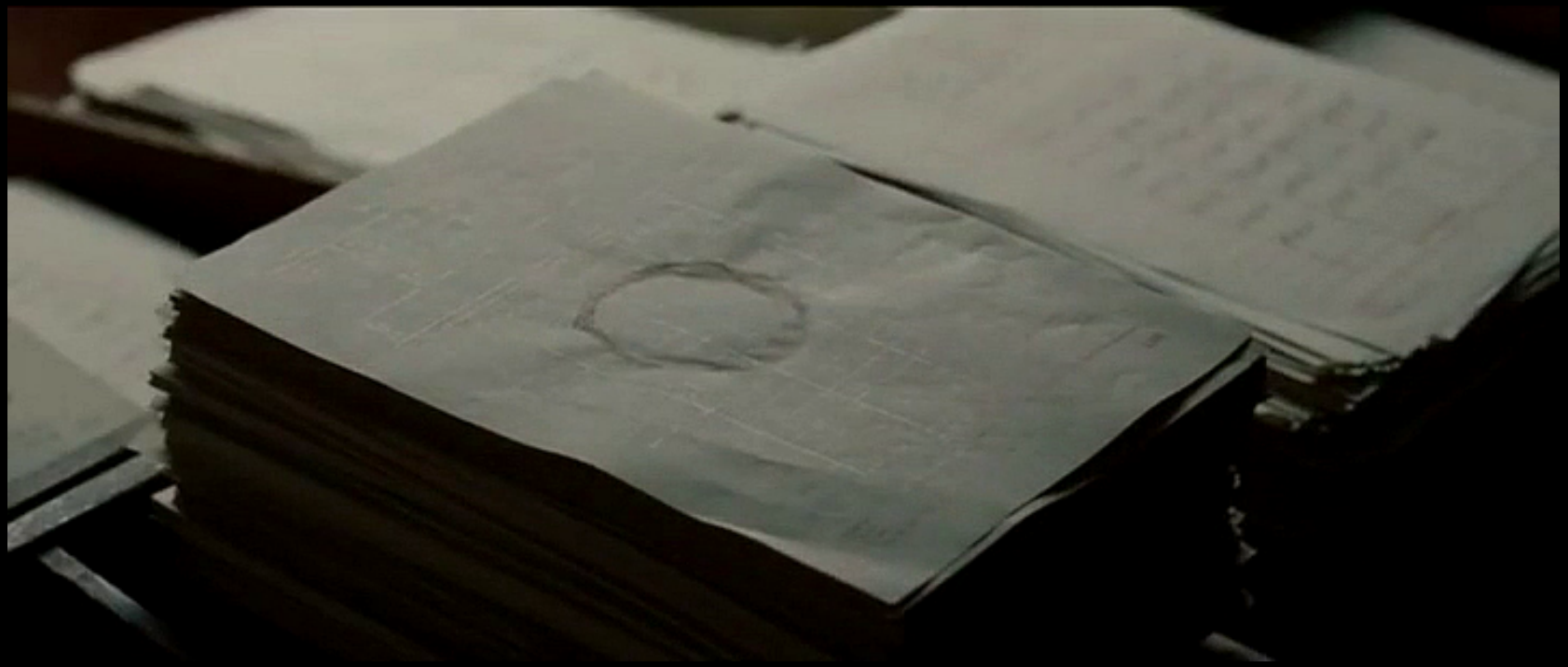
Giovanni A. Cignoni

Banburismus



Giovanni A. Cignoni

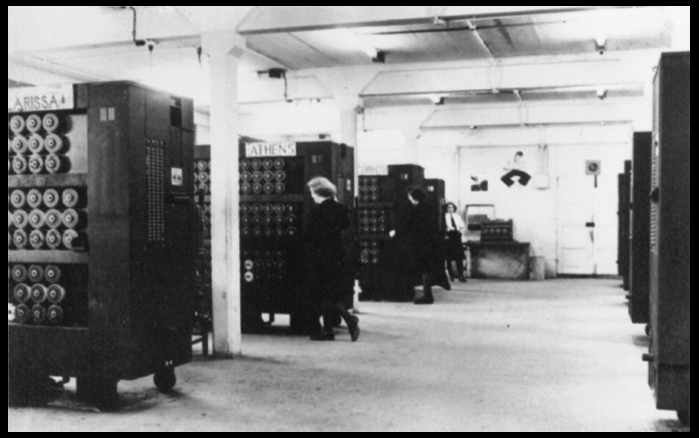
Macchie di tè

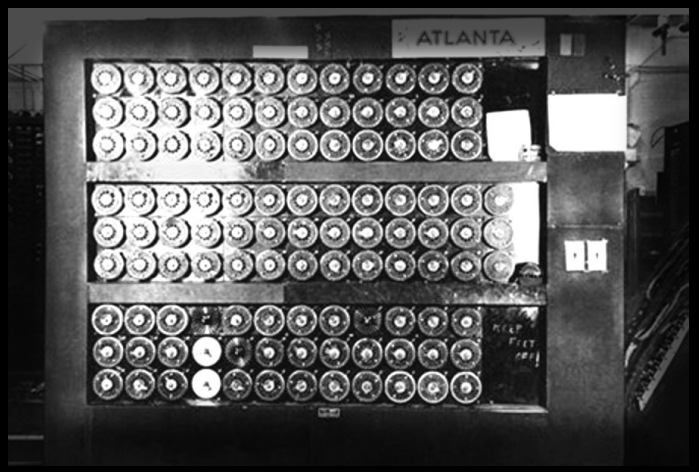


Giovanni A. Cignoni

Le Bombe inglesi

- Progettisti
  - Turing, dalle idee polacche
