

HISTORIA KOMPUTERÓW

2015/16

Bartosz Klin

`klin@mimuw.edu.pl`

`http://www.mimuw.edu.pl/~klin/`

Oś czasu

Turing



Shannon



Zuse



Atanasoff



Stibitz



Aiken

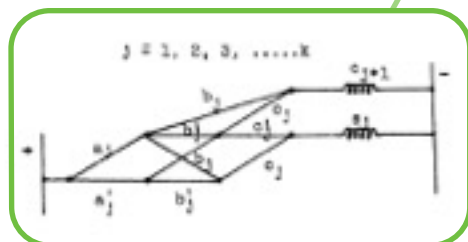
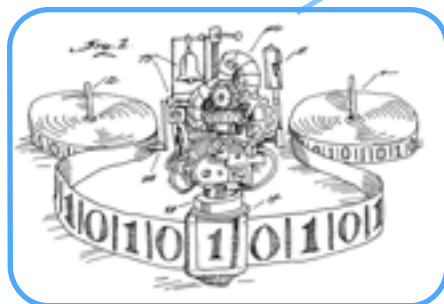


1930

1935

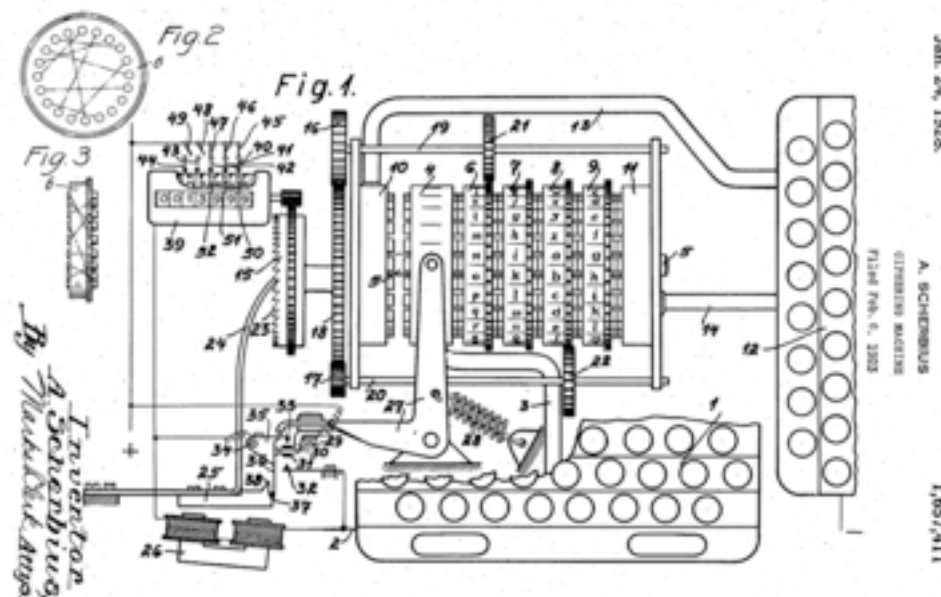
1940

1945



Enigma

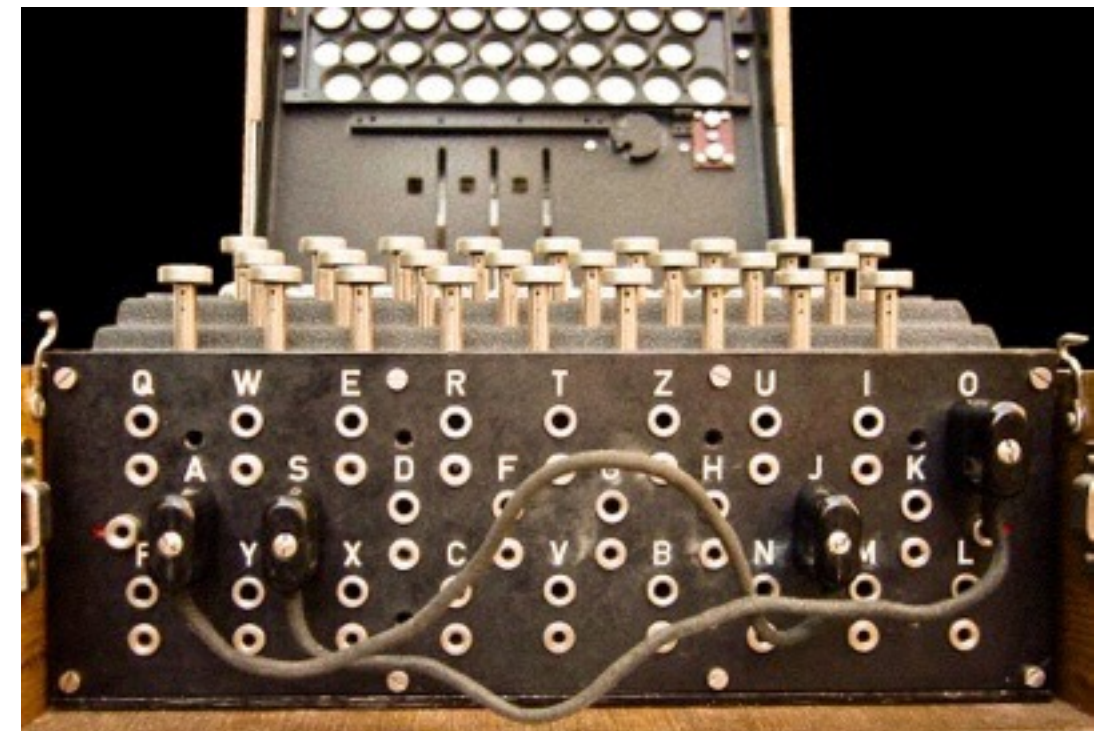
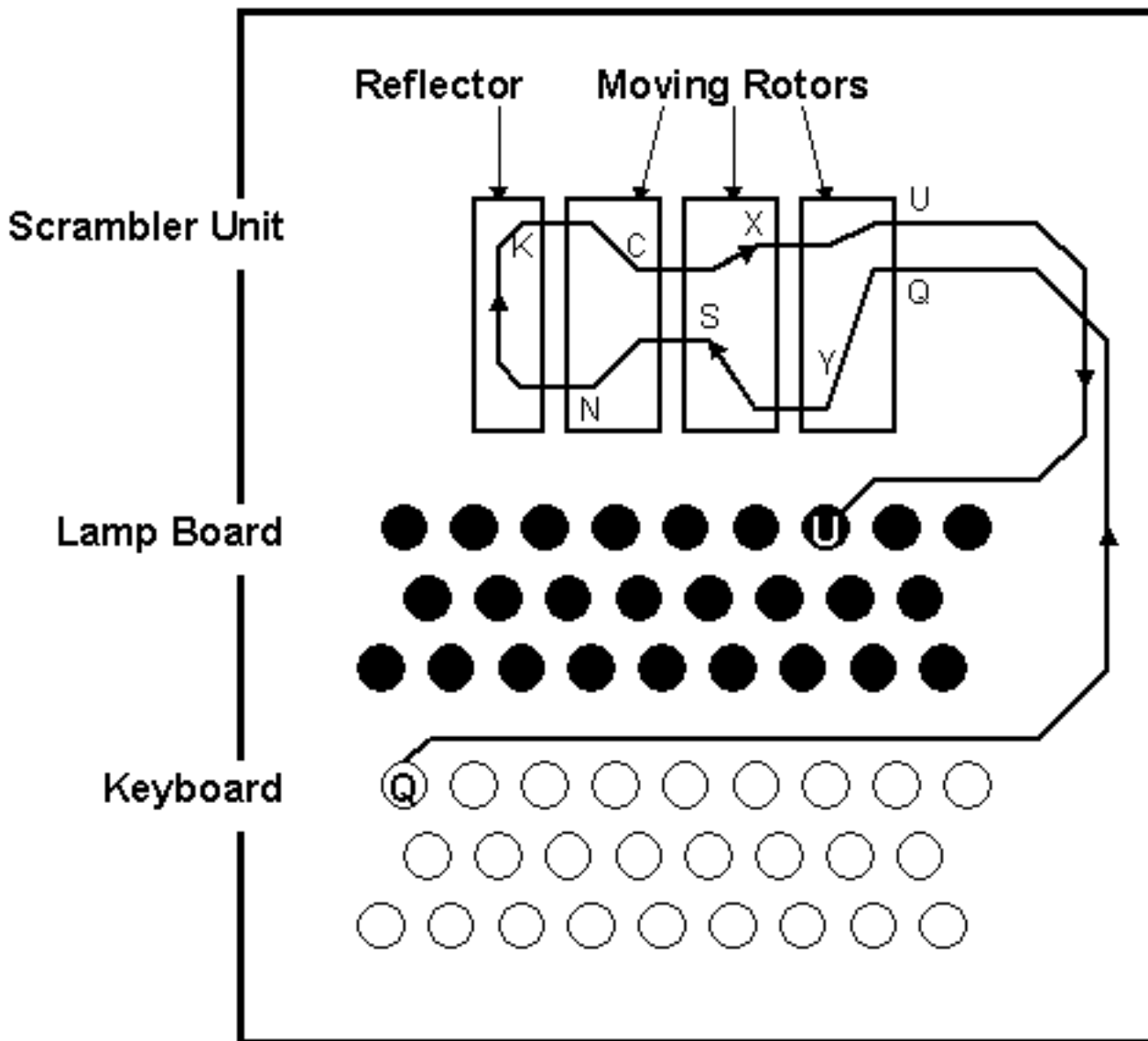
- elektromechaniczna maszyna szyfrująca
- wynalazek: A. Scherbius, 1918
- opatentowana w Niemczech, Anglii, USA



- zastosowania biznesowe
- od 1926 r., używana przez dyplomację i armię Niemiec



Struktura Enigmy



- prawy rotor obraca się przy każdej literze (z ew. przeniesieniem)

Pierwsze przełamania: Polskie Biuro Szyfrów

M. Rejewski (1905-80)

J. Różycki (1909-42)

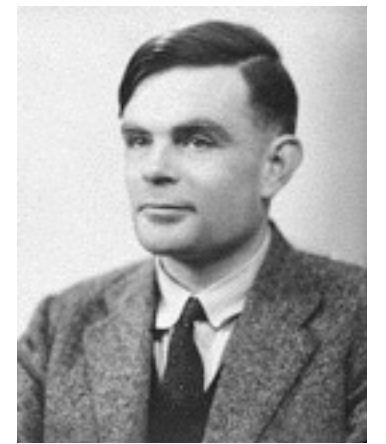
H. Zygański (1908-78)



- pracowali nad Enigmą od 1931 r.
- ustalili strukturę 3 rotorów i reflektora
- zbudowali kopie Enigmy (kilkadziesiąt egzemplarzy)
- od 1933 do 1938 r. rutynowo odczytywali niemieckie komunikaty

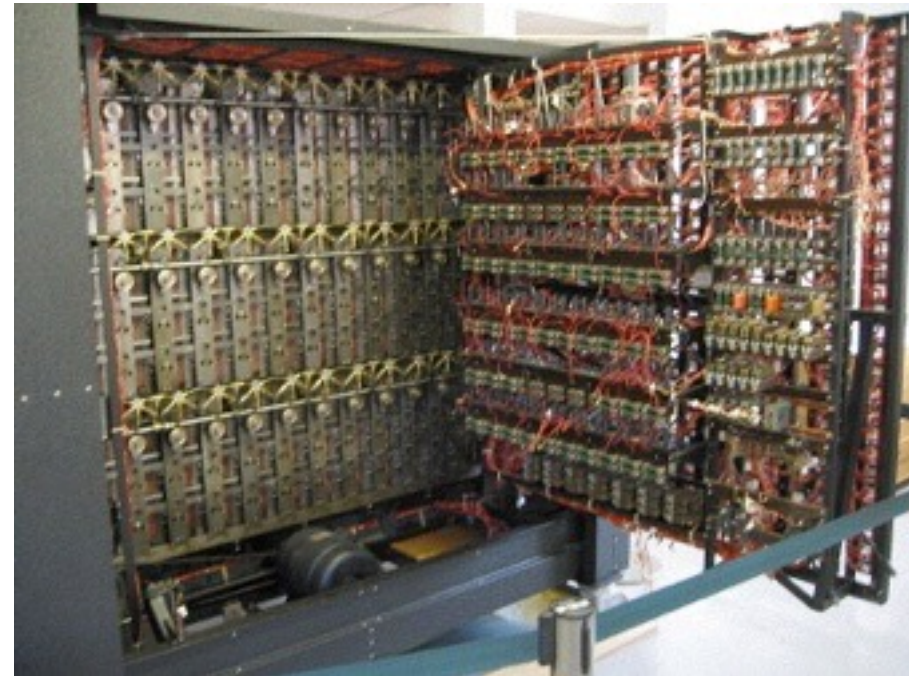
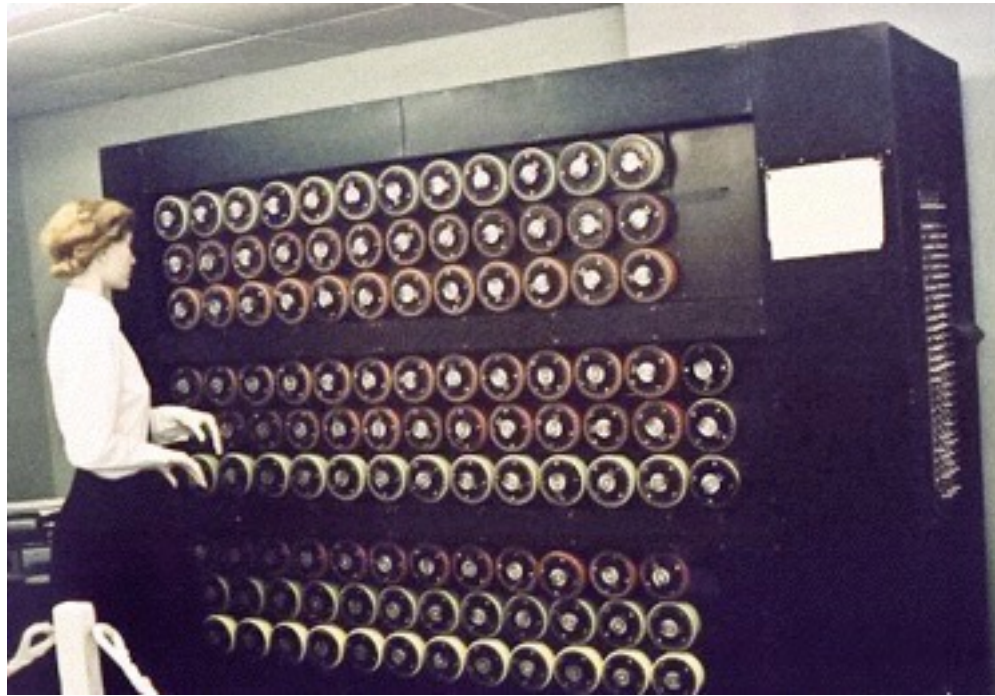
Usprawnienia Enigmy: 1939