  - Harold “Doc” Keen, alla BTM
  - Gordon Welchman, la *diagonal board*
- Una? Christopher?
  - Victory e Agnus Dei
  - Cobra & Mammoth
  - 152 + 57, BP e dintorni





Giovanni A. Cignoni

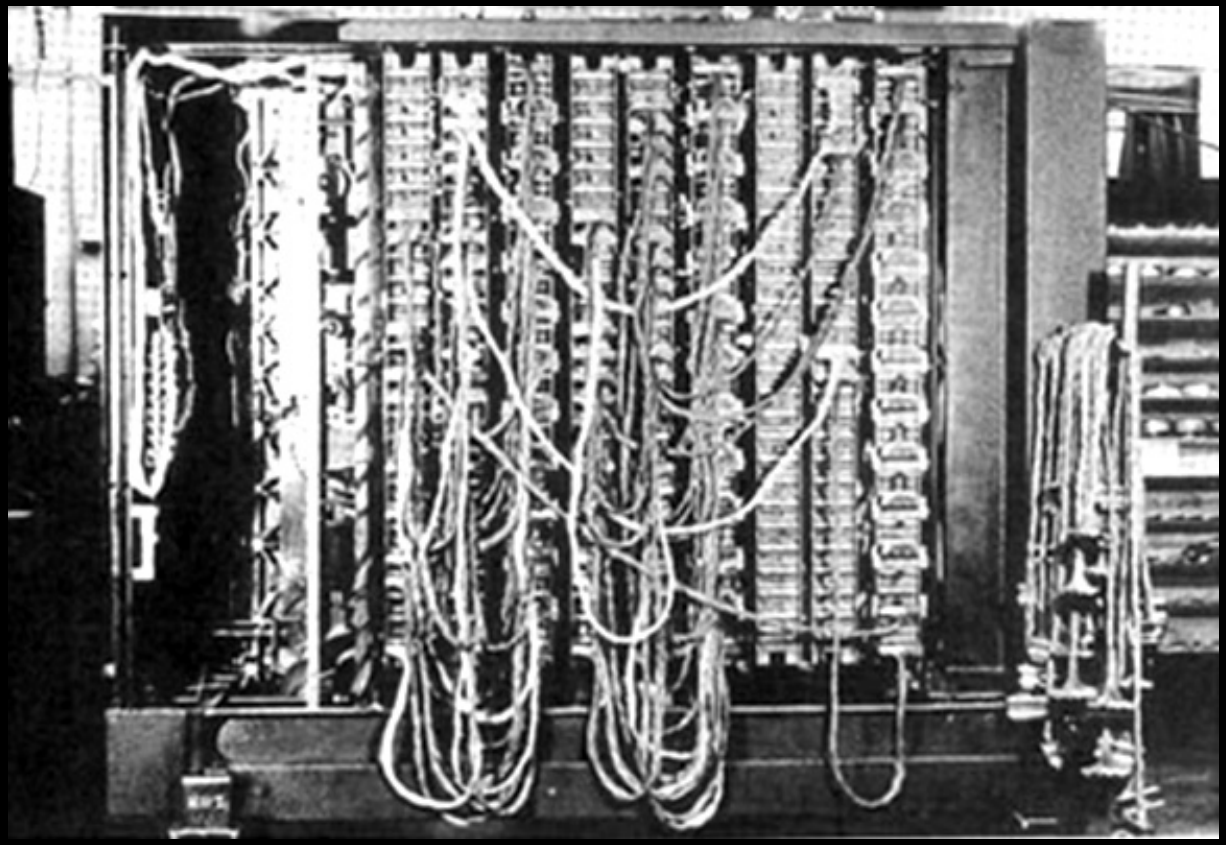
Impostare il menù, i rotori...