- dwa dodatkowe rotory do wyboru
- rezygnacja z dwukrotnego kodowania klucza komunikatu
- lipiec 1939: Polacy przekazują wiedzę Anglikom
- Bletchley Park:
 - od sierpnia 1939 r.
centrum łamania szyfrów
 - osobista protekcja Churchilla
 - w 1945 r. zatrudniało 9000 ludzi
 - nigdy nie było zbombardowane



Angielskie “bomby”

- symulatory wielu Enigm na raz, projekt Turinga



- zbudowano ok. 200 maszyn
- wykluczały początkowe ustawienia rotorów na podstawie konfliktów z domniemanymi słowami w tekście jawnym
- w USA powstała wersja dla Enigmy 4-rotorowej

Szyfr Lorenz SZ40/42

- alternatywa dla Enigmy
- używany przez główne sztaby armii niemieckiej
- idea szyfrowania:
 - koduj każdą literę w 5 bitach

LETTERS FIGURES		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	CARRIAGE RETUN	LINE FEED	LETTERS	FIGURES	SPACE	ALL-SPACE NOT IN USE
CODE ELEMENTS	1	●	●		●	●	●				●	●						●		●		●		●	●	●				●	●		
	2	●		●				●		●	●	●	●				●	●	●			●	●	●				○	●	●	●		
	3	○	○	●	○	○		○		○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
	4		●	●	●		●	●			●	●	●	●	●	●	●		●				●	●	●	●		●		●	●	●	
	5		●					●	●				●	●	●	●	●	●			●		●	●	●	●	●						○

● INDICATES A MARK ELEMENT (A HOLE PUNCHED IN THE TAPE)
○ INDICATES POSITION OF A SPROCKET HOLE IN THE TAPE

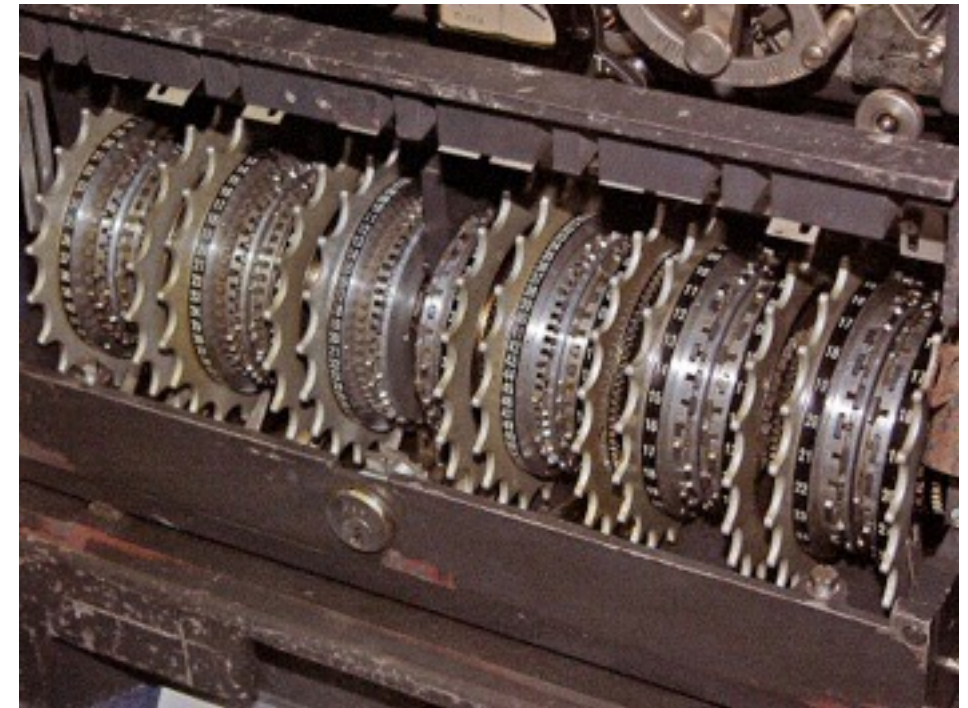
The International Telegraph Alphabet

- szyfruj $C_i = P_i \oplus K_i$
- ciąg K_i generowany w procesie pseudolosowym
- odszyfrowanie = szyfrowanie

Generacja ciągu pseudolosowego

- 12 rotorów z wypustkami

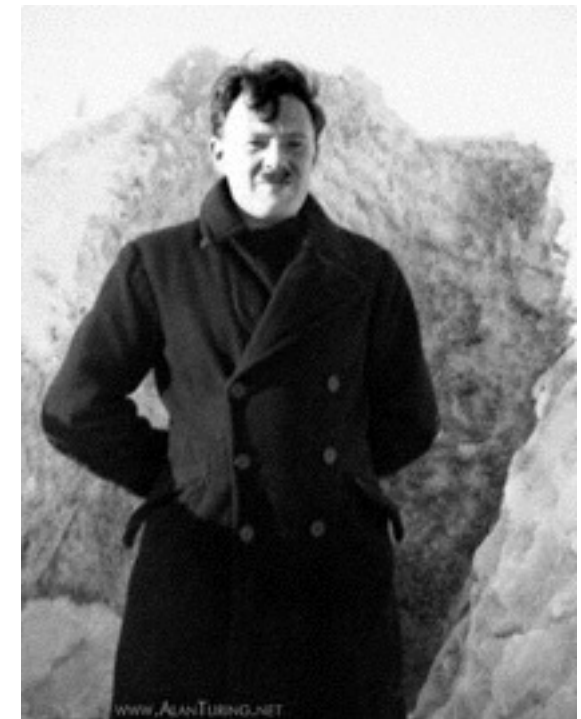
Rotor	ψ_1	ψ_2	ψ_3	ψ_4	ψ_5	μ_1	μ_2	χ_1	χ_2	χ_3	χ_4	χ_5
Rozmiar	43	47	51	53	59	37	61	41	31	29	26	23



- kolejny i -ty bit = wypustka na $\psi_i \oplus$ wypustka na χ_i
- rotory χ_i i μ_2 obracają się za każdym razem
- rotor μ_1 obraca się jeśli jest wypustka na μ_2
- rotory ψ_i obracają się jeśli jest wypustka na μ_1
- i -ty bit jest $\oplus$ -owany z i -tym bitem tekstu jawnego
- rekonfiguracja wypustek: co kwartał, potem codziennie

Łamanie szyfru Lorenz

- Aliantom nie udało się zdobyć żadnej maszyny
- 31.08.1941 błąd szyfrantów:
 - prawie identyczny tekst wysłany dwa razy z tym samym kluczem
 - skutek: prawie 4000 kolejnych elementów ciągu pseudolosowego
 - stąd **W. T. Tutte** wydedukował budowę maszyny
 - A. Turing: zgadnięcie układu wypustek
- jedyny problem: jak dopasować generowany ciąg do tekstu?



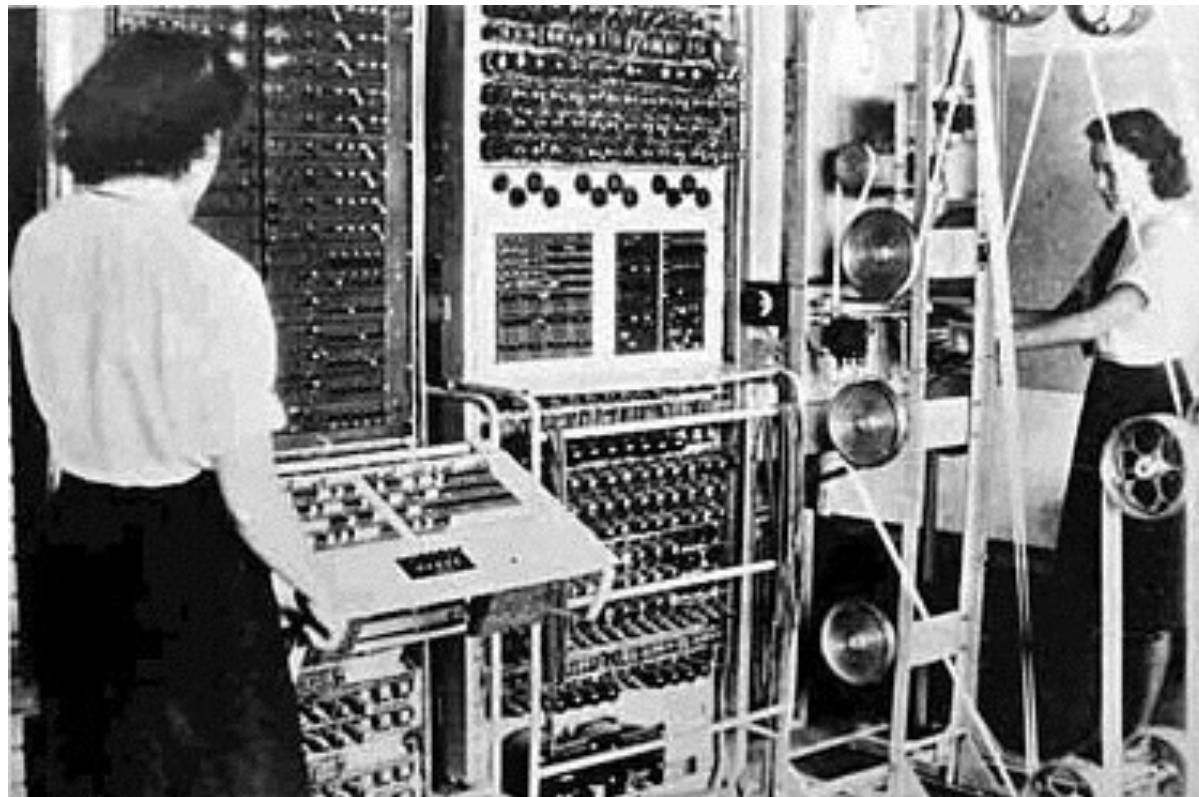
Łamanie szyfru Lorenz

- działanie rotorów χ_i zachowuje nieregularności rozkładu częstości liter
- A. Turing i W. Tutte: funkcja Boole'owska, która wychwytyje te nieregularności
- pomysł: maszyna, która policzy ją dla wszystkich układów χ_i i znajdzie właściwy
- układu ψ_i szukano już ręcznie
- pierwsza maszyna:
Heath Robinson (1943)



Colossus (luty 1944)

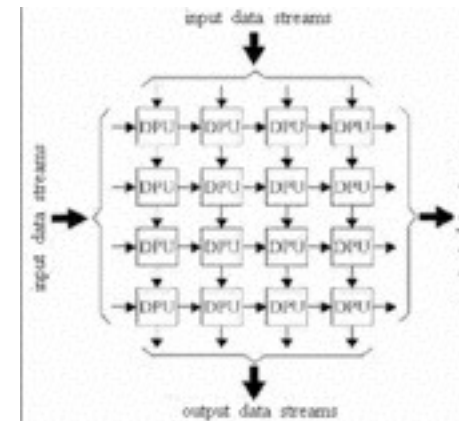
- ulepszenie maszyny *Heath Robinson*
- projektant: Thomas Flowers (1905-1998)



- zaszyfrowany tekst czytany z taśmy perforowanej
- obwód generujący ciąg pseudolosowy
- obwód liczący funkcję Turinga-Tutte'a
- obwód zliczający wartości tej funkcji

Parametry Colossusa

- ok. 1500 lamp elektronowych
- taśma czytana z prędkością 5000 znaków / sek.
- w obwodach Boole'owskich zastosowano m. in. sieci systoliczne



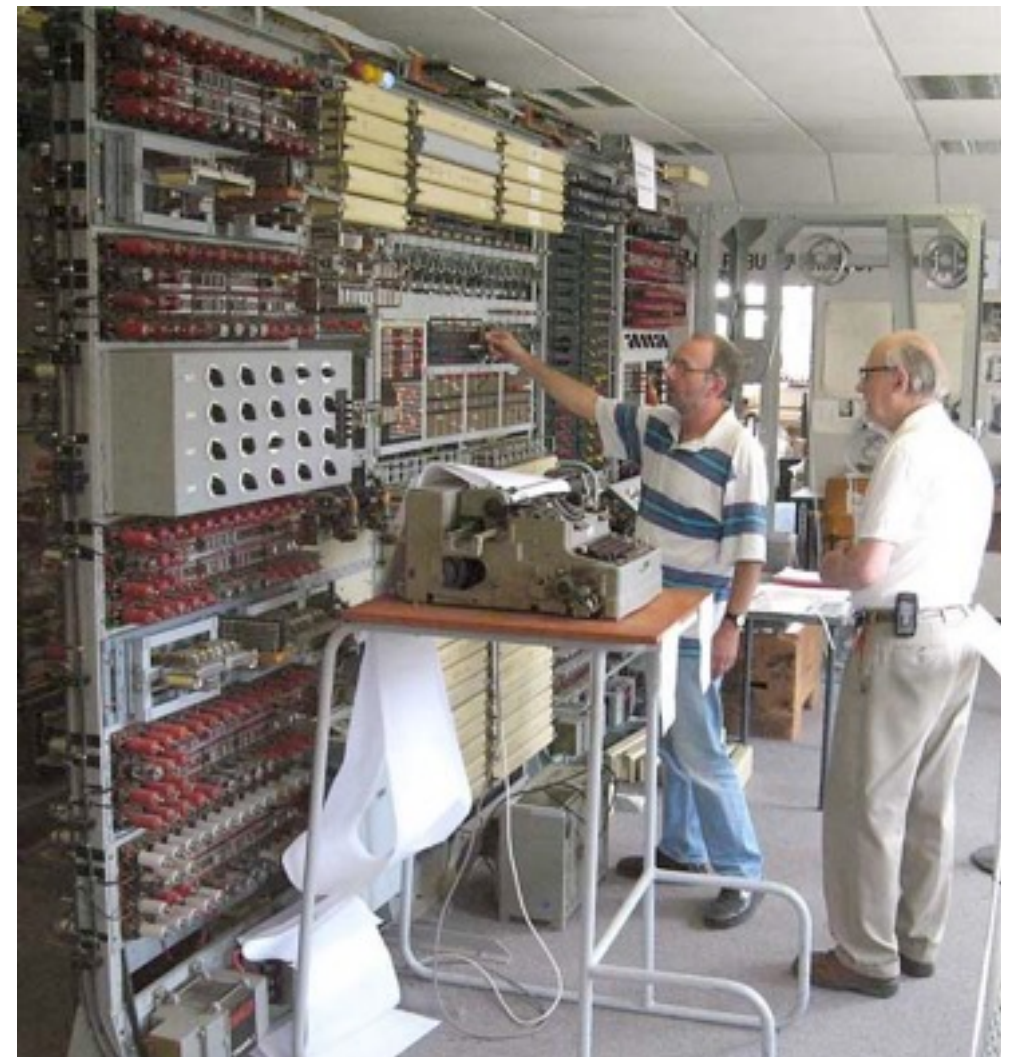
- obwody później poprzestawiano (aby m.in. obliczać układy wypustek na rotorach)

Komputer ogólnego przeznaczenia!