Giovanni A. Cignoni

... e i crib

Giovanni A. Cignoni

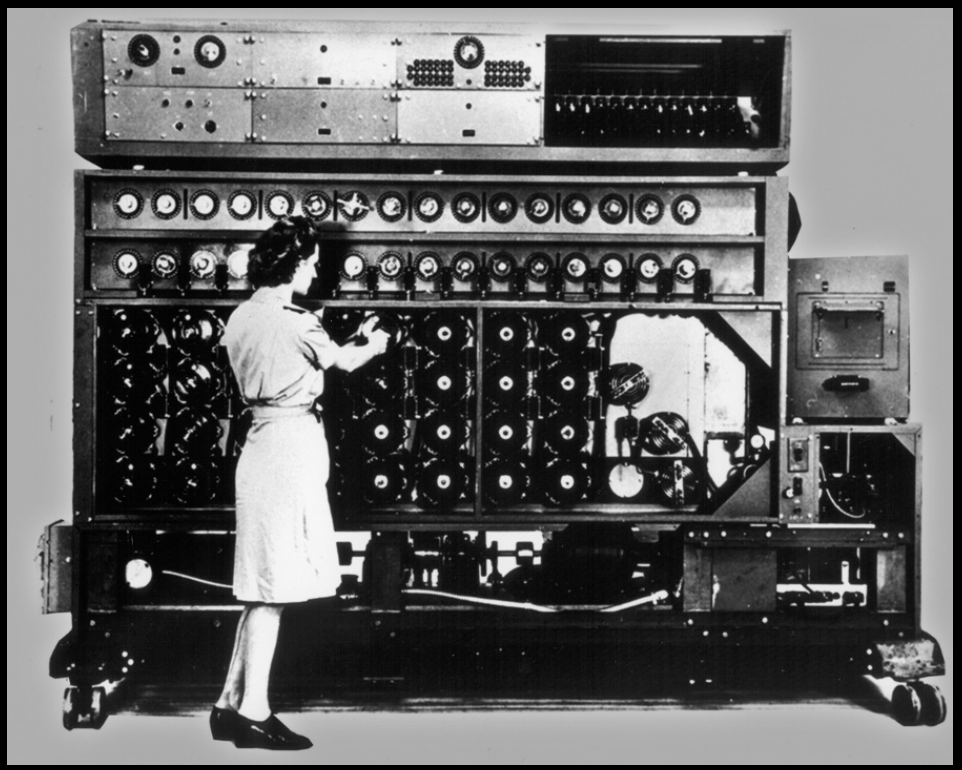
Un po’ più di cavi, in realtà



Giovanni A. Cignoni

Le Bombe americane

- Un progetto condiviso
  - Tiltman e Turing, in due missioni a Washington
  - Joseph Desch, US Navy / NCR
  - 160, meccaniche, con coincidenze elettroniche
  - Le prime due: Adam & Eve



Giovanni A. Cignoni

Di acqua ne è passata...

Quae si qui investigare et persequi velit,
quartam elementorum litteram,
id est D pro A et perinde reliquas commutet

Gaius Suetonius Tranquillus
(De vita Caesarum, Divus Julius, 56,6)

Giovanni A. Cignoni