- ale nie Turing-zupełny

Losy Colossusa

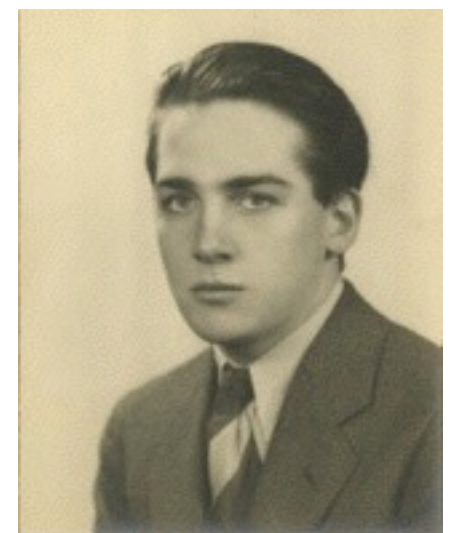
- powstało 10 egzemplarzy
- w sumie odkodowano 30MB niemieckich komunikatów
- po wojnie wszystkie rozmontowano, a dokumentację zniszczono
- projekt tajny do lat 70tych
- 1994-2007: Colossus zrekonstruowany



- [illegible]

Zespół z University of Pennsylvania

- por. Herman Goldstine (1913-2004)
 - matematyk, łącznik z zespołami liczącymi tablice
 - odpowiedzialny za przyspieszenie procesu
- John Mauchly (1907-1980)
 - matematyk, elektronik
 - zainspirowany pracą Atanasoffa-Berry'ego
- J. Presper Eckert (1919-1995)
 - inżynier elektronik
 - student wybrany przez Mauchly'ego



Notatka Mauchly'ego (1942)

- *The use of high-speed vacuum tube devices for calculating*
- nieopublikowana, kolportowana prywatnie

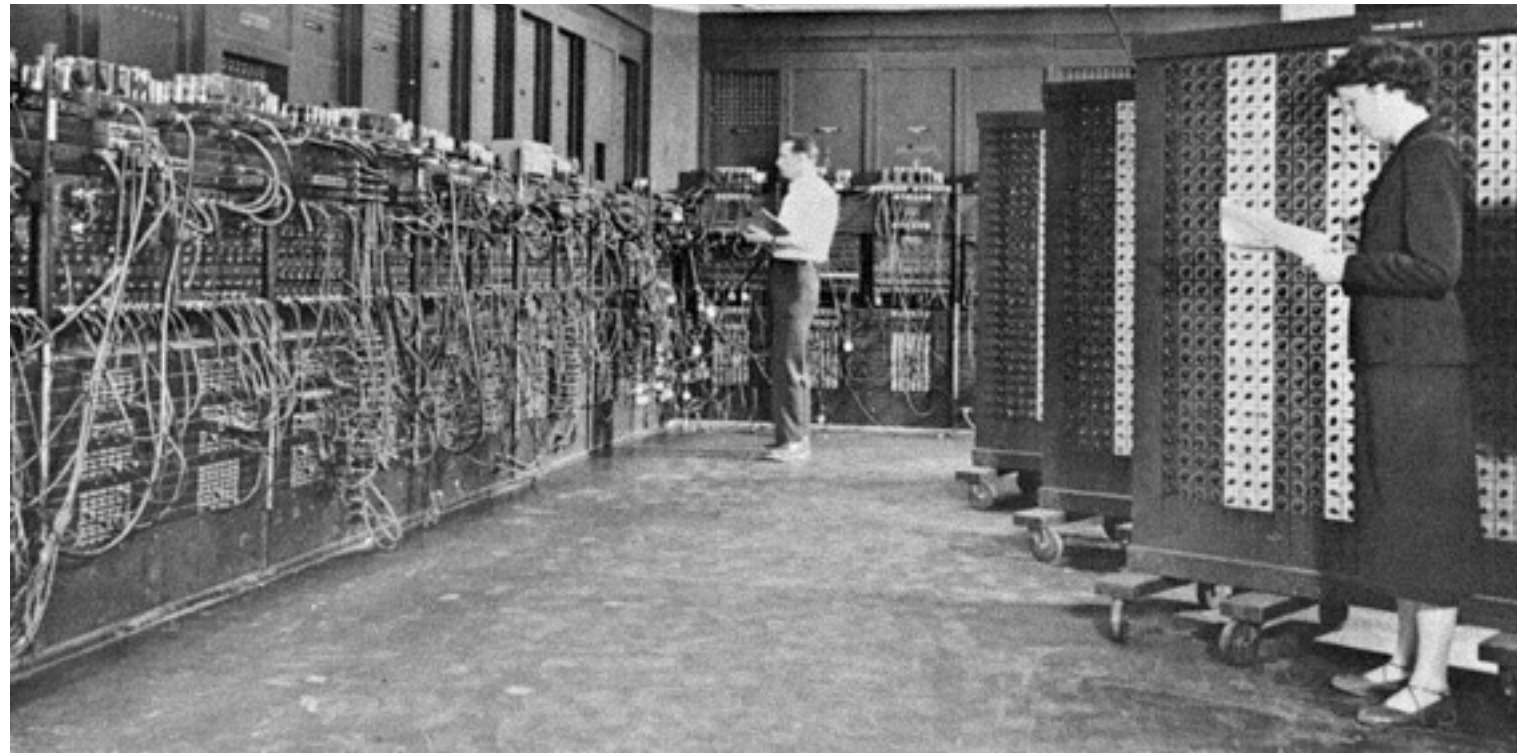
A great gain in the speed of calculation can be obtained if the devices which are used employ electronic means [...]

The ease with which the various components of such a computing device can be interconnected by cables and switching units makes it possible to set up a new problem without much difficulty.

- szacowany czas obliczenia jednej trajektorii: <2 min.
- tekst zainteresował Goldstine'a
- kwiecień 1943: armia finansuje projekt

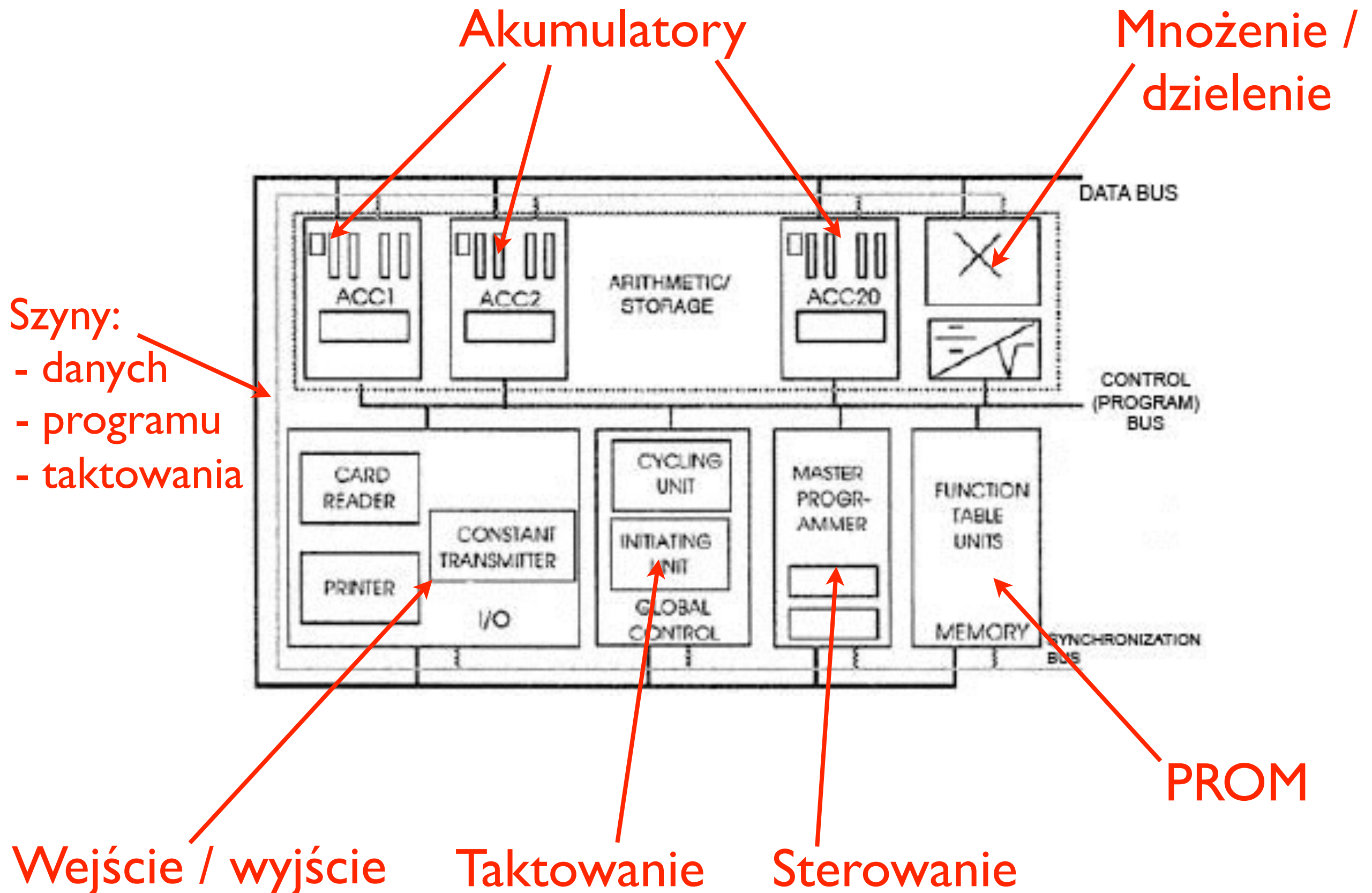
ENIAC (luty 1946)

Electronic Numerical Integrator And Computer



- 18.000 lamp, 1500 przełączników, 70.000 rezystorów
- 30 ton, pokój 10 x 15 m
- moc 150kW
- czas obliczenia 1 trajektorii: 30 sek.
- koszt ok 0.5 mln USD

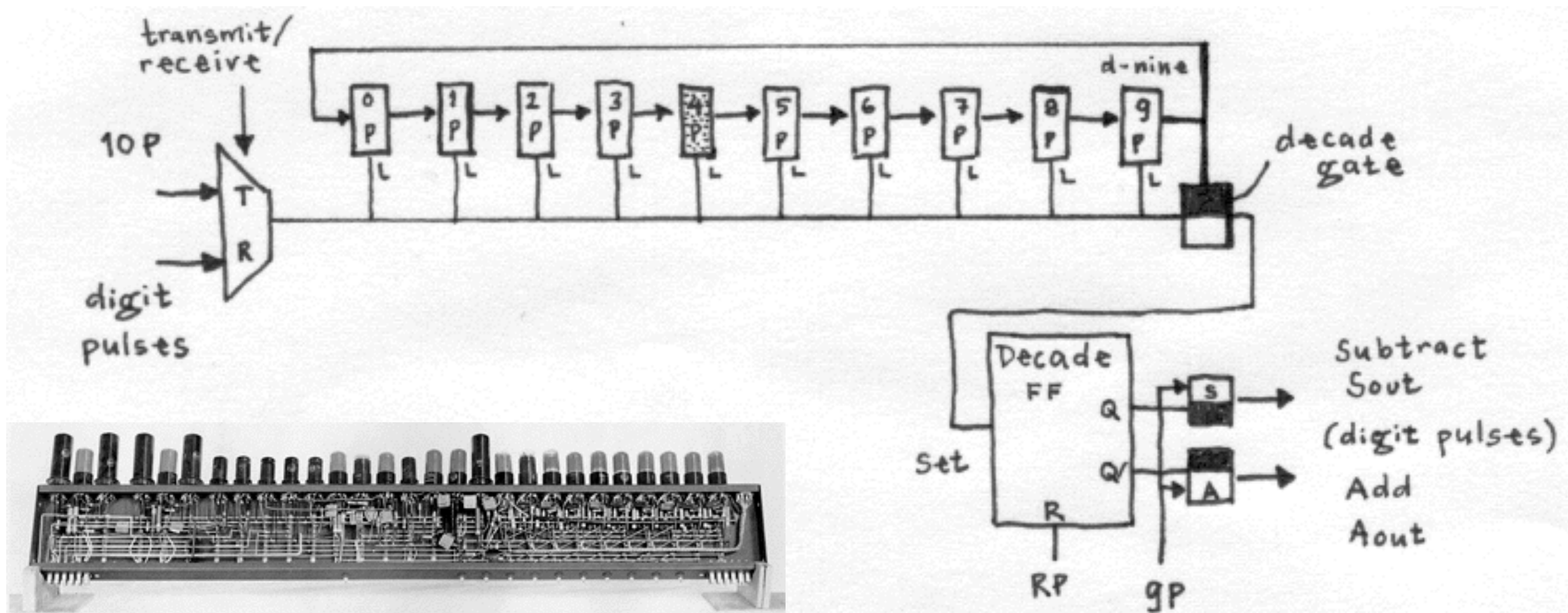
Struktura ENIACa



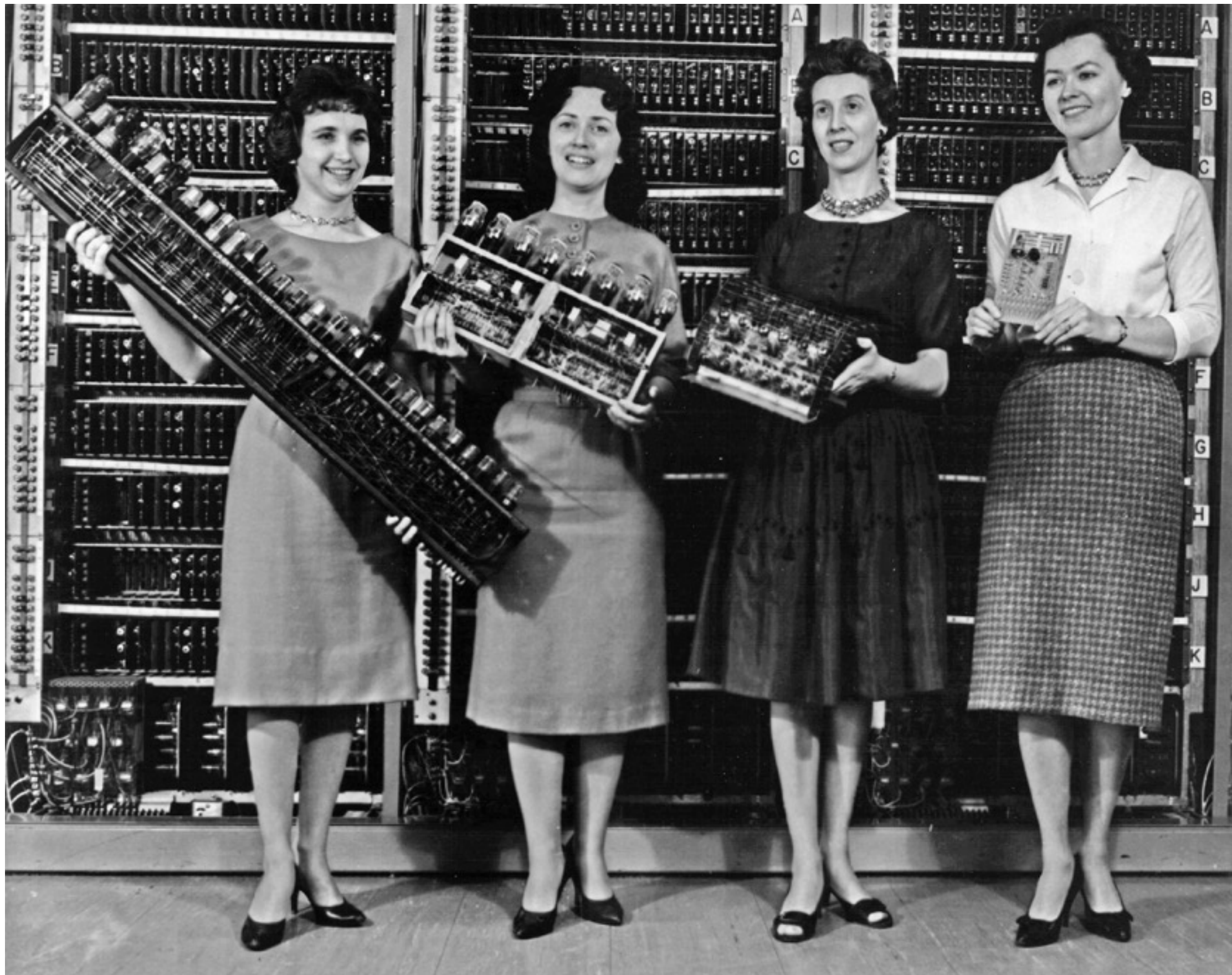
Akumulator: jedna cyfra

- cyfry transmitowane jako serie pulsów
(jak w tabulatorach, nie jak w Harvard Mark)
- seria 10 flip-flopów + bramki wyjściowe

(na rysunku pominięto przeniesienie)



Akumulator: jedna cyfra



Akumulator: panel frontowy

- w środku 10 układów 1-cyfrowych + przeniesienia

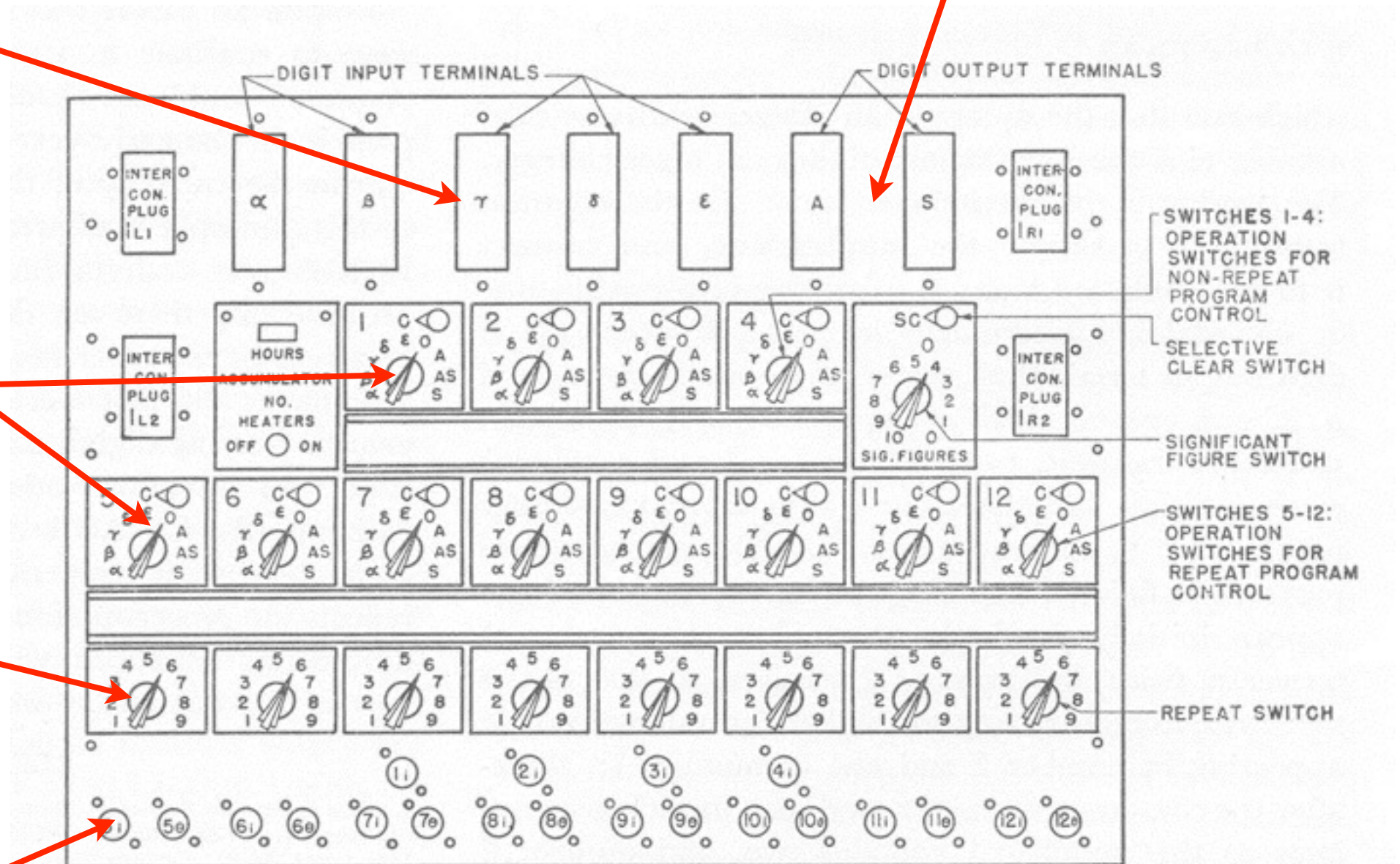
5 portów
wejściowych

2 porty wyjściowe

12 instrukcji

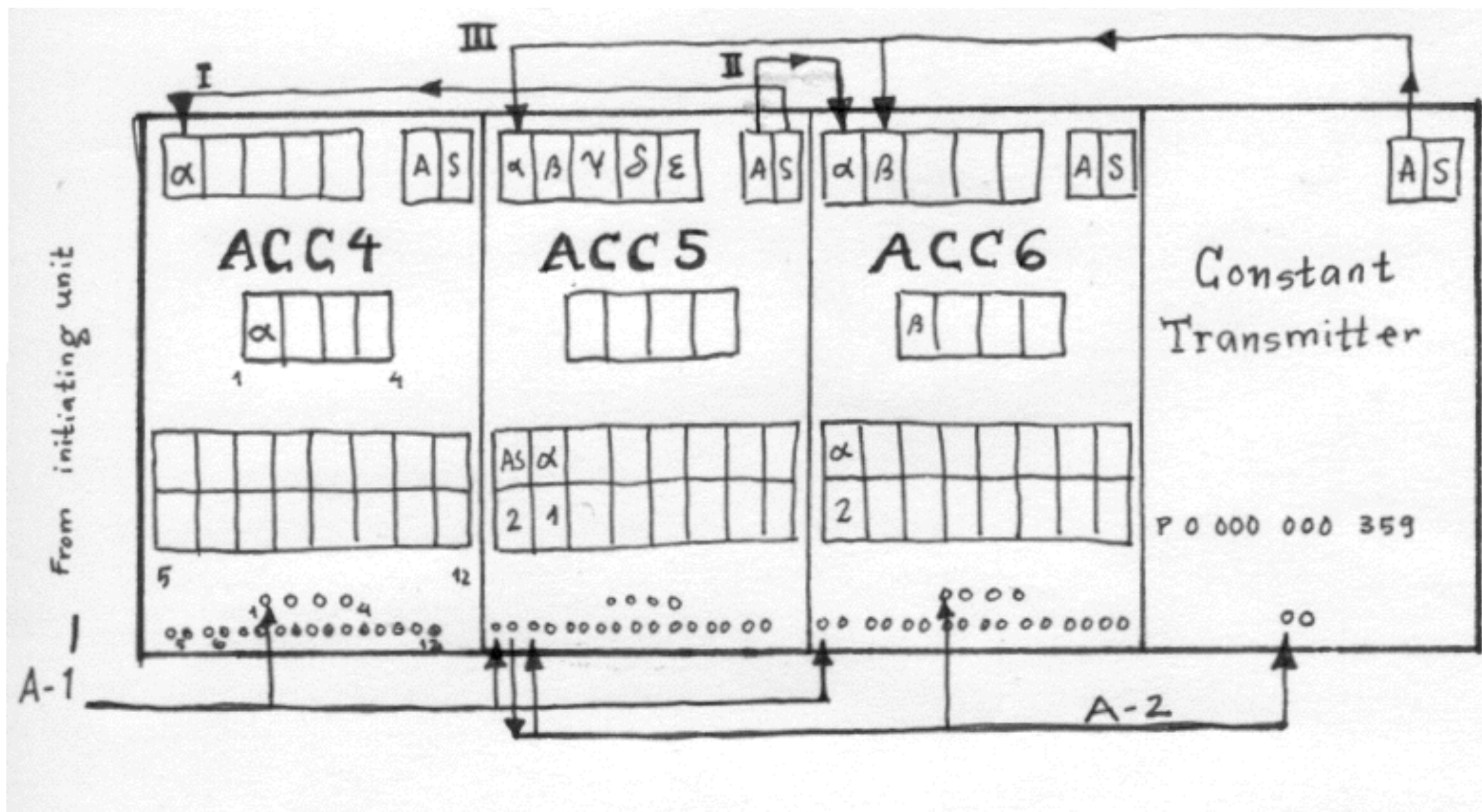
ustawienia
powtórzeń

porty
programu



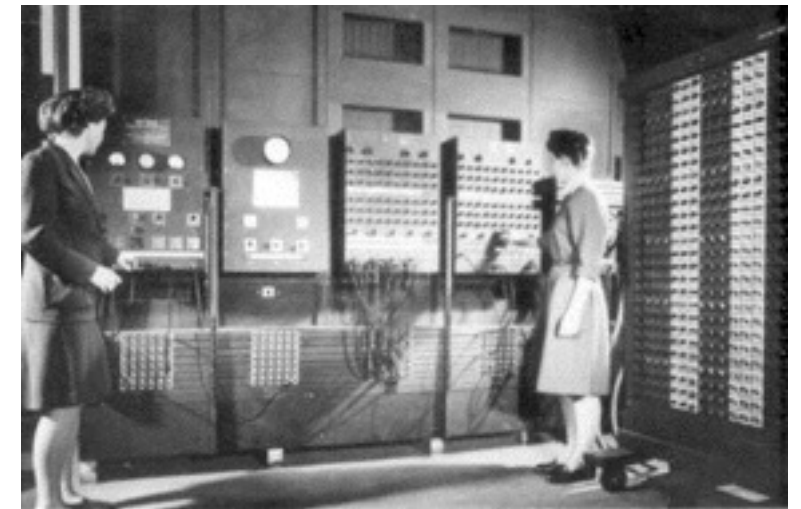
Działanie akumulatorów

Program: $x4 := x4 - x5;$
 $x6 := x6 + 2 * x5 + 359;$
 $x5 := x5 + 359$



Wejście / wyjście

- PROM:
 - tablice liczb ustalanych pokrętłami
 - podłączane do szyn danych
- wejście:
 - czytnik kart perforowanych IBM
- wyjście:
 - lampki na akumulatorach
 - tabulator IBM



Losy ENIACa

- odzew w mediach:

*Electronic Computer Flashes Answers,
May Speed Engineering*

New York Times

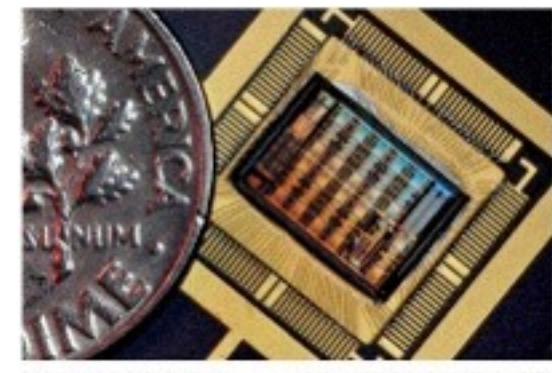
*Lightning Strikes Mathematics:
Equations that Spell Progress
are Solved by Electronics*

Popular Science

*All-Electronic Super Calculator
is a Whizz at Super Problems*

Science & Medicine

- **szybkość**: 5000 dodawań lub 350 mnożeń / sek.
- awarie średnio co 2 dni
- zastosowanie m.in. w projekcie Manhattan
- pracował do 1955 r.
- w 1995 r. rekonstrukcja na chipie



Porównanie wczesnych komputerów

		0 1			
Babbage			✓	✓	✓
Bell Labs I		✓			
Zuse Z3		✓	✓	✓	
Atanasoff	✓	✓			
Colossus	✓	✓	✓		
Harvard Mark			✓	✓	
ENIAC	✓		✓		✓